FATF

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Anti-money laundering and counter-terrorist financing measures

Israel

Mutual Evaluation Report

December 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

For more information about MONEYVAL, please visit the website: **www.coe.int/en/web/moneyval**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

FATF adopted this report at its Plenary meeting in October 2018. MONEYVAL adopted the report at its meeting in December 2018

Citing reference:

FATF-MONEYVAL (2018), *Anti-money laundering and counter-terrorist financing measures – Israel,* Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-israel-2018.html

Table of Contents

Executive Summary

1. This report summarises the AML/CFT measures in place in Israel as at the date of the on-site visit 6 to 22 March 2018. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Israel's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

a) Overall, Israel has a good understanding of its ML risks. Israel's major ML risks are mostly identified and assessed. The understanding of TF risks is generally very good. Israel's major TF risks have been identified and assessed. Activities and policies are in line with the identified ML and TF risks. DNFBP supervisors do not have a strong understanding of the potential ML/TF risks faced by the entities they supervise.

b) Israel has strong, national AML/CFT co-ordination and includes all relevant competent authorities. Israel's domestic co-ordination is driven by the Executive Steering Committee, its Implementation Committee, and sub-committees of the latter committee, which together comprise the country's main AML/CFT policy development tool. Bilateral and multilateral AML/CFT co-operation at the operational level is strong, particularly among the Israel Money Laundering and Terror Financing Prohibition Authority (IMPA), *Shin-Bet*, the Israel National Police (INP) and the Israel Tax Authority (ITA), and also between the Israel Companies Authority (ICA) and the ITA.

c) Israel's highly effective use of financial intelligence largely contributes to the prosecution and investigation of all types of ML, with a large number of cases relating to self-laundering, and cases relating to legal persons. The focus on ML activity deriving from fraud, tax evasion and other organised-crime predicate crimes is in line with the country's ML risk profile. Authorities demonstrated their ability to work together on complex and significant ML cases all the way through conviction and sentencing. The quality of IMPA's financial intelligence and analysis effectively supports the operational needs of LEAs. From 2014-2017, Israel averaged 415 ML investigations, 50 ML prosecutions, and 34 convictions in ML prosecutions per year.

d) Overall, the competent authorities are confiscating the proceeds and instrumentalities of proceeds of crime successfully. Israel set out confiscation of criminal proceeds and instrumentalities as a high-level priority and a policy

objective, and results are in line with the ML risk profile to a very large extent. From 2013-2017, Israel averaged EUR 24.6 million per year in confiscations achieved.

e) Israel has developed a wide range of effective instruments and mechanisms to combat terrorism and terrorist financing in all its aspects. Different types of TF cases are prosecuted, and offenders convicted. These cases are consistent with Israel's TF risk profile. *Shin-Bet*'s and the other security agencies' proactive efforts are effective in disrupting terrorism at the early stages. Israel effectively deprives terrorists, terrorist organisations, and terrorist financers of their assets and instrumentalities related to TF activities. A large amount of funds and property have been frozen, seized, and confiscated.

f) Co-operation and co-ordination of operational matters on NPOs between authorities is strong but the overall jurisdictional response to NPOs is not comprehensively co-ordinated. Israel has established a registration and supervision framework covering the NPOs most at risk of TF abuse. The ICA is a proactive registrar and supervisor and its approach contains strong elements which mitigate the risk of TF abuse.

g) Israel has implemented comprehensive and effective counter-proliferation finance targeted financial sanctions (PF-TFS) with regard to Iran, which are implemented without delay. Since the requirements of PF-TFS in relation to DPRK only came into force during the on-site visit, the compliance programmes for FIs, DNFBPs, and supervisors which were in place to ensure implementation of PF-TFS obligations relating to Iran, were not yet applicable with regard to DPRK.

h) In the financial sector, the application of risk-based supervisory model is ongoing, with Israel Securities Authority being the most advanced, and the Capital Market, Insurance and Savings Authority in relation to money service businesses being less advanced.

i) Regarding DNFBPs, Israel has not included real estate agents, dealers in precious metals, and trust and company service providers in its AML/CFT system. Diamond dealers, lawyers and accountants were only recently incorporated in the AML/CFT regime. Lawyers and accountants do not have STR requirements. DNFBP supervisors are at an early stage in the development of a risk-based model for supervision and awareness-raising initiatives for AML/CFT obligations.

j) There is a good level of transparency of basic information on legal persons and arrangements. The high quality of beneficial ownership information available supports a significant number of cases against legal persons by the ITA and by other LEAs and the SAO in light of the adequacy, accuracy, and currency of such information. Though Israel has sought to understand the risks posed by legal persons and arrangements, the assessment and understanding of vulnerabilities and misuse are not comprehensive.

k) Israel provides constructive and quality information and assistance when requested, but faces occasional challenges in providing this in a timely manner. Israel is successfully receiving responses to its requests for international co-operation. Israel also extensively uses its informal channels of co-operation and authorities are overall well engaged and committed to execute requests where permitted.

Risks and General Situation

2. The main ML risks Israel faces include: ML derived from fraud and tax offences, and organised crime. The Money Service Businesses (MSBs) sector and the use of cash were also identified as high ML risk areas. Predicate criminality also includes false invoicing and the misuse of complex corporate structures, including through offshore centres. Public sector corruption is recognised as an ongoing issue, and has been identified as a moderate-high ML threat in the NRA.

3. Inherent to its geographic location, Israel faces a high TF threat emanating from sources outside Israel. Some of the specific TF sources and channels identified are through funding from other jurisdictions, supposedly legitimate business activities, donations, foreign non-profit organisations (NPOs), smuggling of goods, valuables and funds through border crossings, including through trade, and the use of money transfer mechanisms that include correspondent activity, currency service providers, pre-paid cards, and foreign credit cards.

Overall Level of Compliance and Effectiveness

4. Israel has implemented an AML/CFT system that is effective in many areas. Particularly good results are being achieved in the areas of ML/TF risk assessment and risk understanding, investigation and prosecution of ML and TF, including the use of financial intelligence, targeted financial sanctions related to terrorism financing, preventing misuse of legal structures, and co-operating domestically and internationally. However, major improvements are needed to strengthen supervision and implementation of preventive measures.

5. With regard to technical compliance, the legal framework is particularly strong, with only some areas in need of significant improvement: measures related to wire transfers, internal controls and FI's foreign branches and subsidiaries, and the full range of preventive measures and supervision for several DNFBPs.

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

6. Overall, Israel has a good understanding of its ML risks. Israel's major ML risks are mostly identified and assessed, although there is need for a more comprehensive approach to risk assessment in a limited number of areas (legal persons and legal arrangements, and NPOs). The understanding of TF risks is generally very good. Israel's major TF risks have been identified and assessed.

7. Israel has strong, national AML/CFT co-ordination and includes all relevant competent authorities. Israel's domestic co-ordination is driven by the Executive Steering Committee, its Implementation Committee, and sub-committees of the latter committee, which together comprise the country's main AML/CFT policy development tool. Bilateral and multilateral AML/CFT co-operation at the operational level is strong, particularly among the Israel Money Laundering and Terror Financing Prohibition Authority (IMPA), the Israel National Police (INP), the Israel Tax Authority (ITA) and *Shin-Bet*, and also between the Israel Companies Authority (ICA) and the ITA.

8. The authorities have developed co-ordinated action plans to address identified ML/TF risks, and have implemented a significant number of the priority actions – such as legislation on TF targeted financial sanctions, on the use of cash, and on reduced threshold for disclosure of cash at borders, and the establishment of two new task forces on TF and MSBs.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.3, 4, 29–32)

Use of financial intelligence (Immediate Outcome 6)

9. Israel effectively uses financial intelligence and other information to investigate ML, predicate offences and TF, and to trace criminal proceeds. This is a strong point of the Israeli system and at the centre of its approach to combating crime and terrorism. The database of the Israeli FIU (IMPA) is the primary repository of financial intelligence, and authorities have also direct access to a wide variety of financial intelligence and other information, most of which exist in various governmental databases and registries.

10. IMPA has the resources, both human and technical, and expertise, to effectively conduct in-depth strategic and operational analysis with the view to develop quality intelligence reports for dissemination to LEAs. In particular, IMPA's well-developed IT system and trained analysts greatly contribute to the relevance of the financial intelligence it produces in the conduct of ML/TF investigations. Competent authorities successfully demonstrated that they use this information to develop evidence in support of ML/TF investigations and to identify and trace assets, including abroad.

11. IMPA's high degree of co-ordination and co-operation and exchange of financial intelligence with LEAs (including security agencies) greatly contributes to making the Israeli system highly effective.

ML offence (Immediate Outcome 7)

12. Israel successfully identifies and investigates ML cases, on the basis of the financial intelligence developed by IMPA but also information supplied through law enforcement intelligence, including through ongoing investigation of predicate offences. Authorities provided a number of cases to demonstrate their ability to work on complex and/or significant ML cases. Many of these cases have been progressed at the national level through inter-agency structures, such as the Intelligence Fusion Centre and the thematic task forces, but there are notable contributions to the number of complex investigations from regional and local resources.

13. Israel regularly investigates and successfully prosecutes all types of ML offences, including cases of stand-alone, third party ML and ML involving foreign predicate offending largely in line with the risk profile. Israel pursues its ML activity in line with its national priorities and targets its main domestic ML threats as identified in its NRA - i.e. fraud, fictitious invoicing, tax evasion and corruption. However, nearly four out of five cases of ML prosecutions relate to self-laundering, and there are a low number of stand-alone ML prosecutions. From 2014-2017, Israel averaged 415 ML investigations, 50 ML prosecutions, and 34 convictions in ML prosecutions per year (out of which approximately 20% are non self-laundering).

14. Authorities pursue investigated ML cases through to convictions, including with cases of successful conviction and sentencing of legal persons. Sentencing for ML offences is considered proportionate and dissuasive when compared to the punishments for other similar crimes (e.g. fraud, tax). Sentences are however often combined with other criminality which makes a full determination difficult. There is also a concern about the time taken for certain ML cases to progress through the courts, especially those cases which do not involve persons in custody, and particularly legal persons and NPOs, which can take years.

Confiscation (Immediate Outcome 8)

15. Overall, the competent authorities are confiscating the proceeds and instrumentalities of proceeds of crime successfully. Confiscation efforts extend to the tracing and the recovery of proceeds from abroad, and include the taking of provisional measures. From 2013-2017, Israel averaged EUR 24.6 million per year in confiscations achieved.

16. Israel clearly set out confiscation of criminal proceeds and instrumentalities as a high-level priority and as a policy objective. The results reflect the national strategic objective, i.e. the tackling of all types of organised crime activities, and are in line with the ML risk profile (i.e. tax crimes and fraud) to a very large extent.

17. Despite Israel's legal framework only allowing for value-based confiscation in relation to specific criminality, authorities are in practice confiscating proceeds involving equivalent value through the pursuing of self-laundering cases, which is one of the types of criminality to trigger value-based confiscation, in tandem with the predicate offences. However, this methodology is only relied upon when the suspect has taken a proactive additional action deemed to be ML. Israel's non-conviction based forfeiture regime is restricted to an administrative process and does not extend to any kind of civil confiscation system.

18. There is a strong framework in place to address the threat of cross-border movements of cash and bearer negotiable instruments that are falsely or not declared. The sanctions applied are proportionate and dissuasive.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

TF offence (Immediate Outcome 9)

19. Israel has developed a wide range of effective instruments and mechanisms to combat terrorism and terrorist financing in all its aspects.

20. Different types of TF cases are investigated and prosecuted, and offenders convicted. These cases are consistent with Israel's TF risk profile and include TF cases on the collection, movement and use of funds, as well as TF cases that did not involve terrorism charges. These cover a spectrum of TF typologies. *Shin-Bet*'s and the other security agencies' proactive efforts are effective in disrupting terrorism at the early stages. Between 2013 and 2017, 37 cases resulted in convictions for one or more TF offences, involving 26 natural and legal persons.

21. TF cases are well identified and investigated. *Shin-Bet* leads on counter-terrorism and TF intelligence and is the main source of TF investigations, while INP

leads on formal investigations. IMPA also plays a key role in identifying TF cases for investigation.

Preventing terrorists from raising, moving and using funds (Immediate Outcome 10)

22. Israel implements targeted financial sanctions (TFS) for TF without delay. Israel has demonstrated its ability to implement TFS within the context of UN designations pursuant to UNSCRs 1267/1989 and 1988, domestic designations, and in relation to international requests.

23. The National Bureau for Counter Terror Financing (NBCTF) in the Ministry of Defence leads and co-ordinates the designation process. The Bureau has overall responsibility for co-ordinating national CFT enforcement policies, and works closely with *Shin-Bet*, who initiates most domestic designations, as well as INP, IMPA, and the security agencies. Israel has the necessary mechanisms for identifying targets through this co-operation.

24. Co-operation and co-ordination of operational matters on NPOs between authorities is strong (including sharing of the ICA's database with the ITA) but the overall jurisdictional response to NPOs is not comprehensively co-ordinated.

25. Israel has established a registration and supervision framework covering the NPOs most at risk of TF abuse. The ICA is a proactive registrar and supervisor and its approach contains strong elements which mitigate the risk of TF abuse (including attention to donors). On-site inspections appear to be of good quality. Nevertheless, the overall volume of supervision needs to be increased (as does the use of sanctions); the approach does not include a TF focused risk-based approach and there is some shortfall in the number of staff. The ITA is also proactive in relation to NPOs; it holds substantial information and has a positive role in increasing standards and preventing misuse of NPOs.

26. Israel effectively deprives terrorists, terrorist organisations, and terrorist financers of their assets and instrumentalities related to TF activities. A large amount of funds and property were frozen, seized and confiscated.

Proliferation financing (Immediate Outcome 11)

27. Israel has implemented comprehensive and effective counter-proliferation finance targeted financial sanctions with regard to Iran, which are implemented without delay. The Sanctions Bureau, in the Ministry of Finance (MoF), co-ordinates efforts relating to PF sanctions and the accessibility of the information of sanctions to the public and business sector.

28. Since the requirements of PF-TFS in relation to DPRK only came into force during the on-site visit, the compliance programmes for FIs, DNFBPs, and supervisors which were in place to ensure implementation of PF-TFS obligations relating to Iran, were not yet applicable with regard to DPRK. This is mitigated by the fact that most FIs and some DNFBPs screen customers and transactions against all international lists, including those relating to DPRK.

29. Given the comprehensive prohibitions against Iran, which are well understood and are a priority for FIs, and the trade restrictions and limited exposure relating to

DPRK, no funds or other assets of designated persons and entities have been identified.

Preventive measures (Chapter 5; IO.4; R.9–23)

30. Financial institutions generally have a good understanding of their ML/TF risks and obligations. They have also developed and applied appropriate AML/CFT controls and processes to mitigate risks, including CDD and transaction monitoring, as well as EDD measures. Overall, such understanding and application is more sophisticated in the banking sector and weaker among MSB providers (including credit service providers). Generally speaking, the level of suspicious transaction reporting is commensurate with the level of ML/TF risks faced by Israel and the size of its financial sector. There has been a sharp increase in the level of reporting by MSB providers in recent years, largely due to recent incorporation of the sector in the AML/CFT regime and extensive outreach by authorities. Financial institutions generally have adequate internal controls.

31. Real estate agents, dealers in precious metals, and trust and company service providers are not covered by the Israeli AML/CFT system. Diamond dealers, lawyers and accountants were only recently incorporated in the AML/CFT regime, although lawyers and accountants are not required to report suspicious transactions. Covered DNFBPs have a moderate understanding of ML/TF risks and obligations. Their AML/CFT controls and processes, risk mitigation programmes are generally not advanced, especially when compared to the financial sector. Similarly, the level of internal controls adopted by covered DNFBPs is not as comprehensive. AML/CFT-specific training is also not as frequent and comprehensive.

Supervision (Chapter 6; IO.3; R.26–28, 34, 35)

32. Financial supervisors have a good understanding of ML/TF risks in the financial sectors they supervise, with the exception of the MSB sector. For those supervisors having prudential supervisory duties, they generally rely on their available prudential supervisory programmes for AML/CFT purposes. Overall, financial supervisors are at an early stage in developing a risk-based AML/CFT-specific supervision. The degree to which they follow a risk-based supervision approach varies, and is particularly low for the MSB sector. Most of them have not conducted their own AML/CFT-dedicated sectoral or institution-specific risk assessments. As a result, the supervision programme, including on-site and off-site inspection, general monitoring, follow-up measures, have not been planned and undertaken according to the identified ML/TF-specific risk level of individual supervised entities.

33. Financial supervisors implement robust market entry controls. Israel has also recently introduced a licensing regime for the MSB sector (fully in force by October 2018). Financial supervisors have only applied limited sanctions or remedial actions in case of non-compliance with AML/CFT requirements. Only non-compliant MSBs were subject to relatively higher level of fines, but their deterrent effect could not be fully established. Financial supervisors are generally successful in promoting a clear understanding of AML/CFT obligations. Overall, significant improvement in MSB supervision will be required.

34. DNFBP supervisors do not have a strong understanding of the potential ML/TF risks faced by the entities they supervise. They do not currently conduct risk-based supervision, and are at an early stage in the development of a risk-based model. DNFBP supervisors implement robust market entry controls in relation to lawyers and accountants providing BSP services. However, in the precious stones sector, only diamond dealers (not other precious stones dealers) are subject to a licensing regime. DNFBP supervisors have not applied effective and dissuasive sanctions where entities have failed to meet required AML/CFT obligations.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

35. Basic information on the creation and types of legal persons is publicly available. Israel has undertaken a risk assessment of legal persons and arrangements. Understanding of risks is substantially more developed in practice than the risk assessment suggests but assessment and understanding of vulnerabilities and misuse are not yet comprehensive.

36. The ICA maintains registers of companies, partnerships and public trusts, which are publicly accessible. For the vast majority of legal persons, registered information also constitutes beneficial ownership information. Some steps are taken to manage the adequacy, accuracy and currency of data on companies but these are not yet comprehensive.

37. The ITA maintains a register of Israeli resident trusts and holds information on the beneficial ownership of companies and trusts. It is an important source of beneficial ownership information. Very good quality beneficial ownership information is also available from FIs and DNFBPs. Information held by banks is the highest quality among all supervised entities. The high quality of information supports a significant number of cases against legal persons by the ITA and by other LEAs and the SAO in light of the adequacy, accuracy, and currency of such information.

38. The ICA has taken some substantial steps to impose sanctions. However, the range of sanction powers available to it and its overall use of sanctions are not comprehensive. The approaches to sanctions applied by the ITA and supervisors of FIs and DNFBPs vary and are not sufficiently effective.

International co-operation (Chapter 8; IO.2; R.36–40)

39. International co-operation is particularly important for Israel given that most of the large, domestic ML cases have international links (e.g. laundering of foreign predicates, activities of transnational organised crime groups). Inherent to its geographic location, Israel also faces a high TF threat emanating from sources abroad. Israel generally provides constructive information to foreign requests, including on beneficial ownership. The feedback received indicates that the quality of the assistance provided is good, and supports ML investigations. The feedback also suggests that some problems have arisen in the context of identified delays in executing MLA and extradition requests, time being taken to seek clarifications or to meet the country's evidentiary requirements.

40. Israel seeks international co-operation to pursue criminals and their assets located or moved abroad, through formal and informal co-operation.

41. With regards to other forms of co-operation, supervisory authorities co-operate and exchange information with their counterparts, where permitted (e.g. on the basis of MoUs), while IMPA does not need an MOU to exchange financial intelligence with counterparts. LEAs make extensive use of their informal co-operation mechanisms, through dedicated units in the INP and its police attaches abroad.

Priority Actions

a) Incorporate real estate agents, precious metal dealers, and TCSPs within the national AML/CFT regime, including the introduction of licensing/ registration/other controls to prevent potential market entry abuse for ML/TF purposes by criminals, and implementation of all preventive measures. Introduce suspicious transaction reporting requirements for lawyers and accountants conducting activities covered by the FATF standards;

b) Enhance DNFBP supervisors' understanding of ML/TF risks, especially in relation to precious stones sectors;

c) Ensure that both financial and DNFBP supervisors fully adopt a risk-based approach to supervision, especially among MSBs and DNFBPs;

d) Ensure that financial supervision should focus on verifying financial institutions' application of EDD in higher risk situations in relation to targeted financial sanctions, domestic and foreign PEPs, as well as filing of UARs when CDD processes cannot be completed;

e) Conduct a more in-depth analysis of the risks posed by legal persons and arrangements and establish a co-ordinating mechanism to ensure adequate mitigating measures are put in place in response to the assessment;

f) Ensure that ICA adopts a risk-based approach to ensure adequacy and accuracy of beneficial ownership information, and be provided with sufficient sanctioning powers;

g) A mechanism should be established to increase co-ordination in relation to NPOs, including proactive and effective compliance with measures to address potential TF abuse of NPOs, on a whole-of-government basis;

h) Address the technical gaps in its legislation to fully and directly enable value-based confiscation including the gap in provisional seizure measures;

i) Although the issue does has not hindered effectiveness, Israel should address the technical gaps in the targeted financial sanctions framework so that, in particular, Israeli citizens and residents can be designated, and so that the MoD does not have discretion not to make the automatic designations from the UN permanent.

j) Build and implement comprehensive compliance-ensuring programmes for FIs, DNFBPs, and supervisors for PF-TFS relating to DPRK. The supervisory and monitoring regime in respect of FIs and DNFBPs, in terms of frequency of outreach and inspections should be strengthened.

k) Continue to address noted delays in responding to MLA and extradition requests, by allocating more human resources and/or by considering designating INP as the main recipient of incoming MLA requests requiring investigative action.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings (High, Substantial, Moderate, Low)

IO.1 - Risk, policy and coordination	IO.2 International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	**Substantial**	**Moderate**	**Moderate**	**Substantial**	**High**
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Substantial	**High**	**High**	**Substantial**	**Moderate**	

Technical Compliance Ratings (C - compliant, LC – largely compliant, PC – partially compliant, NC – non compliant)

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and coordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	**C**	**LC**	**LC**	**C**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
LC	**LC**	**C**	**LC**	**LC**	**LC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
C	**C**	**C**	**PC**	**NA**	**PC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	**C**	**C**	**PC**	**PC**	**LC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
LC	**LC**	**C**	**PC**	**C**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
C	**C**	**C**	**C**	**LC**	**C**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	**LC**	**C**	**LC**		

MUTUAL EVALUATION REPORT ISRAEL

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 6 to 22 March 2018.

The evaluation was conducted by an assessment team consisting of:

- Gerardine Coyle, Department of Justice and Equality, Ireland;
- Dick Gould, National Crime Agency, the UK;
- Raoul Jacobs, Federal Financial Supervisory Authority (BaFin), Germany;
- Anurag Kumar, National Investigation Agency, India;
- Richard Walker, Financial Crime and Regulatory Policy, Guernsey; and
- Ian Wong, Singapore Police Force, Singapore.

The team was supported by the FATF Secretariat, represented by Kevin Vandergrift, Masha Rechova, and Janet Ho. The report was reviewed by Andrew Hill (New Zealand), Poovindree Naidoo (South Africa), Vladimir Nechaev (EAG Secretariat) and the MONEYVAL Secretariat.

Israel previously underwent MONEYVAL Mutual Evaluations in 2013, conducted according to the 2004 FATF Methodology. The report has been published and is available at http://www.coe.int/en/web/moneyval/jurisdictions/Israel.

That Mutual Evaluation concluded that the country was compliant with 20 Recommendations; largely compliant with 15; partially compliant with 11; and non-compliant with three. Israel was rated compliant or largely compliant with 14 of the 16 Core and Key Recommendations. Israel was placed under the regular follow-up process immediately after the adoption of its 4th round mutual evaluation report and reported back to MONEYVAL in December 2014, December 2015 and December 2016 respectively. In line with MONEYVAL's rule of procedure, the follow-up was subsequently discontinued one year ahead of the on-site visit under the 2013 FATF Methodology.

CHAPTER 1. ML/TF RISKS AND CONTEXT

42. Israel is situated in the Middle East, along the eastern coastline of the Mediterranean Sea. The country is about 470 km in length from north to south and some 135 km across at its widest point between the Dead Sea and the Mediterranean coast.

43. The population of Israel is approximately 8.5 million. Since the establishment of the State of Israel in 1948, approximately 3.2 million Jewish have immigrated to Israel. In 2016, Gross Domestic Product (GDP) was estimated at USD 317.7 billion (Gross domestic product per capita in current prices USD 37 192) with real growth in GDP being estimated at 4.0%.[1] In 2017 GDP was estimated at USD 350.6 billion (GDP per capita in current prices USD 40 258) with real growth in GDP of 3.3%.

44. Israel has no formal constitution. The State of Israel is a parliamentary democracy whose governance powers are divided between the legislative, executive, and judicial branches. The legislative power of the State of Israel resides in the Knesset, a unicameral parliament. Members of the Knesset are elected by universal suffrage under a system of proportional representation.

45. The courts of the Judicial Branch consist of: Magistrates' courts, District courts and the Supreme Court which functions both as the highest appellate level, as well as the High Court of Justice. Other matters of personal status there are within the authority of the religious courts: Rabbinical (Jewish) Courts, *Sharia'a* (Muslim) Courts, Christian and Druze Courts (the three major communities that exist in Israel). Israel's criminal justice system is closely tailored after the common-law system. Judicial decisions play a significant role in the development and consolidation of criminal law in Israel.

46. In 2017, Israel's main export and import partners were the United States (US), the European Union (EU), the United Kingdom (UK), and China.[2] The main export and import merchandise are manufactured goods, machinery and transport equipment, high-tech services (mainly export) and chemical and related products.

47. Israel has been a member of the Organisation for Economic Co-operation and Development (OECD) since 2010.

1. World Bank (n.d), Country Profile Israel, http://databank.worldbank.org/data/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=ISR
2. WTO (n.d), Country Profile Israel http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=IL

1

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

48. The main ML risks Israel faces include: ML derived from fraud and tax offences, and organised crime. The Money Service Businesses (MSBs) sector and the use of cash were also identified as high ML risk areas. Predicate criminality also includes false invoicing and the misuse of complex corporate structures, including through offshore centres. Public sector corruption is recognised as an ongoing issue, and has been identified as a moderate-high ML threat in the NRA.

49. The overall threat deriving from serious organised crime and related-ML is considerable in Israel. In 2006, the Israeli government, in its effort to combat domestic and transitional organised criminal activity, identified the targeting of illicit proceeds as primary objective by *Government Decision no. 4618 (2006)*. A number of task forces have also been set up subsequently to investigate ML cases generated by organised crime networks and those connected to other crimes identified as high risk.

50. Inherent to its geographic location, Israel faces a high TF threat emanating from sources outside Israel. Some of the specific TF sources and channels identified are through funding from other jurisdictions, supposedly legitimate business activities, donations, foreign non-profit organisations (NPOs), smuggling of goods, valuables and funds through border crossings, including through trade, and the use of money transfer mechanisms that include correspondent activity, currency service providers, pre-paid cards, and foreign credit cards.

Country's Risk Assessment & Scoping of Higher Risk Issues

51. Authorities have drawn upon a range of assessments to identify, assess and understand Israel's ML/TF risks. The non-classified version of (a) the ML NRA (including both the ML risk assessments issued by LEAs and FIs' supervisors) was published in November 2017, and (b) the TF NRA was published in March 2018 (more information in IO.1 and R.1). Israel's FIU (IMPA) led and co-ordinated the ML and TF risk assessments over a period of two years (May 2015 to March 2017) using a self-developed methodology. This methodology is sound and consistent with the FATF Guidance. Representatives from all law enforcement, intelligence community, supervisory authorities, and the private sector (e.g. financial institutions, diamond dealers, and the Israel Bar Association (IBA) were involved in the process

52. The process involved the setting-up of three thematic working groups - LEAs, Supervisory and TF - which reviewed and analysed information collected from relevant authorities by way of a questionnaire prepared by IMPA (and were further adjusted by each supervisor to its relevant supervised sector). The questionnaire aimed at collecting quantitative and qualitative data on ML and TF with the view to examining inherent and residual risks, mitigating measures and consequences. Source data considered included: typologies, legislative and regulatory gaps, enforcement measures (i.e. financial investigations and prosecutions), information received from the private sector, volume and content of reports received by IMPA (Cash Transaction Reports (CTRs)/Unusual Activity Reports (UARs)), information on the scope and volume of predicate criminality,

seizures and confiscation data, supervisory data, international co-operation statistics, and other relevant statistics such as the volume of financial activities (e.g. trading data) and of the cross border inflow/outflow.

53. Previously conducted inter-governmental risk assessments were also taken into account (e.g. MSBs, cash, alternative payment methods, corruption, gambling, etc.). The private sector played an important role by providing a significant amount of data on identified ML and TF sectorial risks, but also the type and nature of services provided and customers, as well as on mitigation measures taken. Working groups also considered self-assessments produced by certain DNFBPs (Israel Diamond Exchange, IBA and the Institute of Certified Public Accountants).

54. There appears to be a sound and consistent understanding of domestic ML/TF risks among competent authorities, including of what constitutes high (and higher), medium and low risk. The NRA concluded that for ML – fraud (i.e. fictitious invoices), tax offences and organised crime are the three main proceeds generating crimes and thus pose the greatest ML threat to Israel. Public sector corruption is recognised as an ongoing issue, and has been identified as a moderate-high ML threat in the NRA. For TF, the NRA concluded that most TF activities in Israel involve financial support through donations to foundations or misappropriation of NPOs' funds, as well funding from other jurisdictions. The assessment team broadly agrees with the findings of the ML and TF NRAs.

55. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by Israel on their national ML/TF risks (as outlined above), and information from third-party sources (e.g. reports of other international organisations). The assessors focused on the following priority issues:

a) ML Investigations and Prosecutions, including how effectively all the various units and task forces (e.g. "*Lahav 433*", ML task forces, the Fusion Centre, the Signal Intelligence Squad, and the Financial Intelligence Analysis Squad) co-ordinate their actions when investigating ML, from a strategic and tactical point of view.

b) Cross-border movements of cash and value, including how Israeli authorities prevent incoming and outgoing illicit flows in the form of cross-border cash movements or through cash couriers, MVTS operators or possible *hawala* or similar service providers.

c) Terrorist financing, including the mechanisms Israel has put in place to tackle this threat and obtain numerous TF convictions, including the co-ordination involved in identifying and targeting terrorist financing, TF channels and source funding, and the ongoing CFT strategies Israel applies.

d) Financial sector supervision, including how the various Israeli authorities ensure consistent and effective application of risk-based AML/CFT supervision and enforcement measures, and the progress made in supervising the MSB sector which is considered high-risk in the NRA.[3]

3. P.26 of Israel's AML NRA Report (unrestricted version).

1

e) DNFBPs, including how the DNFBP sectors may have been misused for ML/TF purposes, and in response, measures undertaken by Israeli authorities in mitigating such risks since some DNFBPs (real estate agents, dealers in precious metals, and TCSPs) are not covered under the AML/CFT framework[4] while others (lawyers, accountants and dealers in precious stones) were recently incorporated in the AML/CFT regime.

f) Real estate sector: The use of real estate transactions was rated as moderate-high risk in Israel's NRA, especially with regard to cash transactions. As no AML/CFT supervision is in place for real estate agents the team seeks to gain a better understanding of the sector and the role of financial institutions and lawyers (designated as "business service providers") in property transactions.

g) Dealers in Precious Metals and Stones: Trading of diamonds has been identified as moderate-high risk in the NRA. In view of the significance of such trade and the identified ML/TF vulnerabilities of the trade, the assessment team sought to understand the size of the sector, volume, and pattern of transactions, ML/TF cases related to the sector, and how Israel is applying risk-based AML/CFT supervision and other controls in this sector.

Materiality

56. The Israeli economy is mainly based on services (77.9% of value-added shares), followed by industry (20.8%) and agriculture (1.3%).[5] Financial services (widely defined to include real estate, accounting, and architecture) contribute to roughly 25% of the services sector. Israel does not serve as a global or regional financial centre. It is also not a major exporter and importer of financial services. There is low foreign participation in the financial sector, which is highly concentrated in the banking system, with their assets amounting to about 140% of the GDP.[6] Within the banking sector, a total of 96% of the assets are concentrated in five major domestic banking groups. The Israeli government has recently sought to lessen the domination of banks over financial intermediation and increase competition in the financial market.[7] Consequently, non-bank services in the capital markets, credit card businesses, and money services business have been on the rise.

57. Regarding DNFBPs, with the exception of casinos and notaries, all other DNFBPs undertake the activities listed in the FATF Recommendations. Among

4. According to input provided by Israel, notaries and other independent legal professionals are not involved in the transactions covered under the FATF methodology.
5. OECD Economic Surveys (Israel, March 2018): http://www.oecd-ilibrary.org/docserver/eco_surveys-isr-2018-en.pdf?expires=1528457445&id=id&accname=ocid84004878&checksum=F1CEBF69553ADC29355FC77F7A8137D1
6. www.imf.org/en/Publications/CR/Issues/2016/12/31/Israel-Detailed-Assessment-of-Observance-of-Basel-Core-Principles-for-Effective-Banking-25844
7. OECD Review of the Financial System (Israel): http://www.oecd.org/finance/financial-markets/49497958.pdf

them, diamond-related trade and real estate transactions have the highest number of activities in terms of GDP. The estimated added value of the diamond sector is close to NIS 2.2 billion (EUR 514 million) – 0.2% of GDP, 13% of total exports as of 2017. The Israel Diamond Exchange is a prominent global trading centre, one of the largest diamond exchanges in the world. Notaries in Israel do not engage in the activities covered by the FATF Standards and casinos are illegal in the country (see DNFBP section below for details). The legal profession is very large – Israel has a high per capita number of lawyers.

Structural Elements

58. Israel has all of the key structural elements required for an effective AML/CFT system including political stability, governmental accountability, rule of law and an independent judiciary.

59. Israel's institutional structure provides the necessary framework to implement its AML/CFT regime. This institutional framework is centred on the Executive Steering Committee (ESC), which acts as the national AML strategy, policy development and co-ordination authority. See section below for a full overview of the institutional framework.

Background and Other Contextual Factors

60. There is a high-level political commitment and strong judicial system in place to tackle domestic corruption. Public sector corruption is recognised as an ongoing issue, and has been identified as a moderate-high ML threat in the NRA.

61. The prevention and countering of corruption has been given high priority at the national level. Israel conducted a detailed risk assessment on corruption in 2015, following the identification of repeated corruption activities occurring in municipal authorities. Israel has also been proactive in identifying and investigating potential corruption cases, including several involving high profile senior government officials. Corruption investigations proceed without political influence.

62. Israel is also member to a number of international instruments, such as the UN Convention against Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. In the *2017 Basel AML Index Report* of August 2017, Israel is ranked 137 out of 146 countries in the level of AML risks, and rated third in the list of top ten improvers.[8]

63. Israel's independent judicial system guarantees access to all citizens. As such any individual can directly make a petition to the Israeli Supreme Court – which is quite a unique feature, and also puts a considerable burden on its judges. Judicial authorities indicated that approximately 10 000 proceedings (which include all kinds of proceedings - civil, administrative, constitutional and criminal) were filed each year to the Supreme Court.

64. Israel high-tech industry is one of the most developed in the world, with a large number of research and development centres working on outsourced

8. Pages 5, 8, 9 – 2017 Basel AML Index Report (August 2017).

1

software development, product design and hardware. Expenditure on the civilian R&D amounted to about 4.3% of GDP in 2016, one of the highest ratios in the world.[9]

AML/CFT strategy

65. In 2006, the government set the targeting of illicit proceeds as a primary objective in the combat against serious and organised crime. As a result, *Government Decision no. 4618 (2006)* was issued requiring all relevant agencies to co-operate, and implement their activities on the basis of work plan adopted at the highest level by the *Executive Steering Committee* (ESC). The ESC outlines the country's integrated AML strategy and policy to counter serious and organised crime (including the targeting of its proceeds). The ESC annually approves the work plan for all relevant agencies and defines priorities for implementation (see section below and IO.1).

66. To effectively combat ML and TF, the ESC follows these six principles: setting goals and co-ordinating policies; sharing of information and expertise between law enforcement authorities; proactively initiating activities (including proactive intelligence development, and the improvement of technological means to so do); integrating activities through operational co-operation; systematically making efforts to fight ML in new ways, combining available tools and sanctions (i.e. civil and supervisory procedures); and developing best practices, removing barriers and "bottlenecks" (e.g. initiation of legislation amendments) and improving operations through the sharing of operational experience and lessons learnt.

67. In relation to TF matters, the Ministerial Committee on National Security Affairs (Security Cabinet) Resolution No. 86/B (January 2003) established a dedicated CFT Committee. The activities of this committee were recently transferred to the National Bureau for Counter Terror Financing (NBCTF). The Bureau, housed within the Ministry of Defence (MoD), is a combined inter-ministerial effort against terrorist financing, and is responsible for outlining the national enforcement policy and co-ordinating national CFT strategies and enforcement policies. Its areas of authority also include conducting CFT risk assessments and the combating of PF.

68. The Sanctions Bureau under the Ministry of Finance (MoF) co-ordinates PF strategy and all efforts relating to proliferation and PF sanctions.

Legal & institutional framework

69. The Prohibition on Money Laundering Law (PMLL) enacted in 2000 is the country's AML legislation. Since Israel's evaluation by MONEYVAL (in 2008 and 2013), the PMLL was amended in 2016, notably to add tax offences to the list of predicate offences to ML, as set forth in the Schedule of the Law. In February 2017, the definition of "beneficial ownership" was amended to align it with the FATF Standards. Another amendment was made in December 2017, which included, *inter alia*, changes to the ML offences, establishing IMPA's authority to disseminate

9. UNESCO Science Report: towards 2030 (2015) - http://unesdoc.unesco.org/images/0023/002354/235406e.pdf, P.409-429.

information to additional LEAs and the supervisors, lowering the threshold for cross-border reporting, amendment to the definition of BO, and others. Since 2015, AML/CFT obligations apply to dealers in precious stones (which includes a reporting obligation to IMPA as of September 2016) and to lawyers and accountants for their activity in providing business services to their customers. A number of laws and Orders were enacted regarding the regulation and supervision of FIs and DNFBPs (e.g. 2016 Law for the Supervision of Financial Services Businesses). Israel also has a new Counter Terrorism Law (CTL), which came into force in November 2016. During the time of the on-site visit in March 2018, a law for the reduction of the use of cash was passed.[10]

70. Israel's institutional framework for AML/CFT encompasses the following institutions:

Ministries and Co-ordinating Bodies

a) The *National Security Council* (NSC) co-ordinates the different security and governmental authorities involved in state security. The NSC was established in 1999 in accordance with a government decision and its activity was institutionalised by the National Security Council Law, 2008.

b) The *Executive Steering Committee* (ESC) is the national AML strategy, policy development and co-ordination authority. It is comprised of the Attorney General, the State Attorneys, the heads of Israeli's main LEAs – namely the Inspector General of Police (INP), the Head of the Israel Tax Authority (ITA), and the Chairman of the Israel Securities Authority (ISA). The ESC is in charge of outlining the country's integrated policy to combat serious organised crime, approving work plans, and defining priority actions based on agreed goals. The ESC reports periodically to the Government on these objectives.

c) The Inter-Agency *Implementation Committee* (IC) is the main operational body that implements ESC's policies and directives into operational mechanisms. As such, the IC was one of the leading authorities in charge of the NRA project. The IC comprises Israel's key AML/CFT agencies, including law enforcement authorities (INP, ITA, ISA), the financial intelligence unit (IMPA), Israeli Prison Service, Bank of Israel, Ministry of Economy and Industry, and Ministry of Justice.

d) *Ministry of Justice* (MoJ) is in charge of public prosecutions, legislation and counselling (including amendments to AML/CFT legislation and regulations). MoJ houses the country's financial intelligence unit (IMPA) and the Israel Corporation Authority (ICA), which is in charge of the registration and supervision of companies, partnerships, public endowments (including trusts) and NPOs. Its Department for International Affairs is also the central authority for outgoing international co-operation (MLA/extradition). Since 2015, its Supervisory Unit for Business Service Providers (BSPs) has also been supervising the conduct of accountants and lawyers providing business services under the AML/CFT framework (including conducting inspections and imposing administrative fines). The

10. This law is due to come into force on 1 January 2019.

MoJ also houses the Council of Certified Accountants which is in charge of licensing of accountants and their ethical proceedings.

e) *Ministry of Finance* (MoF) is responsible for determining the fiscal and economic policy in Israel, managing state revenues, and collecting taxes. It houses the Capital Market, Insurance and Savings Authority (CMISA), the Israel Tax Authority (ITA), and the Israel Securities Authority (ISA). MoF's *Sanctions Bureau* co-ordinates counter-proliferation finance targeted financial sanctions. The Sanctions Bureau co-ordinates designations, serves as the national information centre regarding all aspects of sanctions, and serves as an investigative body regarding sanctions.

f) *Ministry of Internal Security* is in charge of maintaining law and order in Israel. The Ministry oversees the Israel National Police (INP).

g) *Ministry of Foreign Affairs* (MFA) is responsible for the ratification of international agreements. It also houses the *Sanctions Headquarters*, which is responsible for the implementation of the United Nations Security Council Resolutions.

h) *Ministry of Economy and Industry* (MoE) is responsible for promoting trade and international commerce, initiating and enforcing trade restrictions, as well as overseeing the Diamonds, Gemstones and Jewellery Administration which is the AML/CFT supervisor regarding dealers in precious stones in Israel.

i) *Ministry of Defence* (MoD) oversees the *National Bureau for Counter Terror Financing (NBCTF)*, which co-ordinates terrorist financing targeted financial sanctions. The bureau, which was recently moved from the NSC, is a combined inter-ministerial effort against terrorist financing.

j) *Ministry of Communications* (MoC) oversees the Postal Bank and is the designated AML/CFT supervisor of all financial businesses of the Postal Bank (including all local branches).

Criminal Justice and Operational Agencies

a) *Israel Money Laundering and Terror Financing Prohibition Authority* (IMPA), housed within the Ministry of Justice, is Israel's FIU. IMPA is an administrative FIU and assists the Israeli LEAs, security agencies and the supervisors of the private sector in performing their duties according to the Israeli AML/CFT regime.

b) *Israel National Police* (INP) is the national force with territorial districts (Jerusalem, Northern, Shore, Central, Southern and Tel Aviv). It is the only police force in Israel and has the primary responsibility for formal ML and TF investigations. "*Lahav 433*" was established under the Investigation and Intelligence Department and targets serious crime and corruption, on the international, state and the district levels. INP also houses the Intelligence Fusion Centre (IFC) (see below). This unit also houses eight multi-agency task forces. Within INP, the Legal Assistance Unit is the central police authority for incoming MLA and police requests for international co-operation.

c) The *Intelligence Fusion Centre* (IFC) is a joint intelligence body established following the 2006 Government Decision no. 4618 on Countering Serious and Organised Crime and their proceeds (*Decision 4618*), comprised of permanent members from INP, ITA, and IMPA.

d) The *State Attorney*, subordinate to the Attorney General, heads the Prosecution Authority, operates as a separate organisational unit under the Ministry of Justice. The State Attorney's Office (SAO) leads prosecutions for ML, TF, and other offences. The Prosecution Authority operates through nine departments at the State level and 11 district offices.

e) *Shin-Bet* is the national organisation responsible for the defence of the state of Israel and its institutions against the terror threats, espionage, political subversion, and the exposure of state secrets. The agency leads on terrorism and TF intelligence, and conducts CFT investigations and enforcement activities.

f) *Israel Tax Authority* (ITA) is composed of Income Tax, Land Tax, Customs and VAT Authorities. ITA's investigative units, as well as "*Yahalom*" unit are in charge of, inter alia, investigating ML offences connected to the tax offences. ITA also has a key role in supervising the cross-border reporting obligations.

Financial Sector Supervisors

a) *Bank of Israel* (BoI) is the central bank and is the designated authority for both prudential as well as AML/CFT regulation and supervision through its Banking Supervision Department.

b) *Israel Securities Authority* (ISA) is responsible for the prudential and AML/CFT supervision of securities-related services provided by portfolio managers and trading platforms, but only AML/CFT supervision of stock exchange members.

c) *Ministry of Communications* (MoC) is responsible for AML/CFT supervision of the Postal Bank (see above).

d) *Capital Market, Insurance, and Savings Authority* (CMISA), an independent authority established in November 2016, it is the AML/CFT supervisor for the sectors of insurance, pension funds, provident funds, money service business (including MVTS providers and money changers), and non-bank lending and credit services providers (as of June 2017).

DNFBP Sector Supervisors and Self-Regulatory Bodies

a) *Diamonds, Gemstones and Jewellery Administration*, a unit within the MoE, is responsible for the supervision of dealers in diamonds and precious stones in Israel. It is also responsible for operating the licensing regime in relation to diamond dealers.

b) The *Supervisory Unit for Business Service Providers* (BSPs) in the MoJ is the AML/CFT supervisor of lawyers and accountants.

c) The *Israel Bar Association* is a self-regulatory body responsible for the licensing of lawyers. It administers examinations for those who want to practise law in Israel. It is also responsible for imposing disciplinary measures against lawyers in the country (including regarding AML/CFT disciplinary violations).

d) The *Council of Certified Public Accountants*, housed within the MoJ, is responsible for the licensing of accountants. It is also responsible for imposing disciplinary measures against accountants (including AML/CFT disciplinary violations).

Financial sector and DNFBPs

71. In this assessment, the most important weighting has been given to the banking and MSB sectors, followed by diamond trading and securities sectors, given their respective size (including number of practitioners and customers, as well as value and volume of transactions), customer profile, as well as the level of ML/TF risks which they are exposed to and types of ML/TF mitigation measures applicable.

72. The financial sector in Israel is highly concentrated in the banking sector, with their assets amount to about 140% of the GDP, followed by the securities sector (112% of GDP) and the insurance sector (93% of GDP).

73. Within the banking sector, a total of 96% of the assets are concentrated in five major domestic banking groups. There are also representative offices of 12 foreign banks, but these cannot provide credit or accept deposits.

74. Similar to the banking sector, insurance services and pension and provident funds are concentrated in a few large domestic groups. Israel also has a significant securities-related industry and has a total of NIS 1 trillion (EUR 234 billion) of total assets under administration in the life insurance pension and provident funds market. As of March 2018, the Tel Aviv Stock Exchange (TASE) is home to over 453 listed companies, with a total market value of approximately USD 204 billion, 692 corporate bonds, and 714 ETFs.[11] The bulk of the trade volume is traded through banks that are members of the Exchange (stocks 76.4%; bonds 86.9%; and derivatives 88.2%) and the rest through non-bank Stock Exchange Members stocks 23.6%; bonds 13.1%; and derivatives 11.8%). Other non-bank financial institutions include Money Services Businesses, which provide credit, lending or credit card services to retail and corporate clients, wire transfers. An overview of the financial institutions in Israel can be found in the table 1 below.

11. www.tase.co.il/Eng/Statistics/StatRes/Corporate_Fact_Sheet/Stat_124_Corporate_FactSheet_2018_05.pdf

Table 1. **Financial Institutions in Israel by size**

Financial Institutions	Number (as of 2017)	Size/assets
Banking Corporations	20	NIS 1.56 trillion (EUR 365 billion)
• **Commercial banks**	12	
• **Branches of foreign banks**	4	
• **Acquirers**	4	
Joint Services Companies	2	
Postal Bank	1 (with some 650 local branches)	NIS 3.88 million (EUR 907 000)
Insurance companies	25 (with 11 of them handling life insurance)	NIS 1.06 trillion (EUR 248 million)
Insurance intermediaries	1 351	
Portfolio managers	125	
Pension funds	37	
Provident fund managers	84	
Money Service Businesses and Non-bank Credit Service Providers	1 689	NIS 150 billion (EUR 35 billion)
Non-bank Stock Exchange members	6	NIS 337.2 million (EUR 78.9 million)
Trading platforms	6	
Portfolio managers	126	

Note 1: Regarding asset size of the insurance sector, it includes total assets of the public in life insurance, pension, and the provident funds market.
Note 2: Regarding asset size of securities sector, the daily turnover (in shares and convertibles) includes all Stock Exchange Activity (including banking corporations conducting this activity).
Source: BoI, CMISA, ISA and MoC

Table 2**. Financial Institutions in Israel according to the FATF Definition**

Type of financial activities or operations under the FATF Definition	Types of financial institutions in Israel[12]	AML/CFT Supervisor(s)
1. Acceptance of deposits and other repayable funds from the public	Commercial Banks[13]	BoI
	Postal Bank	MoC
2. Lending	Commercial Banks[14]	BoI
	Credit Service Providers (non-bank)	CMISA
3. Financial leasing	Commercial Banks[15]	BoI
	Credit Service Providers (non-bank)	CMISA
4. Money or value transfer services	Commercial Banks (including branches of foreign banks)	BoI
	Postal Bank	MoC
	Stock Exchange Members	ISA

12. While listed as FI in Israel, joint-service companies and acquirers cannot accept deposits.
13. Foreign banks branches can accept deposit.
14. Foreign banks branches and acquirers can also provide credit.
15. Foreign branches and credit card may also operate as well.

Type of financial activities or operations under the FATF Definition	Types of financial institutions in Israel[12]	AML/CFT Supervisor(s)
	Money Service Business	CMISA
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Commercial Banks[16]	BoI
	Credit card companies	BoI
	Postal Bank	MoC
6. Financial guarantees and commitments	Commercial Banks (including braches of foreign banks)	BoI
7. Trading in: **(a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);** **(b) foreign exchange;** **(c) exchange, interest rate and index instruments;** **(d) transferable securities;** **(e) commodity futures trading**	Commercial Banks (including branches of foreign banks)	BoI
	Stock Exchange Members	ISA
	Trading Platforms	ISA
8. Participation in securities issues and the provision of financial services related to such issues	Commercial Banks (including branches of foreign banks)[17]	BoI
	Portfolio Managers	ISA
9. Individual and collective portfolio management	Commercial Banks (including branches of foreign banks)	BoI
	Portfolio Managers	ISA
Safekeeping and administration of cash or liquid securities on behalf of other persons	Commercial Banks (including branches of foreign banks)	BoI
10. Otherwise investing, administering or managing funds or money on behalf of other persons.	Commercial Banks (including branches of foreign banks)	BoI
	Pension Funds	CMISA
	Insurance Companies	CMISA
	Insurance Agents	CMISA
11. Underwriting and placement of life insurance and other investment related insurance.	Insurance Companies	CMISA
	Insurance Agents	CMISA
12. Money and currency changing	Commercial Banks (including branches of foreign banks)	BoI

16. This does not include foreign banks branches.
17. These activities are only allowed by an auxiliary corporation (i.e. subsidiary of a bank). Same applies to item 9, 11, and 12. For item 12: only auxiliary corporation may operate as insurance agents to offer only life or home insurance carried out incidentally to providing housing loans by the parent commercial banks.

Type of financial activities or operations under the FATF Definition	Types of financial institutions in Israel[12]	AML/CFT Supervisor(s)
	Postal Bank	MoC
	Money Service Providers	CMISA

Source: BoI, CMISA, ISA and MoC

75. As for DNFBPs, with the exception of casinos and notaries,[18] the full range of DNFBP sectors exists within the country and undertakes the activities contemplated by the FATF Recommendations. Among the covered DNFBPs, the diamond industry is most significant. In 2017, export of rough diamonds (net) totalled NIS 8.665 billion (EUR 580 million) and polished diamond (net) totalled NIS 16.175 billion (EUR 3.5 billion).[19] The diamond trade represents roughly 0.2% of the GDP. The legal profession is also very large – Israel has a high per capita number of lawyers. However, it is not known how many lawyers and accountants engage in the activities covered by the FATF Recommendations. See below for number of DNFBPs.

Table 3**. DNFBPs in Israel**

Type of DNFBPs	Number of DNFBPs	AML/CFT Supervisor
Casinos	Not applicable	No AML/CFT supervisor has been assigned as casinos are illegal in Israel.
Real Estate Agents	17 500	No AML/CFT supervisor has been assigned as the real estate sector is not covered in the Israeli AML/CFT framework (but the Realtors Registrar of the MoJ administers licensing examination for real estate agents).
Dealers in Precious Metals	No available data	No AML/CFT supervisor has been assigned for dealers in precious metals as they are not covered in the AML/CFT framework.
Dealers in Precious Stones	2 623	MoE
- diamond dealers	2 302	
- other precious stones dealers	321	
Lawyers (including notaries)	77 553 (of which 68 217 are active)	MoJ/Israel Bar Association
Accountants (including auditors)	18 472	MoJ/Israeli Accountants Council
TCSPs	2	No AML/CFT supervisor has been assigned.

Source: MoE and MoJ.

Preventive measures

76. The PMLL is the primary legal instrument setting out the preventive measures (including customers due diligence, reporting, and record-keeping)

18. Casinos are illegal in Israel and hence are not considered in this report. As notaries do not carry out the activities of FATF R.22 in Israel, they are therefore not considered in this report.
19. http://economy.gov.il/publications/publications/doclib/diamondsreport2015.pdf

which applies to the eight covered financial and three DNFBP sectors in Israel. It includes empowering provisions, allowing individual financial and DNFBP supervisors to enact enforceable sectoral rules for specifying the detailed operational requirements of these preventive measures. The range of instruments includes regulations, orders, directives and circulars. In addition, where applicable, Israel relies on general sectoral-specific supervisory power provided under respective laws to implement AML/CFT preventive measures. The regime covers all financial institutions required by the FATF. For DNFBPs, real estate agents, dealers in precious metals and trust and company service providers do not have AML/CFT obligations. Lawyers and accountants are subject to licensing requirements and have some AML/CFT obligations, but are not required to report suspicious transactions. Real estate agents are subject to a market entry licensing regime and have been briefly considered in the national/thematic risk assessments. Dealers in precious stones are covered under Israel's AML/CFT system but only diamond dealers are subject to a market entry licensing regime. Casinos are illegal in Israel.

Legal persons and arrangements

77. Israeli law allows the creation of a range of different types of legal persons and arrangements, but does not provide for the establishment of a foundation and does not recognise the concept of a foundation. For legal persons and arrangements, they are required to be registered with the Israel Corporation Authority (ICA) (including Registrar of Companies, Registrar of Partnership, Registrar of Public Trusts, or Registrar of Associations and the Israel Tax Authority (ITA). Below is a table outlining the features and the number of registered legal persons and arrangements in Israel.

Table 4. **Number of Legal Persons and Arrangements**

Type of Legal Persons /Arrangements	Features of Legal Persons/Arrangements	Number of Registered Entities
Companies	The Israeli Companies Law provides the mechanism for setting up companies in Israel	363 470
Reporting Companies	Public company shares are listed for trading on stock exchange (TASE) or have been offered to the public pursuant to a prospectus as defined in the Securities Law.	570
Private Companies	Since 2016, private companies are not allowed to issue bearer shares. Nominee shareholders of private companies are treated as trustees in Israel (see item on trusts below).	360 000
Foreign Companies	Foreign companies are required to be registered in the same way as domestic companies.	2 900
Partnerships	The Partnership Ordinance provides the mechanism for setting up partnerships	9 000
General Partnership	General Partnership is a partnership where all of the partners are liable for the obligations of the partnership, jointly and severally.	45 057
Limited Partnership	Limited partnership is one where a person who brought capital into the partnership, at the time of the engagement, in money or in an asset valued at an express amount, in order to not be liable for the obligations of the partnership in excess of the amount provided.	3 431
Foreign Partnership	Foreign partnerships are those partnerships established outside of Israel.	360
Trusts		
Public Trusts (Charities) – listed in the ICA	The Trust Law governs the establishment of trusts in Israel. Trusts are a type of non-corporate entity and are not a separate legal entity in Israel. Trusts include all arrangements in which a trustee hold assets for a beneficiary, in Israel or in a foreign country. Public trusts are similar to charitable trusts and private trusts are relationships to any property by virtue of which a trustee is bound to hold the property, or act in respect thereof, in the interest of a beneficiary or for some other purpose. Though foreign trusts are not mentioned under the Trust Law, Israeli law does not prohibit a resident from acting as a trustee or trust administrator for a foreign trust. Foreign trusts, however, are captured under the Income Tax Ordinance for taxation purposes. Under the Income Tax Ordinance, Israeli resident trusts, foreign resident trusts, Israeli resident beneficiary trusts (including family trusts, foreign resident beneficiary trusts, and testamentary trust) are provided for.	3 200
Private Trusts		-
Israeli Residents trusts		2 371
Foreign resident settlors trusts		82
Foreign resident beneficial owners trusts		54
Israeli will trusts		58
Foreign will trusts		2
Israeli resident beneficial owners trusts		33
Family relatives trusts		71
foreign resident trusts		31
Associations		
Public associations (thereafter referred as "*Amutot*")	The Associations Law lays down the framework for establishing associations. Association is defined as an entity created by two or more persons who wish to incorporate as a body corporate for a lawful purpose not aimed at the distribution of profits to its members.	40 000
Charitable Companies		1 200

Source: ICA and ITA

1

Supervisory arrangements

78. The Israeli financial sector is supervised by three supervisors, whose tasks include AML/CFT supervision. The supervisors are the Bank of Israel (BoI) for banks, credit cards, and payment systems, the Israel Securities Authority (ISA) for the securities sector (covering the activities at the TASE, stock exchange members, portfolio managers and trading platforms), and the Capital Markets, Insurance and Savings Authority (CMISA) for the insurance, pension funds, credit service providers, and more recently the MSB sectors. Banks are often engaged in a spectrum of activities and operations under the FATF definition of "financial institution", all such supervision falls within the ambit of the BoI.

79. For the covered DNFBPs, MoE supervises dealers in precious stones while MoJ supervises lawyers and accountants providing business services (defined in the law as those activities covered in the FATF Recommendations). In addition, self-regulatory body of Israel Bar Association is responsible for administering examinations for registration to lawyers.

80. For legal persons, ICA handles the registration and oversees the requirement of filing of annual financial statements. However, ICA is not required to verify the information submitted.

International co-operation

81. Israel is not considered as a significant regional or international financial centre. However, the risk assessment confirmed that criminals often rely on offshore shell companies and other legal arrangements to disrupt the tracing and identification of beneficial ownership. Proceeds are generated annually by criminal activities abroad, including fraud. Criminal groups operating in Israel are national or with connections in Europe, US, and the former Soviet Union. Israel also faces a high terrorist financing threat from funds and assets from abroad. Thus, Israel relies extensively on international co-operation in order to collect the information held abroad, including for the identification of assets located outside Israel, for the purposes of investigating and prosecuting ML/TF cases, and repatriating the evaded proceeds of crime.

82. Israel has a solid legal framework and well developed system for the provision of international co-operation for ML and TF matters. While there is no unique central authority for MLA (see R.37), all competent authorities co-operate with each other domestically and with their foreign counterparts. This is evidenced by the number of successful ML and TF investigations and prosecutions, which involved numerous exchanges of information at the international level, joint investigations and other forms of operational co-operation and co-ordination. The most significant international partners include the US, Canada, and Europe.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key Findings

Israel has achieved a substantial level of effectiveness for IO.1.

a) Israel has prepared a NRA which addresses ML and TF risks; all of the authorities have contributed to the process.
b) Overall, Israel has a good understanding of its ML risks. Israel's major ML risks are mostly identified and assessed, although there is need for a more comprehensive approach to risk assessment in a limited number of areas (legal persons and legal arrangements, and NPOs).
c) The understanding of TF risks (with the exception of NPOs, to some extent, within the country) is generally very good. Israel's major TF risks have been identified and assessed.
d) The Israeli authorities have implemented a number of measures to ensure FIs and DNFBPs are aware of the relevant results of the national ML/TF risk assessments, although such understanding amongst DNFBPs is weaker when compared to FIs.
e) The exemption from some AML/CFT obligations in respect of a range of DNFBPs is not fully supported by the depth of understanding and goes beyond the FATF Standards.
f) The authorities have developed co-ordinated action plans to address identified ML/TF risks, and have implemented a significant number of the priority actions – such as legislation on TF targeted financial sanctions, on the use of cash, and on reduced threshold for disclosure of cash at borders, and the establishment of two new task forces on TF and MSBs. Co-ordination of risk based supervision is at a relatively early stage.
g) The degree to which financial supervisors follow a full risk-based approach to supervision for better alignment with the evolving national AML/CFT policies and with the ML/TF risks identified varies. DNFBP supervisors/SRBs are still at an early stage of planning supervisory activities according to the ML/TF risks identified in the NRA processes.
h) The targeting of illicit proceeds is embodied in a Government Decision dating back to 2006. Israel has strong, national AML/CFT co-ordination and includes all relevant competent authorities. Israeli domestic co-ordination is driven by the Executive Steering Committee, its Implementation Committee, and sub-committees of the latter committee, which together comprise the country's main AML/CFT policy development tool.
i) Bilateral and multilateral AML/CFT co-operation at the operational level is strong, particularly among the Israel Money Laundering and Terror

Financing Prohibition Authority (IMPA), the *Shin-Bet*, the Israel National Police (INP) and the Israel Tax Authority (ITA), and also between the Israel Companies Authority (ICA) and the ITA.

j) Co-ordination of policy and operational activity in connection with combating proliferation financing (PF) is comprehensive, but has been less utilised with regard to the Democratic People's Republic of Korea (DPRK).

k) Strong efforts have been made to provide the public versions of the NRA material and information on risks to reporting entities, but the public versions are too simplified.

Recommended Actions

Israel should:

a) Conduct a more in-depth analysis of the ML/TF risks presented by NPOs and legal persons and arrangements.

b) Provide more detailed NRA material to FIs, DNFBPs, and NPOs; and make clear the reasons for different risk ratings of the same subject considered in the different public reports seen by the third parties.

c) Enhance co-ordination of risk-based supervision of FIs and DNFBPs, and PF co-ordination regarding DPRK.

83. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

Immediate Outcome 1 (Risk, Policy and Co-ordination)

Country's understanding of its ML/TF risks

84. Israel has engaged in very significant effort to identify, assess, and understand ML/TF risks.

85. After a two-year project led by IMPA, involving all AML/CFT authorities, a series of classified reports under the umbrella of the NRA were finalised in March 2017. Israel has issued a ML risk assessment report, a TF risk assessment report, and a joint supervisory risk assessment report on ML risks faced by individual financial sectors. Separately, Israel has issued public versions of each of these reports. The contents of the three classified reports were discussed but not seen by the assessment team, except for extracts in relation to legal persons, legal arrangements, and NPOs. Notably, the assessment material considers all three elements of risk, namely threat, vulnerability, and consequence. In general, the depth of the process is at the top end of the NRA processes which have been undertaken internationally.

86. Israel has demonstrated that ML risks are mostly understood. This is evident from the NRA and discussions with the authorities on-site. The NRA also built on existing thematic risk assessments, including use of tax offences (2003); serious and organised crime (2004); cash (2014); MSBs (2015); corruption (2016); gambling (2016); alternative payment methods (2017); and the INP's

annual intelligence assessments. Private sector entities, including all licensed entities, participated in the NRA. As the ML/TF risks facing Israel are complex and multi-faceted, the NRA enabled Israel not only to consolidate and articulate existing knowledge, but also to develop its understanding in various areas, including fraud, real estate, and legal arrangements in particular. With regard to predicate offences, the key threats and risks of ML are seen by Israel as arising from tax evasion, criminal organisations, fictitious invoices, drug trafficking, gambling and fraud (other than fictitious invoices) – these are consistent with the key threats and risks faced by the country. Organised Criminal Groups (OCGs) are considered comprehensively. They are involved in a wide range of criminal activities, including all of those which Israel sees as having a higher threat and risk. Knowledge and understanding of organised crime increased significantly in 2016 (see IO.7).

87. In terms of Israel's assessment of typologies, methods and instrumentalities, the highest risks are considered to be money services businesses (MSBs) and the use of cash (both high threat and high risk), followed by international/cross-border crime (considered separately in the assessment in light of its importance), diamond trading, real estate, legal persons and arrangements, and NPOs (all moderate-high threat and risk). These findings are commensurate with the key risks faced by the country. The ML risks relating to the shadow economy have been assessed to an adequate extent.

88. The NRA process included consideration of trade based ML. This included international typologies and patterns of data within Israel, including customs data. The authorities also advised that Israel is not a major trading entrepot, has very few ports and that the port authorities have a high degree of security awareness. While agreeing with the overall thrust of the assessment, the assessment team considers that there would be merit in some refinement of it.

89. Israel's risk rating for diamond trading is moderate-high; this is appropriate. On the other hand, gold trading is rated as medium-low. While the Israeli authorities demonstrated understanding of the sector and of the differing risks as compared with diamond trading and were aware of the mitigation measures in place and recent operational focus there is a need to review the risk rating as far as ML is concerned. The authorities recognised this need.

90. There is a separate assessment of the risks of legal persons and legal arrangements, and those businesses that provide services to them. The risk rating of legal persons and legal arrangements was assessed as medium-high largely on the basis that the authorities understood that they possessed insufficient information and that further analysis needed to be undertaken. While the risks of such persons and arrangements and service providers to them (e.g. TCSPs) are not comprehensively understood, a number of cases which have developed since the NRA was completed have clearly improved understanding. As indicated in the NRA action plan, Israel proposes to undertake a fuller analysis of the risks in relation to legal persons and legal arrangements. There would be merit in splitting the risk profiles of lawyers and accountants (currently the rating is combined) to facilitate understanding by the private sector.

91. The separate ML risk assessment of NPO has considered the risks but is not comprehensive. As reflected in the NRA plan, the authorities recognise that there

was insufficient information available on the scale of ML through NPOs and intend to revisit the assessment by taking an in-depth view of the sector in more detail.

92. The financial system report concludes in some cases that individual sectors have different risk levels to those specified in the public report for the whole NRA. Sectoral risks are seen as being different to the overall risks for the financial system. The differences were explained and satisfactorily justified by the Israeli authorities on the basis of the assessment undertaken and by the fact that that the risks of individual sectors can and do differ from national risks. The BoI and the ISA were confident in explaining their approaches to risk and the information from reporting entities and other sources on which it is based. The authorities have advised that there was substantial outreach to the private sector to articulate the reasons for the differences and the reasons for them. Nevertheless, the overall approach is not clear and the narrative in the published NRA material is high level.

93. The NRA addresses the risk of trust accounts, which comprise a combination of customer accounts held by legal professionals and accounts held in relation to express and other trusts. The assessment would benefit from more in-depth scrutiny. There would also be merit in separating the two types of account and extending the analysis, particularly bearing in mind that Israel permits numerous types of trust to be established.

94. Due to its geographic location and its historical and political circumstances, Israel has experienced a high threat of terrorism and, as a consequence, a high threat of TF. Generally, the understanding of TF risks is very good. The public NRA report specifies and describes a number of risks. These include risks arising from jurisdictions, donations from the general public or wealthy individuals and NPOs (see paragraphs immediately below), financing of terrorist organisations by supposedly legitimate business operations, and criminal activities. The transfer of funds to terrorist organisations is mainly carried out by the smuggling of property across the borders (including by trading) and money transfer mechanisms which include correspondent activity, currency service providers, pre-paid cards and foreign credit cards.

95. The TF NRA was intelligence oriented and involved mapping exercises. As indicated in IO.9 and IO.10, the Israeli authorities have had significant success in combating TF. This success has provided significant information on TF risks to *Shin-Bet*, INP, IMPA, the Intelligence Fusion Centre, the CFT Bureau and the National Cargo Targeting Centre and other authorities, which appears to have been comprehensively mined and understood. In addition, questionnaires issued by supervisory authorities also covered TF. Most TF activities do not take place within the financial system or DNFBPs since terrorist networks avoid use of Israeli institutions in light of the levels of awareness and mitigation in place by FIs and disruption activities by the authorities.

96. Generally, Israeli NPOs are not seen by the authorities as presenting a significant TF risk (albeit certain parts of the sector assessed as presenting significantly higher risks). TF risk is considered to be concentrated in foreign NPOs active in Israel and in domestic NPOs with international activities. The NPO Registrar (the ICA) was not directly involved in the TF NRA process, although it was consulted. Looking more widely, the risk profile of NPOs has been assessed to a greater degree in the TF NRA process than for ML – although the next iteration

of the TF NRA would benefit from more direct and detailed input by the ICA. NPO risk has been mapped by considering the type of NPO, the source of its income, and the purposes and actual use of funds.

National policies to address identified ML/TF risks

97. Israel has a strong and longstanding political commitment to ensuring it has a robust AML/CFT framework. For example, the targeting of illicit proceeds as a primary objective in combating serious and organised criminal activity was established as a national objective in a Government Decision in 2006. National policies are also formulated and monitored by a series of committee structures. An Executive Steering Committee (ESC), comprised of the State Attorney General and the most senior representatives of LEAs (INP, ITA, and ISA), was established the same year to develop policies, approve multi-year and annual work plans, and define priorities. Since then, the Committee reports periodically to the committee of ministers on its progress and activities, as well as the progress and activities of the ESC's underlying structures referred to below.

98. The ESC has established an Inter-Agency Committee (IC), chaired by the Head of the IID of the INP, to implement the ESC's decisions by the co-ordination of operational actions by supervisory, intelligence, investigatory, prosecution and confiscation authorities and measure the success of those actions. The committee comprises representatives of LEAs, IMPA, the SAO and intelligence authorities. Representatives of other authorities such as the *Shin-Bet* and other security agencies join meetings as appropriate. The IC periodically develops an intelligence map, integrating information from IMPA, LEAs and others, to inform its strategic thinking. The committee meets every 60 days and, like the ESC, formulates multi-year and high priority annual action plans. It follows six principles, namely setting goals, initiating proactive activities and co-ordinating priorities; sharing of information and professional knowledge; proactive intelligence activity; integrating activities through operational co-operation; holistic and systematic combat; and the development of best practices.

99. The IC operates through five subcommittees, which deal with operational co-ordination, intelligence, legal issues, training and IT. These subcommittees meet approximately every two months, discussing issues such as the co-ordinated targeting of offenders; the production of integrated intelligence products; sharing professional knowledge and expertise; enhancing investigative co-operation; creating models for systematic action against criminals; the identification and resolution of bottlenecks; and mapping and analysis of trends and risks. In addition, there are eight multi-agency task forces, each focussing on a specific theme. Two of these task forces have been recently established subsequent to the NRA, one focussing on MSBs and one on TF. The performance of the task forces is monitored by the IC.

100. With regard to CFT, Israel has continued to consolidate, expand, and update the national system established in 2003 to counter TF. The CFT Committee (the authorities that are members of this Committee are also in the TF task force), was responsible for outlining national enforcement policy, strategy, and co-ordination of the relevant authorities. Responsibility for this system and the inter-ministerial committee recently has been moved to the Ministry of Defence (MoD); the

committee has been remodelled into a new body, the National Counter Financing Bureau. The new Bureau reports directly to the Minister of Defence (see IO.9).

101. A range of positive examples of national measures have been established during and since the NRA was completed. These include the introduction of tax evasion as a predicate offence for ML (2016), new legislation on TF TFS (2016), the establishment of task forces on TF and MSBs (2017 - also see below), the replacement of a registration framework for MSBs with a supervisory framework with more resources, legislation which addresses the significant frauds in relation to trading in binary options (2017), and legislation providing for greater restrictions on the use of cash (2018) and a reduced threshold for disclosure of cash at the borders. In addition to the introduction of licensing regime for MSBs (including credit service providers) (by October 2018), there have also been national supervisory initiatives. In particular, financial supervisors introduced new or updated legislative requirements in relation to reporting requirements on high-risk customers by the BoI (2016); CDD and other requirements to the credit service providers by CMISA (2018); and domestic PEPs, beneficial ownership, and high-risk customers by the ISA (2017-2018).

102. Following the completion of the ML NRA, the authorities engaged in a collaborative process to develop action plans so as to address the risks identified. Both of the ML action plans mentioned above were developed as a result and agreed by the ESC. Progress is monitored by the IC and the ESC approximately every two months. There is a separate action plan for TF; progress and actions are also monitored. There would be merit in supervisors being brought into the committee framework in a more substantial way.

Exemptions, enhanced and simplified measures

103. Israel has elected to apply several exemptions from compliance with the FATF Standards - dealers in precious metals, real estate agents, and TCSPs are not subject to any AML/CFT requirements. Lawyers and accountants are not subject to certain AML/CFT requirements (i.e. UAR). Israel bases these exemptions from AML/CFT regime or requirements on:

a) For dealers in precious metals: (a) gold dealers have been rated as having moderate-low ML risks; (b) the volume of the market is not significant; (c) VAT rendering ML through this sector unprofitable; and (d) the 2018 cross-border cash declaration legislation.

b) For real estate agents: (a) real estate agents were assessed as posing low risks and the risk of using real estate transactions for ML was rated as moderate-high - mainly with respect to limited cash transactions as most transactions take place through the highly monitored banking sector; (b) no indications in intelligence information that agents are involved in ML; (c) real estate agents are required to be registered and supervised by the registrar, though not for AML/CFT purposes; (d) rare occasions that agents perform transactions with funds connected to real estate transactions or holding funds on behalf of their clients; and (e) the role of real estate agents is limited by law to bringing together the two parties involved in a real estate transaction. Israel proposes to introduce legislation to apply AML/CFT obligations on the limited number of agents when they perform transactions.

c) For TCSPs: (a) most of such activities are carried out by lawyers and accountants carrying out activities which are covered by the AML/CFT framework, and (based on survey results or other information from some banks and lawyers, and liaison with an industry body) Israel indicated that there are only two TCSPs which are not lawyers/accountants; and (b) lawyers, accountants and the other trust service providers are required to maintain a separate bank account for each trust and such accounts are monitored by banks.

d) Lawyers and accountants providing BSP services (in relation to an exclusion from UAR requirements): through applying a rule that prohibits these professionals from conducting any high risk ML/TF transaction. The Israeli authorities regard this approach as more effective than a reporting regime, as they consider that these professionals might only submit a very limited number of UARs due to the extensive legal professional privilege which exists under Israeli law.

104. These exemptions are not considered justified as (a) the risk of gold dealers needs reconsideration in light of recent cases; (b) the risk assessment of lawyers, accountants, and TCSPs is not sufficiently comprehensive to understand the risks of these DNFBPs or legal persons or legal arrangements, and a distinction might be made between information where privilege applies and information at customer take on; (c) the assessment of the real estate sector does not justify an exemption for the sector, noting also that the authorities intend to legislate for agents who are part of the transaction. In addition, such wholesale exemptions go beyond the FATF Standards, where it is necessary to demonstrate low risk.

105. Israel has adopted enhanced measures for higher risk scenarios in some circumstances. These is a requirement to report Cash Transaction Reports for cash transactions and enhanced reporting for wire transfers with a value of NIS 5 000 (EUR 1 168) sent to countries designated as high risk (see IO.4 and IO.10) and a cash threshold reporting requirement, which was recently lowered from NIS 100 000 (EUR 23 400) to NIS 50 000 (EUR 11 680), and further lowered to NIS 12 000 (EUR 2 800) for designated land border crossing points.

106. Israel requires FIs to conduct enhanced due diligence and to manage risks by reference in the risk management circulars to the NRA, by requiring FIs to perform risk assessment of their customers and activities, and by setting out a list of specific high risk factors when establishing CDD measures (see c.1.7 and 10.17). There are some requirements and guidance for higher risks or enhanced measures in place for DNFBPs (see c.22.1). Also, see IO.4 for the application of enhanced measures in practice.

107. There are also some simplified due diligence measures (see R.10). However, the list of categories included is not based on adequate risk analysis by Israel or by the FI. There are also no provisions stating that simplified measures should be commensurate with lower risk factors, but there is a requirement to abolish all simplified measures in high-risk scenarios. Simplified measures are permitted after consideration of specific cases by the supervisory authorities after an application has been made by individual insurers or MSBs. See c.1.8, 10.18 and 22.1, and IO.4 for the application of simplified measures in place.

2

Objectives and activities of competent authorities

108. The NRA and the ESC and IC framework mentioned above provide a very strong basis for the objectives and activities of the authorities to be consistent with evolving national policies and identified risks. Significant action has been taken by the authorities to address risk in practice and they are well placed to undertake operational activity in line with risks. Targeting of criminal proceeds has a high priority within Israel. The policies of the authorities, whether articulated by way of strategies, work plans or other mechanisms, largely reflect the NRA and/or the action plans agreed by the IC.

109. Competent authorities generally base their activities on established policies. In particular, LEAs, financial supervisors, and to a lesser extent, DNFBP supervisors, are generally aware of the AML/CFT risks in their areas, and have taken corresponding measures. For example, some of the key financial supervisors have started to develop their understanding and enhanced their supervisory programmes on accounts with intensive cash activities, cross-border wire transfers, currency exchanges and money transmitters in recent year, following the identification of such areas as high priority and detailed action plans. The degree to which financial supervisors follow a full risk-risk based approach to supervision varies. As for DNFBPs, it is too early to conclude whether the supervisors/SRBs follow the national AML/CFT objectives, as they were only incorporated into the AML/CFT framework fairly recently.

110. On transparency of basic and beneficial ownership, the ICA and the ITA hold substantial information. The activities they undertake facilitate the adequacy, accuracy and currency of information in line with national objectives (although the ICA needs to undertake further mitigating measures (see IO.5)).

111. With regard to the supervision of NPOs, Israel has taken positive steps to establish a registration framework for several types of NPO established within Israel and periodically to improve the legislation governing the establishment and conduct of NPOs. The ICA has conducted outreach, undertaken on-site inspections, appointed external auditors to carry out inspections and used the court based liquidation system to good effect; nevertheless, while this proactive approach combats abuse of NPOs for TF, it is not in itself a full TF risk-based approach.

112. IMPA's work plan for 2018 takes account of the NRA and the IC's action plans. It prioritises high risk UARs; increasing co-operation and initiating projects with the ITA in relation to tax offences and cash activity; proactive detection of ML connected with real estate; identification of corruption, promotion of legislation to reduce risks; and the issue of guidance to the private sector on identified risks. IMPA's regular dissemination to LEAs spontaneously and on request. These disseminations include relevant and high-quality information, which is used by other authorities in investigations to develop evidence, trace proceeds and successfully confiscate assets. IMPA also proactively supports investigations.

113. ML investigations by LEAs are focused towards the threats outlined in the NRA and the objectives and goals of Israel's national policies, including that of attacking illicit proceeds from serious and organised crime. ML cases dealing with complex ML and as tasked by the IC are investigated by the task forces, the number

and staffing of which are sufficient to deliver their objectives, and which are consistent with Israel's risks.

114. The INP's work plan targets offenders and prioritises cases on the basis of the NRA and its most recent annual intelligence assessment; its budget is directed towards catching offenders and preventing and reducing crime. It reacts positively to changes in the system to improve effectiveness. In 2014, it established a dedicated financial enforcement unit within *Lahav 433* (INP's lead AML/CFT unit) to assist national units. In addition, there are eight thematic investigative task forces stationed in *Lahav 433* covering criminal organisations, corruption, online gambling, international crime and cross-border activity, professional laundering, professional ML linked to organised crime, MSBs and TF (see IO.7). Finally, INP has a SIGINT (signal intelligence) squad, which serves as support unit to to all financial enforcement teams including the task forces by focusing on large-scale, complex and international ML investigations.

115. The ITA has undertaken significant effort to counter fictitious tax invoices, as well as tax evasion. Its work plan includes co-operation with other authorities on addressing these crimes through investigations and implementation of relevant aspects of the high priority action plan arising from the NRA. This includes targets for ML investigations and confiscation, the establishment of a ML and confiscation unit and continued co-operation with the task forces, the Intelligence Fusion Centre (IFC) and other relevant teams, authorities and committees. It established a unit in 2015 to identify companies and dealers distributing fictitious invoices so as to aggressively disrupt this criminality. More recently it has analysed its databases to locate individuals with an unexplained lifestyle (leading to 40 000 cases and tax collection of NIS 1 billion (EUR 233.7 million).

116. Israel investigates and successfully prosecutes all types of ML offences, including cases of stand-alone and third party laundering, and cases involving foreign predicate offending. There are a high number of cases involving legal persons (see IO.7).

117. A section of the IC's high-level action plan is devoted to confiscation of proceeds and instrumentalities and it is clearly a major policy objective for Israel. The SAO has specified strategic goals, one of which is to enhance the effectiveness of financial enforcement. Its work plan is consistent with Israel's risks (including countering organised crime and terrorist organisations, and disruption of the financial basis of criminal and terrorist organisations). Each district attorney's work plan includes a component which targets ML indictments and confiscation. In addition, a "financial enforcement headquarters" has been established under the leadership of a Deputy State Attorney responsible for financial enforcement, so as to increase the number of convictions relating to organised crime related ML offences and significantly increase the value of confiscated assets.

118. Confiscation is a significant focus as part of investigation activity. Two departments of the SAO specialise in major crimes, including corruption and other financial crimes, and ML (especially those potentially leading to confiscation). Another department of the SAO, the Department of International Affairs, focuses on combating international crime, including serious and organised crime. A gap in the legislation handicaps the wholesale adoption of confiscation of equivalent value but there are proactive attempts to mitigate this gap by using all available

means under the framework to find practical and impactful solutions. Israel also applies, to a large extent, the extremely strong measures which exist to combat the cross-border movement of currency and bearer negotiable instruments that are falsely or not declared (see IO.8).

119. Counter terrorism and CFT have the highest priority. Israel has been successful in identifying TF including by extensive use of financial intelligence. A dedicated terrorism financing task force has been established to assist in detecting TF. Cases, which are led by *Shin-Bet*, are effectively identified and investigated, and terrorism investigations always incorporate a TF component. The investigation of TF is integrated with and supports national counter-terrorism strategies. The types of TF cases investigated and prosecuted are diverse, including cases on the collection and movement of funds. Thirty-nine persons have been convicted in 37 cases. Also, a number of cases investigated have been subject to disruption activity, rendering prosecution unnecessary (see IO.9). In addition, Israel (the MoD) has made numerous designations under UNSCRs 1267 and 1373. A variety of tools has been used to deprive terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities (see IO.10).

120. With regard to international co-operation, Israel has proactively used MLA and extradition requests to pursue criminals and their assets involved in ML, underlying predicate offences and TF. Israel has provided assistance in relation to MLA, extradition, financial intelligence and beneficial ownership. The quality of assistance provided is good although there are some concerns about the timeliness of MLA assistance (see IO.2).

National co-ordination and co-operation

121. Israel has strong and comprehensive national mechanisms to co-ordinate the development and implementation of policies and activities to combat ML and TF. These include the committee structures mentioned above. There has been considerable focus by Israel on adjusting the approach of some years ago of sharing of information to one of active collaboration. This is particularly noticeable in relation to investigation, prosecution and confiscation activity in which targeting of criminal proceeds is a high, joint, priority. There is also active collaboration between the investigation/prosecution/confiscation nexus of authorities with supervisory authorities and the ICA and between the supervisory authorities and the ICA.

122. The Intelligence Fusion Centre (IFC), comprising representatives of IMPA and LEAs, is an important mechanism for co-operation. Its purpose is to facilitate collaboration by LEAs and IMPA so as to produce integrated, multi-agency, high quality, intelligence and (through the IC's operational subcommittee) make recommendations on which cases should be prioritised; it has flexibility to issue intelligence reports beyond targets approved by the IC. It also generates joint investigations, with joint investigation teams being a usual approach to combatting financial crime ML and TF.

123. There are dedicated AML teams within the INP and the ITA and financial enforcement teams in every district of the SAO, and a permanent representative of the INP within IMPA connected to INP IT systems and databases. These mechanisms facilitate co-ordinated investigation, prosecution and confiscation

activity. The authorities also emphasised the importance of the "Joining Hands" initiative, an annual two day event for all LEAs, IMPA and other authorities to improve co-operation and information exchange, using discussion on current risks, trends, case studies, challenges and solutions as a means of achieving this objective at both the strategic and specific case levels. In addition, outside the day-to-day case environment, a separate academy for interdisciplinary enforcement studies has been established to provide a forum to establish inter-agency solutions to complex, tactical, issues in relation to all aspects of enforcement.

124. The SAO has also established a co-operation and co-ordination mechanism. The Financial Enforcement Forum comprises representatives of the SAO, the INP, the Administrator General, the MoJ, IMPA and the ITA. Its aims are to improve the combating of ML and confiscation through review of data collection on confiscation; identification of mechanisms to identify cases and assist prosecutors, and best practice; and address asset management issues. Outcomes have included the development of a model for case handling as between the roles of investigators and prosecutors and an on-line portal for case management by the different authorities involved with each case.

125. In addition to the formal structures described above, there is strong bilateral and multilateral co-operation at the operational case level in relation to both ML and TF, particularly between IMPA, the *Shin-Bet*, the INP, the ITA and the SAO. A significant number of examples of cases were provided to the assessment team which demonstrate the close working relationships of these authorities.

126. There are also formal procedures in place for co-operation at bilateral level in some cases, such as between the INP and IMPA (2006), and the INP and the ITA (2010). Co-operation is not limited to investigation, prosecution and confiscation activities. There is also collaborative work by the ITA and IMPA on projects on identifying tax evasion and ML, cash smuggling, and there was joint analysis of the Panama Papers.

127. The focus on collaborative work for ML also applies to CFT. In addition, LEAs and security agencies co-operate effectively, including co-ordination of work plans to ensure clear responsibility. At the operational level, the *Shin-Bet* works closely with the INP, the ITA, IMPA and other intelligence authorities to trace the movement of terrorist funds. The new task force on TF has also already generated benefit.

128. There are also mechanisms in place for co-ordination and co-operation between the FIU/LEA nexus of authorities and the supervisory and registration authorities. IMPA works closely with the supervisory authorities to enable them to assist reporting entities to improve the quality of UARs and also to contribute to audit and enforcement activities (see IO.6). It also participates as a member on all supervisory decision making committees on the potential imposition of sanctions. In addition, it has conducted outreach on ML and TF to the ICA. Furthermore, there are procedures in place between the INP and the ISA (2010), and the Roundtable and *Menifa* projects. These projects have facilitated joint activity between enforcement authorities and supervisory authorities in relation to defined subjects of interest or a person/place.

129. There is strong co-operation between the ICA and the ITA, with the ITA being provided with direct access to all of the ICA's databases at the end of each day. The ICA responds to requests for assistance from IMPA and *Shin-Bet* but does not receive case feedback from these authorities in relation to the assistance provided.

130. IMPA established the AML/CFT Regulators Forum in 2009 to co-ordinate the consistent implementation of AML/CFT standards by supervisory authorities. It meets three times a year and comprises representatives of IMPA, all the supervisory authorities and the ITA and, when required, the INP, prosecutors from the SAO or district attorneys, and the MoJ (including the legislation department and the ICA). In addition to the MOU signed in 2007, the BoI, the ISA and the CMISA signed an additional MOU in 2012 to increase co-operation among them and introduce a framework for the Regulators Forum. It is not considered necessary to extend the 2012 MOU to the other supervisory authorities on the basis that they participate regularly in the Regulators Forum and there is active co-operation in practice. Israel has demonstrated that there is strong co-operation between the authorities both through the Regulators Forum and operationally. The supervisory authorities consult each other on various aspects of their work, such as the introduction of the sectoral orders and the issue of circulars (e.g. the joint circulars on Bitcoin risks and on-site inspections).

131. With regard to PF, co-ordination of policy and operational activity related to Iran is comprehensive, with significant efforts having been made by Israel based on *Government Decision no. 3160 (2011)* and the 2012 Law for Countering Iran's Nuclear Programme (which resulted from the recommendations of an inter-ministerial committee (the Governmental Committee for Sanctions Policy against Iran)). A committee within the Sanctions Bureau within the MoF, collects data, co-ordinates potential designations for recommendation to the inter-ministerial committee, and serves as a central national mechanism for the dissemination of information (including the establishment of a publicly accessible website) and for investigating PF sanctions issues. The committee comprises representatives of the Prime Minister's Office, the MoF, the MFA, the MoJ, the Ministry of Energy and Water, the Ministry of Trade and Industry, the Ministry of Defence, the National Security Council, the INP and the BoI. There is a Sanctions Implementation Team within the MFA, the purpose of which is to improve the implementation of all aspects of UNSCRs in Israel at the legal and administrative levels and co-ordinate the actions of various authorities; its role is also pertinent to PF. However, the PF framework is less advanced regarding DPRK (noting that a certain degree of co-operation was demonstrated through a case study). The overall system has recently been strengthened by new legislation, and a revised committee structure and responsibilities as described above; the enhanced Sanctions Bureau now includes responsibilities for PF relating to DPRK.

Private sector's awareness of risks

132. Both before and during the NRA process, IMPA published substantial information relating to risks to improve private sector's awareness of risks. This included: (a) red flags documents on real estate, the diamond trade, NPOs, lawyers and accountants providing BSP services, tax offences, on-line gambling; (b) guidance on corruption and bribery of foreign PEPs; (c) TF typologies and

indicators; and (d) best practices for FIs (including a separate document for MVTS) and DNFBPs. It has also published updated guidance on key words which reporting entities should use in UARs and newsletters. FIs are aware of the guidance published by IMPA and consider them useful when considering filing of UARs.

133. During the NRA processes, FI supervisory authorities issued a NRA questionnaire, adjusted based on each individual sector's profile, to all supervised entities. As an example, the BoI considers that completion of the questionnaire improved banks' understanding of risk. The BoI also followed up with some of the banks before they completed the questionnaire to clarify issues, and review and follow up responses after completion of the questionnaire. The ISA met with all stock exchange members before the issue of the questionnaire and with some of them following receipt of the responses. In addition, the Supervision Department of the Postal Bank met with some local branches and the CMISA met with some MVTS entities after the responses were received to better understand the answers.

134. After the completion of the NRA, IMPA distributed the public NRA and financial sector NRA reports to all members of the ESC and the IC, as well as all LEAs and supervisory authorities – with the BoI, ISA, CMISA, the Supervision Department of the Postal Bank, the diamond dealers supervisor (MoE) and the BSP supervisor (MoJ) uploading the reports on their websites. These supervisors discussed the NRA contents with licensees/entities prior to the NRA publication. Financial and DNFBP supervisors/SRBs, in collaboration with IMPA, also arranged outreach activities to inform supervised entities the results of the risk assessment reports (e.g. the BoI with the Compliance Officers Forum for banks in July 2017; the ISA for stock exchange members and trading platforms in June 2017 and for portfolio managers in October 2017; the CMISA for its licensed entities on NRA findings and typologies). IMPA also issued the reports to all licensed entities, published them on its website and issued a media release at the time of publication.

135. As indicated in IO.4, not all FIs and DNFBPs agree with the findings of the NRA, with some FIs considered that the NRA might have overestimated the ML/TF risks that their sectors face while lawyers and accountants providing BSP services and diamond dealers considered that the rating has not taken into account the mitigation measures implemented by their sectors. While recognising that the authorities have much more information available to them and the differing points of view (including bias by high risk sectors), there is scope to enhance understanding by distributing further information after the next iteration of the NRA and including more detailed information in the public version of the NRA. The distribution should include all DNFBPs as it is possible that not all of them (especially those not included in the national AML/CFT regime) have seen the NRA reports.

Overall conclusions on IO.1

136. **Israel has achieved a substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

Israel has achieved a high level of effectiveness for IO.6.

a) Israeli authorities have access to and regularly use financial intelligence and other relevant information to investigate ML, predicate offences and TF. The use of financial intelligence is a strong point of the Israeli system and at the centre of its approach to combating crime and terrorism.
b) Financial intelligence and other relevant information are also used for identifying investigative leads, developing evidence in support of investigations, and tracing of criminal proceeds related to ML, predicate offences and TF.
c) The Israel FIU (IMPA) regularly disseminates financial intelligence both spontaneously and upon request. IMPA also frequently exchanges information with foreign counterparts to facilitate the tracing of proceeds abroad.
d) The quality of financial intelligence and analysis produced by IMPA is high and supports the operational needs of the various LEAs. IMPA provided many examples of its high-quality disseminations and these have contributed to good outcomes in terms of prosecutions and convictions (including confiscation) for ML, associated predicate offences and TF. Feedback from INP and *Shin-Bet* shows that a high percentage of IMPA's intelligence reports were used for the purpose of conducting ML and TF investigations and a significant proportion contributed to tracing proceeds and the seizure and confiscation of assets.
e) IMPA has a well-developed IT system to perform strategic analysis and identify ML/TF trends and patterns. This in turn contributes to IMPA's operational functions.
f) IMPA has a high degree of ongoing co-ordination, co-operation and exchange of financial intelligence with LEAs (including security agencies). This is most evident at the level of the Intelligence Fusion Centre and the eight inter-agency task forces, all of which involve officers from IMPA, INP and ITA.
g) Statistics on the use of financial intelligence information are not comprehensively maintained by LEAs and IMPA. The current method of tracking the number of requests made by LEAs as a proxy tends to grossly under-represent the actual use of such information. This is due to the practice of sending batched requests which can contain requests for multiple cases.

3

Immediate Outcome 7

Israel has achieved a substantial level of effectiveness for IO.7.

a) Israel is successfully identifying and investigating ML cases through a mix of financial intelligence packages developed by IMPA, information supplied through law enforcement intelligence or as a result of ongoing predicate criminal investigations.
b) Israel places a significant, and entirely appropriate, emphasis on training investigators and prosecutors in ML typologies, processes and procedures.
c) Many complex and/or significant ML cases are investigated by nationally co-ordinated, inter-agency structures (i.e. the Intelligence Fusion Centre, task forces) that progresses criminal investigation matters, with the assistance of either the State or District Attorney's Office, through to prosecution. ML cases are also investigated by regional and national units within the INP e.g. *Lahav 433*. The majority of ML activity investigated and prosecuted is associated to organised crime-related offences – i.e. fictitious invoicing, tax evasion, fraud and corruption, which is in line with the major ML threats identified by Israel.
d) Israel investigates and successfully prosecutes all types of ML offences, including cases of stand-alone, third party ML, and ML involving foreign predicates to a large extent and largely in line with the risk profile. This also includes, when compared to other jurisdictions of a similar size and level of economic development, a high number of individual cases involving legal persons. However, with nearly four out of five cases of ML prosecutions relating to self-laundering and the large number of legal persons prosecutions, only six ML charges related to stand alone ML activity between 2014 and 2016.
e) Israel prosecutes legal persons, and provided cases where legal persons where convicted of ML and sentenced to a fine.
f) Sentencing for ML offences is considered proportionate and dissuasive when compared to the punishments for other similar crimes (e.g. fraud, tax) where accurate data can be identified. Sentences are often combined with other criminality which makes a full determination difficult.
g) The time taken for certain ML cases to progress through the courts is a concern; those cases which do not involve persons in custody, and particularly legal persons (and NPOs), can take years.

Immediate Outcome 8

Israel has achieved a high level of effectiveness for IO.8

a) Israel clearly has the confiscation of criminal proceeds and instrumentalities as a policy objective; this is delivered upon to a large extent. Each agency has clear, current policies on confiscation procedures and provides training on the subject, which are embedded across their respective organisations and work plans.
b) Overall, the competent authorities are confiscating the proceeds and instrumentalities of crime successfully. The significant levels of confiscation confirm the various authorities' policies for prioritising confiscation.

Compared to other jurisdictions of a similar size and economic development the net recoveries, be they from criminal, administrative or by way of the tax assessments processes, are impressive (mindful however that the data presented also includes fines).

c) Israel does, to a large extent, discharge its international responsibilities in relation to the confiscation of the proceeds of crime. Israel takes action to address the recovery of the proceeds of crime which has been acquired through foreign predicate offending or by taking action to trace and recover proceeds that have been moved to other countries.
d) Authorities are also confiscating proceeds involving equivalent value for ML and predicate offences. Confiscation results are consistent with the ML NRA to a very large extent. Since equivalent value cannot be automatically triggered in confiscation proceedings relating to most predicate offences, this is done through pursuing self-laundering cases run in tandem with the predicate offences. However, the methodology utilised to enable value-based confiscation is only relied upon when the suspect has taken a proactive additional action or activity which can be deemed to be ML; the additional ML charge is not routinely added. This limits somewhat the ability of the authorities to seek value-based confiscation across all areas of acquisitive crime.
e) Israel has very strong procedures and mechanisms in place to address the threat of cross border movements of currency and bearer negotiable instruments that are falsely or not at all declared. The sanctions applied to breaches of the declaration obligation are proportionate and dissuasive.
f) Israel's ARFO has shown effectiveness in managing assets it is aware of. However, it has no capability to compel information from any party at any time which would assist the wider policy objective of confiscating criminal proceeds. Israel views the investigation of recoverable assets a function of law enforcement authorities only. Whilst the ARFO can share information with competent authorities, its effectiveness to broaden the confiscation investigation through the identification of additional assets or the development of intelligence alongside competent authorities and thereby releasing resources of law enforcement agencies should be considered in order to further improve the system.

Recommended Actions

Immediate Outcome 6

a) INP should request financial intelligence information from IMPA for all predicates offences, when relevant, without first assessing whether the case meets certain criteria, such as complexity.
b) Authorities in Israel (especially LEAs and IMPA) should have consistent method of tracking the use of financial intelligence information, by keeping record of the number of cases rather than number of requests made

Immediate Outcome 7

a) Israel should consider improving the number of stand-alone ML investigations and prosecutions to demonstrate that all types of laundering will be pursued by the authorities even when the precise underlying criminality cannot be established and thus improve the overall dissuasive impact of their approach to ML activity.
b) Israel should continue to invest in the training of investigators and prosecutors involved in ML (and TF) cases within the Financial Academy to enhance succession planning and ensure that performance is maintained.
c) Israel should consider appropriate steps to rectify the delays in the completion of criminal ML cases, specifically when they involve legal persons, to ensure that the deterrent factor that such proceedings represent is seen to be effective and proportionate. In this regard, Israel should consider the development of specialist economic crime courts.
d) Israel should consider reviewing the sentencing guidelines for ML offences to ensure the penalties reflect the breadth of the sentencing options available. The review should also include requesting the judiciary to identify which elements of the sentence relate to which elements of the offending thereby making sanctions derived from ML offending more transparent and thus more likely to be dissuasive.
e) Israel should take steps to remove the 'wilful blindness' exclusion (see R.3) from the s.4 PMLL offence as this is seen as unnecessarily restricting the options available to prosecutors in pursuing ML prosecutions.

Immediate Outcome 8

a) Israel should address the technical gaps in its legislation to fully and directly enable value-based confiscation including the gap in provisional seizure measures (see R4) relating to cases that do not include ML or predicate offending that does not engage value-based confiscation measures.
b) Israel should consider the development of a full and wide-ranging non-conviction based legal framework for the confiscation of property.
c) Israel should consider developing specialist economic crime courts (see IO.7 recommendations) and including in their remit confiscation. This would expedite proceedings and natural justice whilst also allowing for a closer correlation of seizure and confiscation data.

137. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

138. Israeli authorities make extensive and regular use of financial intelligence and other relevant information to identify investigative leads, develop evidence in support of investigations, and trace criminal proceeds related to ML, TF and associated predicate offences.

139. The assessment team based its conclusions on a variety of elements including: sources of financial information and statistics provided by IMPA; discussions with relevant Israeli LEAs (INP, ITA, ISA, and *Shin-Bet*); discussions with members of the Implementation Committee (and its sub-committees), the head of the Intelligence Fusion Centre and officers operating in the task forces. The team reviewed volumes of the financial intelligence reports produced and disseminated by IMPA, and many cases demonstrating that financial information and intelligence is being used in practice to support ML and TF investigations and asset tracing and confiscation.

140. LEAs and IMPA have access to, and use financial intelligence and other information from a large number of sources (see Box 1 below). Information held abroad may be requested through the Egmont Group of FIUs, Europol, Interpol, the EU's Camden Asset Recovery Inter-Agency Network (CARIN), and bilateral channels with international counterparts (see IO.2).

Box 1. **Non-exhaustive list of sources of financial intelligence and other types of information used by competent authorities**

- IMPA's database is the primary repository of financial intelligence, developed on the basis of reports received from reporting entities (e.g. CTRs and UARs), but also with information IMPA can get access to directly (e.g. number of government and private databases, tax information) (more information on IMPA's database in section 3.2.2).
- Government databases – which include INP's databases: Criminal Registry (information on ML/TF cases investigated/indicted/convicted), *Mivzak* (an online channel of communication between INP and banks), *Pettan* (IT tool allowing the analysis of financial transactions and identification of potential assets for confiscation using FIs' information). Other government databases include information on residents, corporate, motor vehicles and property registries.
- Tax Information is also available through ITA's participation in the Intelligence Fusion Centre, the Task Forces and joint investigations (upon request). It includes access to all government official databases and registries, the National Insurance database, and import / export records.
- Border Crossings Authority Database (travel information): Cross-border cash declarations (with customised threshold of NIS 12 000 (EUR 2 800) when entering or leaving Israel via land border crossing area).
- Information from Sanctions Committees on reporting entities and individuals that have breached their reporting or declaration duties.
- Commercial, legal, business databases and open source (e.g. MAYA is a database on publicly traded companies).

141. LEAs rely on IMPA as a key source of financial information. In relation to banking information, Israel does not have a bank account register. However, there are only 20 banks operating in Israel, and a total of 96% of the assets are

concentrated in five major domestic banking groups. LEAs can obtain financial information from banks, including bank statements and whether or not they hold any assets for possible confiscation, through court orders. This is done in practice rather routinely and easily, sometimes through special judges assigned to issue such court orders. INP submits the court orders directly to all banks using the *Mivzak* system, which is an online platform to correspond with banks and obtain financial information from them.

142. Israeli authorities provided numerous cases which demonstrate that financial intelligence provided by IMPA and other relevant information that can be accessed by LEAs are also frequently being used to successfully investigate ML/TF and identify new targets.

Table 5. **Use of IMPA's Intelligence Reports in LEA investigations**

	Number of intelligence reports disseminated (spontaneously and upon request) by IMPA to LEAs				
	2013	**2014**	**2015**	**2016**	**2017**
INP**	495	531	593	686	641
INP Terminal and IFC	47	30	44	41	35
ITA*	N/A	N/A	N/A	N/A	27
ISA**	N/A				
Security authorities	65	83	53	57	85
Total	**607**	**644**	**690**	**784**	**788**

Note: Until April 2017 the exchange of information to ITA was made via INP. Between 2013 and April 2017, 109 Intelligence reports were disseminated to the ITA. ITA also receives intelligence reports and financial information in the framework of joint investigation.*
*Note **: Intelligence reports to ISA are disseminated through the INP. Between 2013 and 2017, IMPA disseminated 64 intelligence reports to the ISA.*
Source: *IMPA.*

143. Table 6 reflects the number of convictions that resulted from IMPA's spontaneous disseminations and in response to LEA requests with information on entities other than the requested ones, which subsequently led to new investigation channels. Due to their current method of maintaining statistics, IMPA does not have easily available statistics on convictions obtained when responding to an LEA request specifically on the requested entities.

Table 6. **Judicial proceedings (in cases) generated by FIU disseminations or when FIU disseminations revealed new investigation channels**

Year	Prosecutions					Convictions				
	Total number of cases prosecuted		Cases based on FIU disseminated information			Total number of convictions (Final)		Cases based on FIU disseminated information		
	ML	TF	ML	TF	Pred. Off.	ML	TF	ML	TF	Pred. Off.
2014	31	3	21	3	13	33	3	15	2	12
2015	56	22	38	3	26	30	5	21	1	13
2016	50	28	30	3	28	33	9	25	2	17
Total	137	43	89	10	67	96	17	61	5	42

Source: IMPA, SAO.

144. The use of financial intelligence and other relevant information is also evident in the context of the Intelligence Fusion Centre (IFC) (see Chapter 1). The IFC was set up to provide a holistic approach to ML/TF investigations, including through the identification of significant ML/TF threats and targets for investigation. The IFC is led by an INP senior officer and has permanent representatives from INP (2), ITA (3), and IMPA (2), as well as representatives from other LEAs and security agencies on an ad hoc basis.

Box 2. **Example of IMPA's financial information feeding into ML investigations**
The "F" Case

Background – The case relates to an acting domestic PEP.

Relevance to IO.6 – IMPA undertook an initial analysis on the basis of a UAR received, and sent an intelligence report to INP on the suspect and his family members, with details on suspected ML activity potentially arising from bribery. INP and ITA subsequently commenced an investigation. During the investigation, IMPA assisted in requesting additional information from relevant local FIs and sent requests to counterpart FIUs. This additional information substantiated the original suspicion and provided information on the financial trails (including assets) linked to the suspects.

Outcomes – In 2018, this PEP and other suspects were indicted and assets of approximately. NIS 10 million (EUR 2.3 million) were frozen. The case is still pending.

145. The IFC exchanges information and intelligence amongst its member agencies on a daily basis. Its analysis and proposal for targets are presented to the Inter-Agency Implementation Committee for approval. The intelligence reports produced by experienced LEA officers that form the IFC support ongoing investigations launched by investigative units as well as new ones. They include indication of intelligence gaps (if any) as well as recommendations for further action.

Box 3. **Use of financial intelligence by the Intelligence Fusion Centre**
The "DDO" Case

Background – This is a TF-related case which illustrates the use of financial information and intelligence from IMPA by LEAs. It is also a positive example of informal international co-operation, TF investigation, and designation.

Relevance to IO.6 – IMPA played a key role in the DDO case. As part of ongoing monitoring of the unusual activity reports, IMPA detected diversion of financial activity from entities that had been previously designated as an unauthorised association for TF purposes. As part of the financial investigation, IMPA sent requests to receive supplementary information from abroad and from a financial institution in Israel. The voluminous data obtained by IMPA and the IFC assisted in the primary task of identifying and mapping various entities that together comprised the elaborate network of the DDO. The case exposed a vast network of illicit TF activities, and yielded important new knowledge about radical Islamist methods of ML and TF. For detailed information on this case, please refer to IO.9.

146. The use of financial intelligence is an integral part of Israel's response to terrorist financing and terrorism cases. Excellent outcomes have been achieved in terms of detecting TF activity, contributing to arrests of TF suspects, and leading to subsequent TF convictions. The high degree of relevance and utility of IMPA's disseminations is attributable to INP's and *Shin-Bet*'s regular and close consultations with IMPA throughout the investigation. Financial intelligence from IMPA is also used to successfully develop TF cases and evidence and expose terrorist networks and methods. See the full case examples in IO.9. Summaries of these examples are as follows.

Box 4**. Use of financial intelligence in TF cases**

The "I" Case: IMPA's proactive reports contributed to the intelligence gathered in the case, assisted in the arrest of an attorney that abused her status to disguise the source and destination of funds, and led to the detection of new methods of activity of terrorist financiers.

The "C" Case: MPA's intelligence reports, in response to requests that came both from *Shin-Bet* and INP, assisted in the arrest of the offenders that had used a network of foreign shell companies to raise funds for a terrorist organisation, and exposed new entities which were suspected to be involve in the TF activity.

The "A" Case: IMPA's reports, in response to both *Shin-Bet*'s and INP's requests, exposed the offender's bank accounts used for the funnelling of TF funds). The case involved the abuse of NPOs for TF purposes.

The "M" Case: IMPA's reports, first proactive and then responsive, led to the exposure of TF activity. The case involved *Hawala*-type transactions.

The "N" Case: The case demonstrates the efficient use of financial information in TF investigations, and as a tool to continue monitoring TF activity after an organisation was designated for TF activity. The case involved the abuse of foreign NPOs for TF purposes.

For more details on these cases, see IO.9.

147. Another good example of financial intelligence and other information being used for the purpose of ML/TF/predicate offence investigations are the eight

investigative Task Forces. These Task Forces are operational teams comprising of representatives from INP, ITA, IMPA and SAO. All Task Forces are led by an INP senior officer and focus on a defined crime or ML/TF phenomenon, such as international organised crime, corruption. As part of its mandate, the Task Force cross-checks and exchanges financial information and intelligence accessible to its permanent members, in particular IMPA's intelligence. For more details on the Task Forces, see IO.7.

Box 5. **Use of financial intelligence by a Task Force**

The "SL" Case

Background - This case was investigated in 2013-2014 by the Task Force dedicated to professional money launderers. It related to a large-scale investigation of a professional ML operation, which used a network of foreign connections (e.g. front companies, NPOs, and diamond dealers) to launder and transfer of large amounts to and from Israel, without declaring them.

Relevance to IO.6 - During the investigation, the Task Force made extensive use of financial intelligence, requesting IMPA to collect financial intelligence (including from foreign countries). In response to the 19 requests received, IMPA provided 37 intelligence reports, which enabled the worldwide mapping of the ML ring (including companies owned by suspects and the use of an MSB owned by the main suspect). The information also exposed previously unknown accounts and details on the ultimate BO behind these accounts. The financial information provided by IMPA in this case significantly assisted in providing new targets for investigation and in establishing ML suspicions.

Outcome - IMPA continued to work with the Task Force until 2016 when the case was sent to the Tel Aviv District Attorney's Office (Taxation and Economics) for prosecution. Case is ongoing.

148. As for asset confiscation, IMPA's intelligence reports contain a section which lists potential assets for confiscation, including the nature, location, and beneficial ownership of the asset. Feedback from INP showed that a high percentage of IMPA's intelligence reports were useful and relevant to investigations and contributed to the seizure/confiscation of assets.

Box 6**. Examples of the use of financial intelligence for the tracing of criminal proceeds**

The "P" Case

IMPA provided information that included a mapping of the network of involved accounts and entities, as well as information on possible assets for confiscation. Defendants were convicted in 2014 and a total of NIS 35 million (EUR 8.2 million) was confiscated. A fine of NIS 2 million (EUR 467 000) was also imposed.

The "NH" Case

IMPA's intelligence reports provided information regarding real estate assets acquired by a professional money launderer. IMPA's information revealed the

ML scheme and properties criminally purchased. These assets were seized and confiscated during the legal proceedings. Suspects were indicted in June 2017. Property in the amount of approximately NIS 16 million (EUR 3.7 million) was confiscated.

The "B" Case

This case, which began in 2017, relates to an investigation of fraud, tax and ML offences committed in in a third country. The financial information provided by IMPA identified fund transfers from abroad to accounts held in Israel. IMPA also identified the transfers' timeline and the source of funds. An investigation was carried out on that basis and resulted in the conviction for ML offences under s.(3)b of the PMLL, and the confiscation of NIS 27 million (EUR 6.3 million) in the identified accounts.

STRs received and requested by competent authorities

149. INP, ITA, and ISA request and receive from IMPA relevant and accurate unusual activity reports (UARs), currency transaction reports (CTRs),[20] and customs declarations.[21] These are the three main types of financial intelligence in IMPA's database. These contain relevant and accurate information, which greatly assists law enforcement authorities to perform their duties. To date, IMPA's database contains approximately 540 000 UARs, 16.3 million CTRs, and 66 000 customs declarations – all of which can be shared domestically and with foreign counterparts. IMPA's database also contains information from foreign FIUs, including information that was requested from IMPA (2 542 requests), by IMPA (492 requests), and at the request of a domestic LEA (1 308 requests received). IMPA also requests additional information from reporting entities in relation to reports submitted by the same or another reporting entity, and this information is also kept in its database and shared with law enforcement.

150. As reflected in table below, compared to 2013 figures, there has been a significant increase in the number of CTRs (by approximately 18%), customs reports (by approximately 44%) and UARs (by approximately 78%) received by IMPA which is attributed to better implementation and understanding of reporting obligations by FIs, supervisory actions and extensive outreach to all types of reporting entities. While a decrease of approximately 35% was noted in the number of received customs reports between 2015 and 2017, the overall increase is of 42% between 2013 and 2017. The recent change of threshold for specific designated land border crossing points (see IO.8) already increased the number of received customs declarations reports (December 2017-March 2018).

20. CTRs include: cash deposits and withdrawals, currency exchange, wire transfers, and remittance. CTRs (transactions involving with risk countries) have a lower threshold (NIS 5 000/ EUR 1 168).
21. Customs declarations at land crossings (NIS 12 000) and customs declarations when entering/leaving Israel (NIS 50 000/EUR 11 680).

Table 7. **Number and breakdown of reports received by IMPA (2013-2017)**

Type of Report	2013	2014	2015	2016	2017
CTRs	1 534 862	1555 810	1 687 675	1 701 070	1 819 227
UARs	49 798	60 585	73 863	78423	88 443
Customs	5 744	9 437	12 529	10688	8 189
Total	1 590 404	1 625 832	1 774 057	1 790 181	1 915 859

Source: IMPA

151. The vast majority of reported UARs come from the banking sector – average of 80% of the total number of UARs received. This is largely due to the guidance and feedback provided by IMPA to the banking sector over a course of 92 meetings held between 2013 and 2017. In 2017, most of the UARs received from FIs originate from banks (approximately 60%) and MSBs (approximately 26%), which is consistent with the country's risk profile (see IO.1 and IO.4).

152. IMPA conducts ongoing monitoring of the quality of received UARs. It published a set of key words to assist reporting entities to focus on higher-risk/more suspicious activities when reporting UARs. IMPA also periodically reviews to what extent FIs are using these key words and provides periodic feedback to reporting entities, including a review of the quality of their UARs (including where further improvements can be made). Whenever defensive reporting is detected, IMPA follows up with the FI concerned.

153. IMPA's focus on MSBs in recent years resulted in a substantial increase in the number of UARs filed by this sector - from 435 UARs received in 2013 (i.e. 0.25% of received UARs) to 23 327 in 2017 (i.e. approximately 25% of received UARs). This can be explained by IMPA's commitment to raising awareness on the obligations of PMLL within the sector, with the view to improving the sector's risk-based reporting, in terms of quantity and quality. IMPA, in collaboration with the relevant supervisor, held 15 conferences for the MSBs between 2013-2017, as well as 4 meetings with IT companies providing software services to the majority of MSBs to improve MSBs reporting systems. IMPA noted an improvement in the quality of MSB's reporting as a result of this engagement.

154. Whenever available, IMPA also includes CTRs and customs reports in its intelligence reports (in addition to UARs). These reports are used as intelligence in investigating both ML and TF cases, and assist in identifying international money flows and links to foreign jurisdictions. CTRs reported by MSBs are very useful and have been used in investigating tax offences, illegal gambling, corruption cases and more.

155. IMPA exchanges financial information with competent authorities on a daily basis, including disseminating its analysis directly to INP and ITA both spontaneously and upon request, and to ISA through INP. The total number of spontaneous disseminations has remained relatively constant over the past few years, whereas the number of disseminations upon request has increased. The decreased number of spontaneous reports disseminated to INP in 2017 is due to changes in IMPA's work procedures. These changes aimed at enhancing the efficiency and effectiveness of IMPA's disseminations. As such, IMPA began sending "batch spontaneous reports" to its INP terminal for a pre-check before formally disseminating a full intelligence report to INP. In doing so, IMPA wants to

make the best use of its human resources (i.e. analysts) and focus on its most significant spontaneous disseminations.

Table 8. **IMPA's disseminations – spontaneously and upon request (2013-2017)**

Year	Spontaneous Disseminations	Disseminations Upon Request	Disseminations through IFC and INP Terminal*	Total Disseminations
2013	247	313	47	607
2014	248	366	30	644
2015	245	401	44	690
2016	252	491	41	784
2017	97**	656	35	788

*Note *: Disseminations through IFC and INP Terminal include both spontaneous disseminations and disseminations upon request.*
*Note**: Decrease is due to changes in IMPA's work procedures – which includes the use of batched disseminations.*
Source: IMPA.

156. The overall increase is due to a number of measures taken by IMPA to improve its work processes and analytical capabilities. IMPA is routinely involved in providing training to LEAs on ML/TF matters, and has contributed to raising LEA's awareness on the value of financial intelligence and IMPA's capabilities. IMPA worked with LEAs to better understand their investigative needs, and developed procedures and tools to better respond to these needs. Examples include:

- The setting-up of a prioritisation mechanism for incoming requests. In "extremely urgent" cases, IMPA disseminates financial information without in-depth analysis within two working days.
- Changing the structure of its intelligence reports to reflect LEA's feedback.
- Responding to specific questions and issues raised by LEAs in their requests.
- The setting-up of an INP police terminal within IMPA, which now facilitates batch screenings and the dissemination of large volumes of information.
- The ongoing development and trial use of a risk-scoring engine to better identify ML/TF suspicions (to be completed in 2019).
- The development of IT solutions to reduce analysts' working time on intelligence reports without compromising on quality, thus resulting in speedier disseminations.

157. IMPA also has strong internal collaboration between its research and analysis department and its collection and control department. Both departments provide each other regular feedback on the quality and relevance of the reports received, supplemented by the feedback provided by IMPA's Alert Centre.

158. Lastly, IMPA is routinely involved in LEAs trainings on ML/TF issues, with the aim to raise LEAs awareness on its operational and strategic analytical capabilities. INP feedback to IMPA indicates that 8.5% of IMPA's spontaneous dissemination by IMPA led to the initiation of an investigation by INP.

Box 7. **Example of IMPA's spontaneous disseminations leading to the commencement of investigations**

The "Checklist" Case - a complex ML case which was initiated following strategic analysis undertaken by and subsequently disseminated by IMPA to INP. The analysis identified new ML patterns and a professional ML scheme. See detailed information on this case in IO.7.

The "X" Case - a high-level corruption case, initiated by a proactive intelligence report sent by IMPA to INP. The information provided was identified in the course of IMPA's ongoing monitoring of unusual activity reports (UARs) relating to possible corruption offences by a senior public official, his family, and by way of using straw men and corporations. IMPA conducted additional analysis of the financial information, cross-checked with information from other sources, requested information from foreign FIUs and additional information from FIs in Israel. Further intelligence reports on this case were sent to INP detailing all the relevant parties, bank accounts and funds transfers, in Israel and abroad. IMPA continued to be involved to provide ongoing UAR monitoring and analytical support after the investigation was launched. The investigation is still ongoing.

159. INP has a work terminal within IMPA's premises. This is managed by police officers with ML/TF training. These officers work closely with IMPA's analysts on operational and strategic analysis both for proactive projects and in response to INP's requests for information. Units in INP regularly request financial intelligence information from IMPA in ML/TF investigations, and in investigating associated predicate offences regarded as having potential for ML/TF.

Table 9. **LEA's request for information from IMPA (2013-2017)***

Year	INP requests	INP requests via IFC	Security authorities' requests	ITA requests
2013	201	47	24	**
2014	270	30	16	
2015	271	37	14	
2016	333	28	15	
2017	375	31	34	35
Total	1 450	173	104	35

*Note *: Including batch requests (that can include 6 to 12 different cases, in most instances).*
*Note **: Before April 2017, the exchange of information was made via the INP.*
Source: IMPA.

160. The number of INP's requests for information to IMPA can appear as somewhat low. For example in most years, there were fewer requests for information from IMPA than the actual number of ML investigations. This is due to some INP units' practice of sending requests in batches to INP officers stationed at the IMPA terminal, rather than making one request for each case. For statistics purposes, INP would treat a batched request containing requests for several cases as one request. The assessment team sighted a number of "batched" requests. In

most cases, a batched request would contain about 6 to 12 different cases.[22] Therefore, the figures in the table above tend to under-represent the actual number of requests made by INP.

161. In order to avoid overloading IMPA with requests for information, INP officers are instructed to approach IMPA in all ML cases, and with respect to predicate offences, INP uses its discretion while submitting IMPA with requests for information; e.g. INP may decide not to approach IMPA if the sum involved is small, or if it already has substantial financial information obtain through court order (see above for broad authority to issue orders to all financial institutions), etc. However, there are concerns that by not approaching IMPA for information on what may initially appear to be a less serious offence, the opportunity to detect more serious offences from available information may be missed.

Box 8. **Examples of investigation initiated as a result of a dissemination by IMPA in response to a request**

The "KA" Case – IMPA's financial intelligence exposed the currency service providers used in the ML scheme, as well as the criminal organisation entities involved in the receipt and depositing of funds into accounts owned by heads of the criminal organisation. The cross-checking of the information available to the investigation team with IMPA's reports established the suspicion of fictitious transactions use by the criminal organisation.

Outcome – IMPA's financial information assisted in the tracing of funds and accounts of currency service providers, and the ultimate confiscation of approximately NIS 1.2 million (EUR 280 400). Property was also seized in the total amount of approximately NIS 17 million (EUR 4 052 460).

The "512" Case – Financial information obtained from IMPA contributed to the suspicions against one of the largest criminal organisations in Israel (international network of drug trafficking and money laundering) and identifying property for seizure and confiscation in Israel and abroad (after receiving responses to requests to the counterpart FIUs.

Outcome – The defendant was convicted of ML offence as per s.4 of the PMLL and EUR 1.9 million confiscated. Some proceedings were still ongoing by the time of the on-site. See more details on outcomes in IO.7.

The "NA" Case – illustrates IMPA's contribution through its participation (as a member) in the Ports and Border Crossings task force. IMPA assisted in the investigation by providing intelligence reports and participating in joint working meetings that confirmed the suspected ML activity, including of the identification of involved parties and their inter-connections, but also the identification of assets for seizure and confiscation.

Outcome – An indictment was filed against all involved parties. Subsequent convictions in 2017 led to fines and confiscation of funds totalling NIS 4.6 million (EUR 1 million). Case also referred to in IO.7.

The "M" Case – illustrates IMPA's contribution through its participation (as a member) in the joint task force dedicated government corruption. IMPA

22. There was an instance of one unusually large batched request that had 42 entities said to be involved in 42 different cases.

assisted in the investigation by providing substantive financial information with enable to task force to formulate and establish ML suspicion. Information also revealed involved entities and their inter-connections, exposed the ML patterns and methods used as well as the channel for transferring funds.

Outcome – The case ended with seizure of the property totalling approximately NIS 97 million (EUR 21 712 260).

162. Following the 2016 amendments to the PMLL (i.e. making tax offences a predicate offence to ML), IMPA can directly disseminate financial intelligence information to ITA. ITA issued a directive requiring its investigators to make requests for information to IMPA for all tax and tax / ML investigation and intelligence cases. The Directive was operationalised in April 2017, and ITA made 35 requests for financial intelligence in 2017. This number appears to be low. ITA explained that this was the first year of the operationalisation of direct screenings with IMPA, and more attention was given to the cases regarded as being of higher priority to ITA. In the first quarter of 2018, ITA significantly ramped up its requests for information from IMPA. It sent two batched requests involving 306 entities from 306 different cases. IMPA's financial intelligence reports have strong value and relevance to ITA, which explains the above-mentioned ITA Directive and the sharp increase in requests for information received from ITA in the first quarter of 2018.

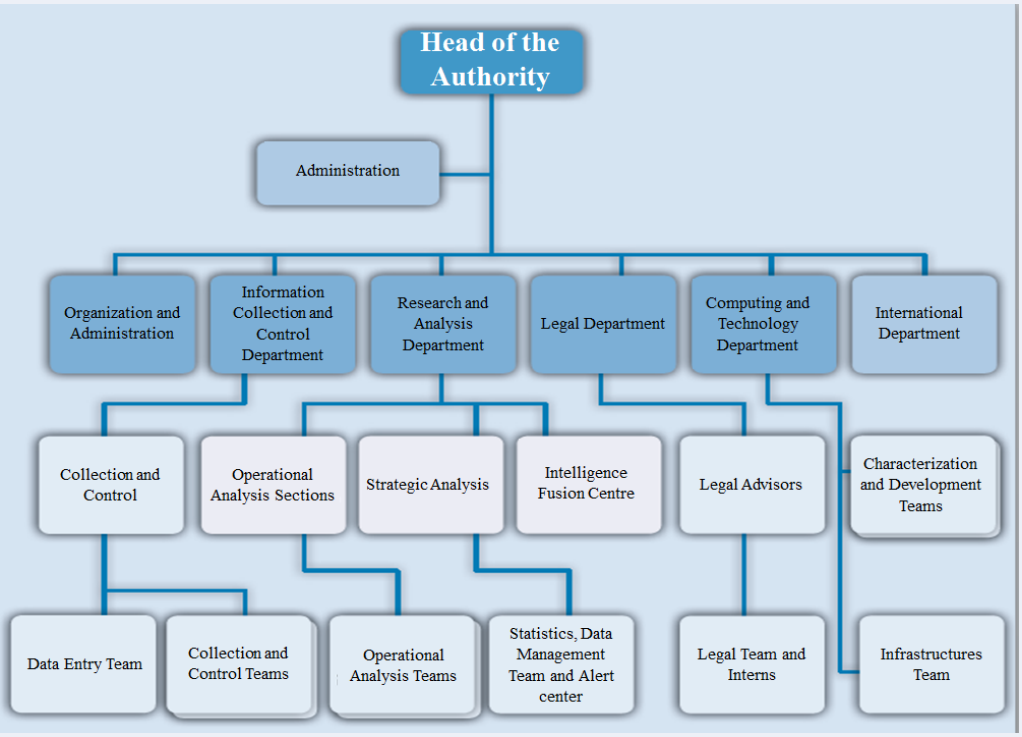
Operational needs supported by FIU analysis and dissemination

163. IMPA's financial analysis and dissemination support the operational needs of relevant LEAs to a very large extent. This includes the investigation and prosecution of ML and predicate offences, the confiscation of criminal proceeds, and TF investigations. The provided case studies also demonstrate that financial intelligence has been used to identify new targets in existing cases and in relation to asset profiling.

164. In terms of process, IMPA's Collection and Control Department is responsible for receiving and collecting all submitted reports and other sources of information. These reports are subsequently sent for analysis to the dedicated Research and Analysis Department. IMPA currently has 28 trained analysts. This department includes units dealing with strategic analysis, operational analysis and analysts assigned to the IFC.

165. The analytical process includes the review of the financial information with respect to all relevant entities, and the cross-checking of the information in the databases which IMPA has access to (see first box in this chapter). It aims at identifying additional entities, linkages to the criminal activity, as well as possible assets for confiscation. The analysis of IMPA's additional activities (e.g. request for information from FIs, ITA, foreign FIUs, etc.) are an integral part of the intelligence reports that IMPA disseminates to LEAs, spontaneously or upon request. These intelligence reports include all relevant factual information, an analysis and assessment sections, which includes details on the identified ML/TF suspicion and patterns, possible assets for confiscation and recommendations for future action. There are guidelines and work procedures in place to determine the scope of the information to be included in an intelligence report and the timeframe.

Box 9. **IMPA's structure and staffing**



Department	**Employees**
Information Collection and Control Department	11
International Department	6
Research and Analysis Department	28
Legal Department	8
Computing and IT Department	18
Headquarter, Administration & Knowledge Management	7
Sub-total	**78**
Outsourcing Services	
Data Entry Team	20
External IT Professionals and Services	7
Total (including outsourcing)	**105**

166. IMPA has designated teams for strategic and proactive analysis, which proactively-identifies new ML/TF patterns and trends. Potential ML/TF cases and

targets from such patterns are identified and disseminated to LEAs. As part of its strategic function, IMPA also looks into new risk areas, and works on projects with LEAs (See Box 10 below). The outcomes of these projects are used to identify new risk areas, typologies, issue red flag to reporting entities and other relevant stakeholders, and to identify new specific targets for investigation by LEAs. To do so, the team uses technological tools capable of processing and analysing of large volumes of financial information. Such tools include an alert centre, which identifies an ML/TF suspicion and directs it to the analytical team for further analysis; a module to monitor UARs based on key words (i.e. pre-identified risk areas); statistical and scoring tools are used to identify the most significant ML/TF suspicions. IMPA also uses advanced graph database and visualisation tools to support its operational and strategic analysis, especially for the mapping of ML/TF networks.

Box 10. **Examples of ML/TF Projects based on areas of risks conducted in 2013-2017**

Co-operation with INP - Governmental Corruption:

Project on Domestic PEPs (2 projects in 2016)

Co-operation with security agencies on TF intelligence targets:

Data Mining project (2013).

Co-operation with ISA:

Using Stock Exchange Members' reports (2015) - CTRs and UARs sent by Stock Exchange Members, the system scoring model found 14 entities having a high suspicion score.

Project on Internet Ventures (2016) - Internet ventures that were identified as suspicious according to Israel Securities Authority's list. The scoring model found two ventures having a high suspicion score.

Financial instruments:

Real Estate (2015) - The scoring model identified 16 entities having a high suspicions score.

Unusual Cash Activity (2016-2017) - The scoring model found 96 entities having a high suspicion score (i.e. natural persons who carry out unusual cash transactions).

167. In addition to its human expertise, IMPA conducts extensive analysis based on financial information using self-developed IT tools and statistical modules. IMPA developed an elaborate IT system with visualisation tools, data mining capabilities and in-house analytical software. The system was developed and is maintained by a dedicated team of more than 18 staff, specialised in information technology. IMPA's dedicated IT personnel work on a regular basis to improve both its infrastructure and software.

168. IMPA prioritises its analysis and dissemination based on the findings of the ML NRA (e.g. increased focus on cash, MSBs, tax offences), as well as priority areas and targets approved by the Implementation Committee (see IO.1).

169. Upon request from LEAs but also spontaneously, IMPA requests additional information from reporting entities in Israel and also information from foreign counterparts. As demonstrated in a number of cases provided by the authorities, this additional information assists LEAs in establishing ML or TF suspicions and the detecting financial networks and criminal assets (see the "D" case and the "F" case).

170. IMPA provided samples of its disseminations, which were found to be of a high quality. IMPA's dissemination is the product of IMPA's assessment of the information that it can access. As evidenced in a large number of case examples reviewed during the on-site, these intelligence reports often contribute to the identification of new connections, natural and legal entities, financial and real assets and financial transactions that were previously unknown to LEAs, but also of foreign financial transactions, bank accounts and assets located both in Israel and abroad.

Co-operation and exchange of information/financial intelligence

171. IMPA has a high degree of ongoing co-ordination, co-operation and exchange of financial intelligence with LEAs (including security agencies). This is most evident at the level of the Intelligence Fusion Centre and the eight investigative Task Forces, all of which involve officers from IMPA, INP and ITA. A number of case studies provided by authorities demonstrate examples of IMPA's contribution to the work of the taskforces – e.g. Checklist case (see IO.7), the SL case (see Box 10 above), but also a number of other cases reviewed by the assessment team. IMPA also participates at the highest level of AML/CFT co-ordination by being a permanent member of the Implementation Committee (see IO.1).

172. In addition to the work done at the task forces and the Implementation Committee, IMPA also collaborates with INP on a daily basis through INP's terminal located in IMPA's offices since 2014. The Director of IMPA also regularly meets with the head of INP to discuss new targets and align work plans. As a result, in 2017 alone there was a 12.6% increase in the number or requests made by INP to IMPA, and a 31% increase in the number of reports disseminated to INP in response to a request. Over a five-year period (2013-2017), the increase was 86% and 81% respectively.

173. Similarly, IMPA works closely with the ITA (in relation to fictitious tax invoices and other tax offences, and cash smuggling) and more recently with the ISA (project on the identification of ML suspicious indicators). With the amendment of the PMLL in 2016, ITA and IMPA can exchange information directly. ITA has been requesting information from IMPA since 2017, and significantly increased the number of cases involved in its requests in 2018. IMPA has also been proactively sharing information regarding tax offences with ITA (27 spontaneous disseminations in 2017).

174. IMPA also closely works with all supervisors, in support of their function to regulate, control and audit the reporting entities under their supervision and improve the overall quality of UARs. As such, IMPA disseminates periodic reports to supervisors, focusing on reporting entities' level of compliance, based on analysis and processing of financial information, internal criteria, and on a risk-based approach. The reports include, among others, quantitative and qualitative aspects of the reports filed by the reporting entities. The reports are sent to supervisors to assist with formulation of annual work plans regarding audits, control and regulation activities. IMPA also disseminates focused sectorial reports, which provide detailed information regarding the quality and number of reports including additional statistics. These reports assist also in the development of modules allowing for more focused supervision. IMPA provided information to assist supervisors in audit and enforcement activities on 287 occasions between 2013 and 2017.

175. IMPA and other competent authorities fully secure and protect the information they exchange and use. IMPA offices are located in a government building, secured and guarded on a round-the-clock basis. Visitors to IMPA are required to be accompanied by IMPA officers at all times. IMPA's database is protected by a number of safeguards and can only be assessed by IMPA officers through three-factor authentication: biometric information, smart card, and password. Dissemination of financial intelligence information is through secure systems. The legal duty of confidentiality (as per s.31 PMLL) applies to non-IMPA personnel as well.

176. IMPA engages in a wide range of international co-operation with its counterparts, through a number of informal channels (e.g. Egmont Secure Web) (see IO.2).

Overall conclusions on IO.6

177. **Israel has achieved a high level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

178. The assessment team based its conclusions on a variety of elements including: material provided by and discussions with relevant Israeli LEAs (INP, ITA, and ISA) and IMPA; discussions with members of the Implementation Committee (and its sub-committees), the head of the Intelligence Fusion Centre and officers operating in the task forces. The team reviewed numerous cases demonstrating that Israel investigates and prosecutes ML offences and undertakes parallel financial investigations, asset tracing, and confiscation (in reference to IO.8).

ML identification and investigation

179. Israeli LEAs are very focused on pursuing ML investigations and trace assets for confiscation. To a large extent, authorities in Israel identify a wide range of potential ML cases through financial intelligence originating from a range of sources including material developed by the IMPA, ongoing predicate criminal investigations, overseas requests for assistance and general law enforcement

intelligence obtained from operational deployments including, but not limited to, undercover operations and the interception of communications. IMPA has all the necessary IT tools and mechanism to identify developing threats/risks, criminal networks and potential ML cases, including these originating abroad. IMPA disseminates typology reports or case specific intelligence packages designed for adoption/consideration by law enforcement; the latter will include details of financial transactions conducted by or assets held by the relevant suspects and connected entities in order to assist with the parallel financial investigation.

180. At a national level, ML cases are often investigated by *Lahav 433* which includes a number of specialist taskforces (see table below). There are eight of these INP-led units, all of which incorporate officers from the ITA and IMPA and have ready access to the appropriate levels of legal advice and guidance from the SAO/DAO. SAO/DAO's guidance also includes the drafting of Letters of Request. The number of these taskforces and their compliment is sufficient for the goals and objectives they are tasked with, also taking into account the size of Israel and the overall ML risks. Two of the eight task forces (on MSBs and TF) have been created following the adoption of the NRA. These taskforces undertake the covert stage of the investigations, which is then handed over to "parent" units in the INP at the overt stage. The majority of the cases developed by the task forces are passed to the national units in *Lahav 433* within INP. The investigation team often enters into a Joint Investigation Team agreement with a relevant partner agency, such as the ITA.

Table 10. **INP's Task Forces**

Task Force	Areas of High Risks
Professional ML	Diamonds, cash, MSBs, cross-border crime, fictitious invoices, legal persons
Professional ML linked to organised crime	Real-estate, criminal organisations, BSPs and MSBs
Online gambling	Gambling, tax offences, cross-border crime
Corruption	Bribery and corruption (and relations to crime organisations), cash
Criminal organisations	Criminal organisations, international crime and MSBs
Ports and border crossing	International crime, legal persons, fictitious invoices
MSBs (currently being established)	MSBs, tax offences (direct tax and fictitious invoices)
TF	TF

Source: INP.

181. Investigations undertaken at a local level have the support of District Units that specialise in financial crimes. These district teams and the wider INP units also have the support of the HQ-based Financial Enforcement Teams, which also focus on parallel financial investigation generating outcomes (see in IO.8).

182. All LEAs involved in financial investigations receive a comprehensive training program (although not all LEA officers do). New LEA officers are also trained on financial investigations. The various training provided equips officers with the skills, knowledge and understanding required to undertake ML investigations. The training also ensures that all LEAs (i.e. INP, ITA, IMPA or ISA) understand the capabilities, contributions and benefits of working with partner

agencies. The courses are supplemented with regular continuing professional development (CPD) seminars, conferences and events provided by the Financial Enforcement Academy. The supplementary training ensures that changes in policy, case precedents, typologies and operating practice can be easily disseminated and understood. The courses include dedicated sessions delivered by the SAO. Delegates from both SAO and DAO attend the continuing professional development events. The approach taken in relation to financial training provides the best opportunity to embed effective, practical and relevant knowledge.

Box 11. **ML case successfully identified and investigated through parallel financial investigation**

The "Checklist" Case

Background – this is a complex professional ML case relating to the diamond industry, initiated by IMPA and investigated by the Task Force dedicated to professional money launderers.

Relevance to IO.6 – The case originated from a spontaneous dissemination by IMPA. IMPA spontaneously disseminated an intelligence report to INP. The report contained IMPA's strategic analysis based on a suspicion that an "underground" bank was being managed in the Diamond Exchange, raising serious concerns about a large-scale ML activity. In this specific case, IMPA identified new ML patterns and a professional ML scheme.

Relevance to IO.2 – As part of the investigation, IMPA sent 15 requests for information to five different FIUs (using the Egmont channel). Foreign FIUs provided in return intelligence on companies owned by the suspected individuals and their bank accounts, including associated transactions. This significantly contributed to the Task Force investigation. A number of requests for MLA were subsequently successfully executed.

Relevance to IO.7 – Professional money-launderers and fictitious invoicing are among Israel's areas of increased focus, due to the ML risk they pose. The dedicated Task Force used IMPA's intelligence report to open a joint investigation, made of INP officers and representatives from ITA and SAO. During the investigation, funds, diamonds and real estate properties were seized. The investigation resulted in indictments and convictions against several parties for ML (on the basis of s.3(a) and 3(b) of the PMLL).

Relevance to IO.8 (outcomes) – Over NIS 12 million (EUR 2.8 million) were confiscated. Confiscated property included real estate properties in a foreign country. In its decision, the court did not require the confiscated property to be directly linked to the crimes, and determined that it suffice that the confiscated property be of equivalent value to the proceeds of crime due to the indictments being for ML offences.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

183. Israel has a comprehensive governance structure to ensure that ML investigations are focused towards the threats outlined in the NRA as well as the objectives and goals of the country's national policies. *Government Decision no. 4618* of 2016 confirms that attacking illicit proceeds is a primary long-term

objective of Israel's fight against serious and organised crime. This *Government Decision* requires that all relevant LEAs and regulatory agencies work together to deliver on objectives drawn from the annual work plan approved by the Executive Steering Committee (ESC). To do so, authorities developed a high-level action plan that enables a co-ordinated and comprehensive approach to tackling the threats as set out in the NRA.

184. The Inter-Agency Implementation Committee (IC), which reports to the ESC, is the main working forum for governance of activity against ML threats within Israel. The ESC has four sub-committees covering a range of issues which would affect performance against the annual work plan (e.g. a sub-committee on intelligence, on operational co-ordination, on legal issues and on training). All investigative activities undertaken by the taskforces and the IFC are reviewed by this governance framework. This reviewing function extends beyond the initial tasking. It also aims at ensuring that the on-going investigation is delivering expected goals, that objectives are on target and that evidenced threats are still in line with the NRA and the wider national AML policies. Cases which no longer met the expected criteria are re-assigned. Task force resources also remain focused on targeted threats as tasked by the IC. An assessment of case divide between local and national level reveals that, in 2016, 25% of ML cases were investigated at the national level.

185. The picture at the local level is less certain. Whilst ML cases addressing national risk are not restricted to those investigations progressed by national teams, there is tension between the need to trigger value-based confiscation and the strict adherence to the national ML risk assessment. Some examples of how local/regional resources are deployed to address national risks are set out in Box 12 below. Local and regional resources do take into account opportunities to utilise ML or predicate offences that lead to confiscation wherever possible. An example provided concerned local INP commanders developing a ML investigation strategy with a district enforcement officer targeting, for predicate tax offences, those running prostitution syndicates in the Tel Aviv area in 2017.

186. The addition of an ML charge when wider predicate offending is being investigated is only permitted when the suspect has taken a clear additional step which supports ML activity. This in itself represents the most significant factor contributing to statistic of nearly four out of five ML cases being derived from self-laundering. By way of an example, this could include moving criminal proceeds to the bank account of a family member or buying a car using criminal proceeds and having the ownership in a third party name. On the other hand, cases where individuals are in simple possession of criminal proceeds derived from a predicate offence rarely leads to a ML charge. This approach cannot be confirmed on the basis of the statistics provided in section 3.3.3 on the type of ML offence being pursued. However, in view of the range and materiality of the cases provided, and the fact that most of them were not in fact investigated at the national level, it appears that the investigation of ML cases by local and/or regional investigative teams is broadly in line with country's risk profile.

Box 12. **Examples of ML cases investigated and prosecuted cross-referenced with the country's risk profile and location of investigative resources[23]**

The "Checklist" Case – Task Force investigation of a complex ML cases. See box 10 (fictitious invoices, tax evasion, diamond trading, the use of cash) [national investigation].

The "SH" Case – ML case developed by the IFC and investigated by the *Lahav 433* and the ITA (fictitious invoices, tax evasion, criminal organisations, legal persons) [national investigation]

Background – This case is about an Israel-based criminal organisation involved ML through fraud and tax evasion. The ML scheme was centred on short-term loans granted to traders with intentionally extortionate interest so to avoid paying income tax and VAT. Fictitious invoices and the use of legal persons were an integral part of the loan scheme.

Relevance to IO.7 – This case fully aligns with Israel's ML risk profile and demonstrates Israel's efforts to combat tax evasion, fraud and fictitious invoices, which were identified as high and moderate-high ML risk in the 2015 NRA. Over a period of one year, offenders granted 17 loans to six different individual and received in return an amount totalling NIS 13.8 Million/EUR 3.2 million (principals and interests). They later issued fictitious tax receipts to borrowers totalling NIS 25 million (EUR 5.8 million), and recorded these fictitious invoices in their books as legitimate expenses. Borrowers paid the principal and the interest payments in respect of the loans by checks. The investigation revealed that a secret account (for the deposit of these checks) was opened in the name of a shell company. The case also demonstrates effective sentencing. See also Table 16.

Outcomes – Over NIS 4 million (EUR 935 000) were confiscated, including funds in an MSB account, vehicles and a luxury watch. However, the defendant appealed the verdict and the confiscation proceedings are still awaiting the court's decision.

The "512" Case – ML case investigated by *Lahav 433* (criminal organisations, drugs trafficking, international crime) [national investigation].

Background - This case is centred on two major criminal organisations in Israel, involved in an international drug trafficking ring.

Relevance to IO.2 – This case requires a number of actions to be taken to trace assets abroad – this included: IMPA sending requests to FIUs of the relevant countries (this led to information being produced on assets in three foreign countries), an application via CARIN (no result), and a number of MLA requests (which led to information being produced on bank accounts located foreign jurisdictions). Overseas activities also included locating suspects, arrests, extradition and witness protection requests – in 11 countries.

Relevance to IO.7 – This case fully aligns with Israel's ML risk profile and demonstrates Israel's longstanding efforts to combat organised crime (which was an area identified as posing a high threat of ML in the 2015 NRA). Lahav 433 led the investigation of this case, involving police officers from national

23. i.e. local/regional or national level [shown in brackets]

and district units. The investigative team collected evidence that confirmed that the suspects involved in drug trafficking operations were also engaged in the laundering of the generated proceeds (totalling an estimated tens of millions of NIS).

Outcomes – In 2015, 18 indictments were filled for a number of offences, including ML (s.4 PMLL) against members of the criminal organisations and their relatives. Some proceedings are still ongoing. The defendant charged with ML was convicted and sentenced to 18 months imprisonment and a fine in the amount of NIS 1 million (EUR 234 000). NIS 8.1 million (EUR 1.9 million) were also confiscated (of which NIS 3.6 million (EUR 841 000) were designated for the forfeiture fund).

The "B" Case – Tel Aviv District Fraud Unit investigation (fraud, international crime) (local/regional investigation) See box.6 relating to the use of financial intelligence to trace criminal proceeds.

The "HL" Case – INP/ITA *Yahalom* Unit investigation prosecuted by the Northern District Attorney's Office (criminal organisations, tax evasion, use of cash, money service businesses) (local/regional investigation].

Background – The case involves a criminal organisation extorting monies from contractors and businesses under the guise of "guarding services".

Relevance to IO.1 – The case addresses some of Israel's high-risk areas - MSBs and criminal organisations- through a joint investigation undertaken by local investigators in conjunction with regional ITA resources.

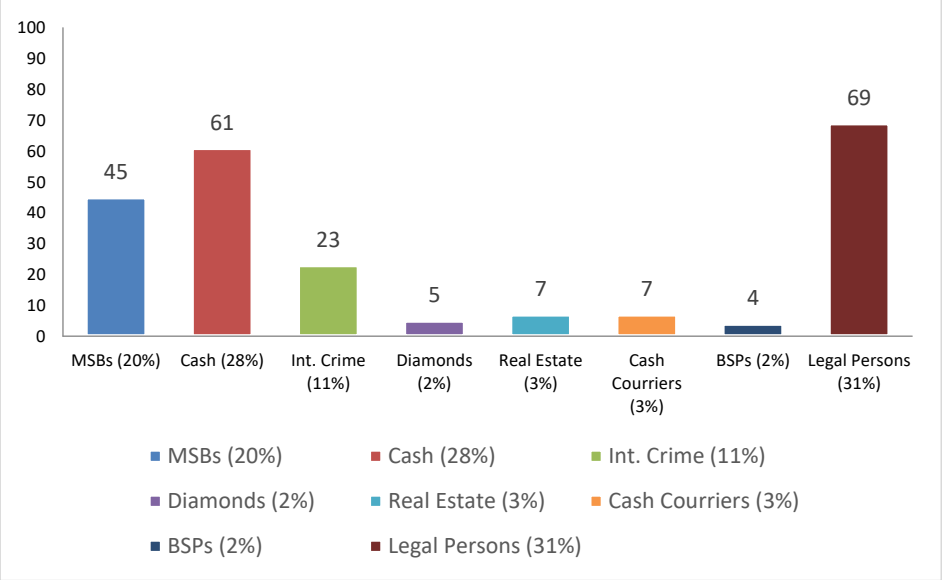
Relevance to IO.7 – The case demonstrates effective co-operation at local/regional level in investigating ML activity derived from criminal organisations. The investigation involved a significant review of communications data, funds flows and business documentation. Testimony was collected from 229 witnesses. A wide variety of investigation techniques was deployed against the heads of the criminal organisation. Additionally, alternative measures were called upon to enhance the disruptive impact of the investigation as the appropriate authorities, after liaising with the investigation teams, revoked the security licenses of the company involved in the criminal activities.

Outcomes – In February 2017, indictments were filed which included charges relating to PMLL and CCOL. Assets to the value of NIS 30 million (EUR 7 million) are subject to provisional seizure pending prosecution.

187. A number of case examples were provided under the "diamond" typology, which demonstrated that diamond trading was used as a cover for an underground banking system laundering millions in cash. This type of investigation appears to be at the expense of investigating cases in which the proceeds of the criminal activity are already within the financial systems; the exception to this being tax offences (including VAT, income tax and other related taxes). This could be explained by the way authorities designed their risk assessment, namely that it does not look at the laundering of proceeds that are already in the financial system as a specific typology. In practice, there are a number of cases where criminal proceeds are, and always have been, in the financial system, and these are covered as part of wider typologies (e.g. fraud and, potentially at least, fictitious invoices). Thus, despite what could appear as being an over focus on cash-related ML

investigations (which in any case would be in line with the country's risk profile), it can be concluded that ML typologies within the risk assessment are generally adhered to when cases are adopted and investigated.

Figure 1. **ML Cases in accordance to ML Typologies 2014-2016**[24]



Source: SAO

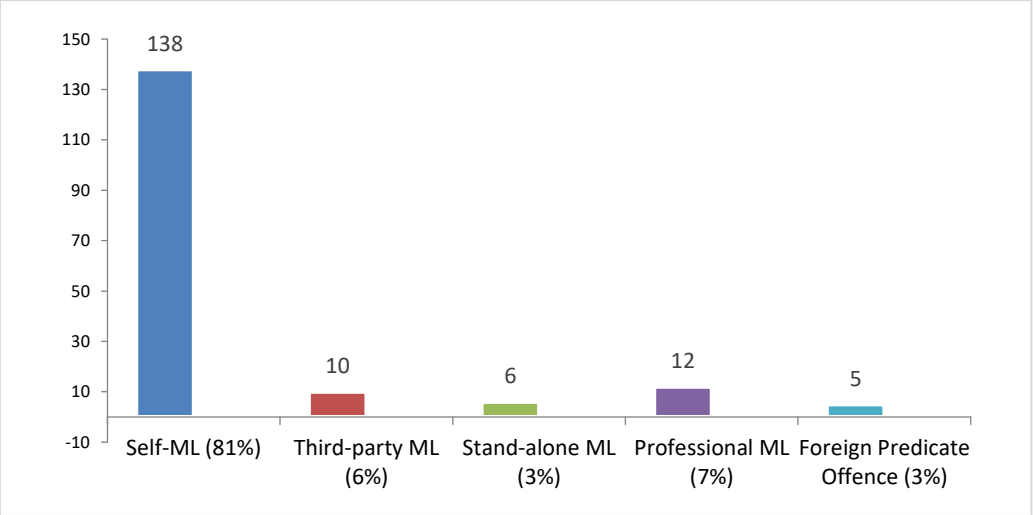
Types of ML cases pursued

188. To a large extent and broadly in line with the NRA, Israel investigates and successfully prosecutes all types of ML offences, including cases of stand-alone, third party ML and ML involving foreign predicate offending. However nearly four out of five cases of ML prosecutions concern self-laundering, the reason being that self-laundering cases often allowed authorities to also pursue value-based confiscation, which is not available under the confiscation provisions across the breadth of general predicate criminal offences. The data in the chart below identifies the types of ML activity investigated by Israel. However, professional ML is a flavour of third-party ML activity,[25] rather than a specific ML type. When considering the use of self-laundering and the combination of third-party laundering and professional ML activity, it appears that there is a lower number than anticipated of stand-alone ML prosecutions. There were only six instances of charges related to stand-alone ML identified between 2014 and 2016.

24. In most cases there is more than one typology assigned to an indictment. It should be noted that all typologies also include the use of the financial system. The use of MSBs could indicate several financial transactions, including cash checking, international wire transfers, bank transfers and cash.

25. See report on Professional Money Laundering discussed at Plenary in Paris, June 2018.

Figure 2. **ML Charges according to ML Type 2014-2016**



Source: SAO

Box 13. **Examples of investigation and prosecution by types of ML**

The "BI" Case - foreign predicate offence

Background – Authorities in Country A suspected that a criminal that had indicted domestically had managed to transfer some of the illegal proceeds to Israel, namely into the mother's bank account.

Relevance to IO.2 – This case was initiated by the MLA request received from Country A and investigated domestically by the *YALAC* (INP). In their MLA request, authorities of Country A requested investigative activities and the freezing of funds located on the mother's bank account. See IO.2 – Box 23

Relevance to IO.7 – Because of the urgency of the situation, YALAC's investigation centred rapidly on the mother's account. An estimated NIS 1 million (EUR 234 000) were frozen during the investigation. Israeli authorities subsequently reached a settlement with the mother (who admitted making false disclosures in transferring the assets). The conviction was made on the basis of s.3(b) of the PMLL. The mother received a suspended prison sentence and a fine of approximately EUR 57 000.

Relevance to IO.8 (outcomes) – Over NIS 1.9 million [USD 650 000] were confiscated in Israel, in addition to the USD 1.25 million confiscated in Country A.

Other relevant example: Checklist case - professional money launderers case

189. When compared to other jurisdictions of a similar size and level of economic development, Israel prosecutes a high number of individual cases involving legal persons. However, there appeared to be issues with subsequently convicting those within this group in a timely manner.

190. Delays in concluding prosecutions can be explained by the country's judicial system, which prioritises those cases in which a defendant is in custody.

As a consequence, criminal proceedings involving legal persons take many years to conclude (since there are no persons in custody). Closer examination of the statistical data for 2014 revealed that of the 34 instances in which the prosecutions of legal persons had commenced, only 8 cases had been convicted and a remaining 26 (25 of them were all part of one case) were still ongoing at the time of the on-site visit; however, shortly after the on-site visit 25 out of the 26 were convicted, in that one case. No cases had led to acquittals. All outstanding cases related to the activities of NPOs.

Table 11. **ML investigations, prosecutions, and convictions in ML cases**

Number	Investigations			Prosecutions commenced			Convictions		
	Cases	**Natural Persons**	**Legal Persons**	**Cases**	**Natural Persons**	**Legal Persons**	**Cases**	**Natural Persons**	**Legal Persons**
2014	327	681	56	31	71	34	33	36	8
2015	669	620	24	56	127	53	30	47	11
2016	349	423	41	50	94	44	33	62	7
2017	316	517	16	62	153	58	38	54	29

Source: LEAs, SAO

191. Given that that number of legal persons subject to such criminal proceedings appears to be growing, the delay in finalising the prosecution element of the process is not likely to remedy itself naturally. As such, the delays have the potential to weaken the effectiveness of Israel's response to the NRA and the wider FATF standards as they apply to this issue. Presently two thirds of all ML indictments lead to convictions, if those cases which incorporate some form of plea bargain are included, and this level of success contributes well to the overall characteristics of an effective system. However, ultimately delays in the prospect of conviction and punishment for legal persons have the potential to undermine this impact and demonstrate a significant level of dissuasiveness. Authorities indicated however that there is an action plan in the pipeline that would aim at addressing the issue of timelines of criminal proceedings (and thus outstanding caseload) in 2019.

Effectiveness, proportionality and dissuasiveness of sanctions

192. Criminal proceedings for ML offences can result in punishments that range from a custodial sentence or a fine or both. Custodial sentences, depending on the specific ML offence, range from five years up to ten years, with fines ranging from eight times the maximum statutory amount for a fine through to 20 times the maximum statutory amount. The maximum threshold is set by reference to the s.61(a)(4) of the Penal Law; at the date of this report that sum is NIS 226 000 (EUR 52 800).

193. The determination of the exact penalty attributed by the court to the ML conduct was difficult, as often this was merged with the penalties handed down for other offending. However, the few cases in which penalties had been clearly allocated to the ML activity by the sentencing judge are aligned with the wider case studies and the penalties that defendants in those cases had received.

194. To a large extent, courts impose moderate sentences in relation to ML offences, and have successfully imposed a range of custodial penalties, fines and

periods of probation and/or community service. The sentences can be estimated to normally be in the range of 1.5 to 3.5 years for the ML activities. There were case studies supplied (see table below) which demonstrate penalties at the highest end being imposed but also some with penalties below the range outlined in the previous sentence. The maximum period of community service that a court may issue is six months. The high level of community service shown for 2016 is due to a single case in which ten defendants were issued with a 6-month community service order each (60 months in total).

Table 12. **Sentencing Statistics**

	Fines (in NIS)	Imposed prison sentences (average in months)	Suspended prison sentences (average in months)	Community service (total in months)
2013	17 408 235	39.8	16	4
2014	16 834 660	56.3	26.3	24
2015	17 711 000	54.45	12.93	18
2016	9 378 537	41.94	14.2	83
2017	6 210 807	36.7	13	12

Source: LEAs, SAO

Table 13. **Examples of sentencing in ML cases (under the PMLL)**

Case	Offences	Sentences imposed
"G"	Several economic offences, incl. s.3(a) of the PMLL and s.3 of the CCOL	Punishment scale set for 2.5-4.5 years imprisonment (total). Plus EUR 46 550-93 100 (NIS 200 000 – 400 000) fine
"LR"	ML, fraud and tax offences	6 years imprisonment – of which 18-40 months for ML only Plus EUR 23 275 (NIS 100 000)
"Glam"	ML and tax offences	10 years imprisonment and 18 months' probation (total) Plus EUR 1 163 745 (NIS 5 million) fine
"HA"	ML – various offences including non-registration as an MSB and ML s.3b of PMLL for intentionally not reporting	3 years of imprisonment, increased by the Supreme Court in appeal to 4.5 years. Plus EUR 174 562 fine (NIS 750 000) and confiscation of EUR 861 171 (NIS 3.7 million)
"NA"	ML – s.(a) and s.3(b) PMLL (case of third party ML)	Legal person convicted for ML and sentenced to a fine of EUR 23 274 (NIS 100 000)
"SH"	Corruption	8 years imprisonment Plus confiscation of EUR 1 027 354 (NIS 4 414 000) including property and funds.

Source: SAO, ITA

195. The majority of sentences are at the lower end of the penalty scale. This could be as a result of the higher percentage of self-laundering offences. Many sentences are being amalgamated (thus representing penalties from both ML and predicate offences) making it difficult to accurately assess the dissuasiveness and effect of the sentences issued in Israel. In order to evaluate the sanctions related to ML offending correctly and to publicise the consequences and seriousness of ML offending, it would greatly assist Israel if the judiciary were encouraged to clearly

identify the exact sanction handed down in ML convictions when prosecuted alongside other criminality. However, in general, sanctions are assessed as being broadly dissuasive based on the information provided by prosecutors involved in such cases and their estimate of what proportionate of the total sanction relates to the ML offences.

Use of alternative measures

196. Israel pro-actively pursues ML investigations and prosecutions when it is the appropriate measure to adopt. However there are a range of measures which Israel deploys when ML prosecutions are unavailable or not the appropriate disposal (e.g. for lack of sufficient evidence). When the ML offence cannot be included in the indictment, authorities prosecute for other offences (preferably predicate offences and tax offences).

197. There are multiple case examples of the application of these alternatives which range from the utilisation of administrative sanctions through to referrals to supervisory bodies and potential of the revocation of operating licences.

> Box 14. **The "O" case - action by an administrative sanctions committee**
>
> This was an INP-led ML investigation on a violation to s.3(b) PMLL. The defendant brought small amounts of cash into Israel, thus avoiding declaration. The SAO decided not to prosecute due to a lack of sufficient evidence. The case was transferred to customs (ITA), and brought in front of the administrative sanction committee, which imposed a sanction of NIS 200 000 (EUR 46 700) on the defendant.

198. In instances that arise as a result of an offender being outside of Israel or cannot be located, LEAs can, if assets are known to be associated with the offending, take civil action under section 22 of the PMLL (see case example in IO.8 - Box 15).

Overall conclusions on IO.7

199. **Israel has achieved a substantial level of effectiveness for IO.7.**

Immediate Outcome 8 (Confiscation)

200. The assessment team based its conclusions on the same variety of elements as those listed in IO.7, with a focus on the investigating and prosecuting authorities. The team also visited the Jordan Inland Crossing Point and conducted a number of interviews the relevant officers.

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

201. Israel clearly has the confiscation of criminal proceeds and instrumentalities as a policy objective; to a large extent this is delivered upon.

202. The Asset Recovery and Forfeiture Management Office (ARFO) set up in 2014 is responsible for managing the assets that are seized and, once the court has

ratified the confiscation of those assets, their realisation. In so doing, it ensures that LEAs are freed up from trying to preserve the value of assets seized and ensures that, where necessary, the appropriate specialists are used to confirm or preserve values.

203. The national governance platforms that originate from *Government Decision no. 4618* (see IO.1) apply to confiscation as much as they do to ML activity. Furthermore, authorities dedicated an entire section of the high priority action plan to confiscation issues. The implementation of this plan is monitored by the IC. An example is the reduction in the thresholds for reporting cross border movements of cash (see below).

204. Additionally the various relevant authorities adopt a top-down thinking on the issue by ensuring each agency has clear, current policies on confiscation procedures and that training on the subject is embedded across their respective organisations and work plans. The strategic approach is underpinned by regular conferences which seek to explore best practice, future goals and current effectiveness/performance in the confiscation arena; these events are known as the "Joined Hands" interagency conferences.

205. However, there is a self-acknowledged gap in the legislation that prevents the wholesale adoption of an equivalent value-based confiscation. The confiscation of equivalent value is restricted to ML cases and selected other predicate offences. Many of these other predicate offences are considered to be high risk offences according to Israel's NRA. However, fraud, which is one rated as high risk in the NRA, does not, if pursued as stand-alone predicate case without the related ML charges, trigger the value-based confiscation regime. Israel has identified this as a matter which requires attention and is moving to overhaul the confiscation regime. New legislation is before the Knesset and is, if normal progress is maintained, likely to come into force towards the end of 2019.

206. In order to overcome the challenge represented by the lack of a general value-based confiscation regime, authorities make use, when appropriate, of ML offences prosecuted in tandem with wider predicate offences. Authorities underlined that this approach is taken only when the actions of a suspect are considered to justify an ML charge (e.g. when the acts forms concealment, when the financial system is misused etc.) and not as a mechanism to activate the more far reaching confiscation regime that then becomes available. No data was available to confirm this view. However this would go some way to explaining the high percentage of self-laundering cases which progress to prosecution (see IO.7) although it should be stressed that Israel's numbers are not significantly out of line with data that has been provided in other recently undertaken assessments (including those that do have value based confiscation regimes for all types of crime).

207. Israel's approach to the confiscation of instrumentalities is in line with the FATF standards. Whilst various administrative actions[26] are taken in relation to criminal proceeds, either in monetary form or more general asset form, these are

26. See examples set out in Criminal Procedure (Arrest and Search) Ordinance, Prohibition on Money Laundering Law, Struggle Against Organised Crime Law and Dangerous Drugs Ordinance.

generally triggered as reactive measures as result of other actions (e.g. failure to declare cross-border movements of money or when, following a criminal investigation, a criminal justice disposal is not considered appropriate).

208. There is some concern on the lack of a wide-ranging civil (non-criminal conviction based) assets recovery regime. Such a regime would allow for the proactive pursuit of criminal property without the need for a complex investigation into the conduct of a suspect; with civil recovery regimes being predominantly *in rem* and focused on assets which are believed to be derived from criminal conduct. This approach has the potential to increase the already significant performance delivered by Israel in relation to the value of proceeds deprived from criminals. Currently the civil forfeiture regime restricts recovery to instances in which assets are linked to ML and a specified suspect cannot be found or is not permanently resident in Israel.[27]

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

209. Israel demonstrated the implementation of the confiscation policy objectives by reference to a range of statistical data. Israel is achieving effectiveness on this to a large extent.

210. The data provided in relation to the effectiveness of the confiscation regime, which includes the utilisation of the tax system, demonstrates considerable effectiveness. This is further evidenced by the increasing figures over the years which confirm the various authorities' policies and actions for prioritising confiscation.

Table 14. **Total sum of property taken from criminals (in EUR)**

	2013	2014	2015	2016	2017
Requested confiscation	24 822 200	39 470 900	126 977 000	53 410 700	59 142 900
Seizure made	70 758 800	124 318 000	157 689 000	175 976 000	224 175 000
Property, instrumentalities, and proceeds of crime taken from criminals					
Confiscation	17 009 700	12 014 200	18 193 500	63 631 400	11 920 500
Tax	52 124 000	30 570 500	97 092 700	43 527 400	23 521 500
Fines	5 718 590	2 294 140	1 940 130	39 941 700	19 624 500
Total	**74 852 200**	**45 508 900**	**117 226 000**	**147 101 000**	**55 066 600**

Source: SAO.

211. Seizures in one year may not become subject to a confiscation request (and reflected in the confiscation statistics) until several years later. Fines are not relevant to the overall picture of Israel's effectiveness as confiscation is in addition to criminal sanction; although fines are often taken from the sums initially seized. Data also shows that a substantial percentage of assets made subject to an initial seizure is subsequently made subject to a confiscation request by SAO. About 90% of the assets initially seized during investigations are subsequently made subject of requests for confiscation. Courts generally grant orders for confiscation that amount to 75% of the confiscation requests. That 75% figure includes any

27. See s.22(a)(1) and a(2) of the PMLL.

amounts recovered or deprived from criminals by way of tax and victim compensation schemes.

212. Israel also takes action to confiscate assets derived from predicate offending abroad when appropriate to do so. An example is set out in the following case study.

Box 15**. The "MB" case - civil action pursuant to s.22 PMLL**

The defendant had been extradited to a foreign country, where he was convicted for fraud. Before being extradited, the defendant signed an agreement with Israeli authorities admitting having purchased property using criminal proceeds. After the extradition, the court in Israel ordered the confiscation of that property in accordance with s.22 PMLL.

213. The figures for seizures (see table above) represent, on the whole, assets directly linked or assets that can be traced back to the criminality, and thus indirectly represent the proceeds of the criminality. However, in some cases seizure cannot be obtained. This is the case when the offender (suspect or defendant) benefited from crime and then spent the proceeds, enabling them to retain, without diminishing, legitimate income. That said, seizure can be obtained on contents of bank accounts through which illicit funds can be shown to have flowed. This interpretation extends to cash as authorities can seize the equivalent value of cash and not simply the original cash criminal proceeds. The high levels of assets actually seized under provisional measures do reflect the effective use of the combination of approaches available in Israel under the PMLL and the CPO (see R.3).

214. The provisions within the legal framework currently do not address cases in which assets are identified post-conviction (or post the completion of the confiscation proceedings) unless those assets are specifically linked to the original criminal activity. When assets are held under management of the ARFO information can be asked of a suspect or defendant to ensure the effective management of the property. The ability of ARFO to secure information about assets not known to the relevant authorities or subject to current seizure is limited by the defendant's willingness to co-operate, as there is no incentive for them to reveal such property. It is accepted that the approach adopted by Israel enables a joint investigation into assets that could be recovered. In practice, it appears as though the majority of the burden falls to the law enforcement authorities; when the approaches of other jurisdictions are considered this could be a wasted opportunity in terms of rationalising the use of investigative resources. However this does not impact on the effectiveness the ARFO's ability to manage the assets it is assigned.

215. IMPA provides high-quality intelligence packages relating to parallel financial investigations to all law enforcement agencies to ensure the best possible outcomes in the confiscation arena. However, there is some concern that the resources available to IMPA led to a need, particularly for INP, to triage requests of the FIU. This limits access to all forms of financial intelligence/evidence and

therefore Israel's ability to successfully demonstrate effectiveness to a very large extent.

216. Overall, the general ability of the competent authorities to access financial intelligence and evidence results, and theoretically even more so when combined with the restrictive investigative abilities of the ARFO, in some limits to the effectiveness of the confiscation regime. This risk is further underpinned by the inability of Israel to seek international assistance in relation to certain aspects of confiscation activity and action due to its lack of reciprocal arrangements for value based confiscation.

217. There is also some concern about the length of time confiscation proceedings are taking to work their way through the court system. This has the potential to have a significant impact on victims and the rights of legitimate third parties. Given the measures that can be utilised to compensate the majority of victims early in the process (which is by way of judicial approval), this is considered to be a minor issue.

218. Israel does, to a large extent, discharge its international responsibilities in relation to proceeds of crime. Israel takes action to address the recovery of the proceeds of crime which has been acquired through foreign predicate offending or by taking action to trace and recover proceeds which have been moved to other countries. The assessment team were provided with a range of case studies in which both aspects of this part of the core issue were addressed. As previously mentioned, the lack of a simple value based confiscation system does hamper Israel to some extent; however Israel finds practical and impactive solutions to this defect.

219. Israel has taken positive action to address some of the most significant impact of crimes by way of compensating victims. Israel created a fund for the victims of human trafficking which is sourced from proceeds recovered in confiscation proceedings in slavery and human trafficking cases. The administration of the funds permits the payment of specific sums to victims if any compensation sums previously awarded to them in criminal proceedings cannot be fully recovered. The compensation payments are available to those who have remained in Israel or, at the time of the compensation order being made by the court, are abroad.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

220. Israel has highly effective measures to combat the cross-border movement of currency and bearer negotiable instruments that are falsely or not declared. These measures are applied to a very large extent.

221. The enforcement of the declarations regime is undertaken by way of intelligence, profiling, specialist resources (e.g. dog units) and risk testing. Cases are progressed quickly and efficiently with the overwhelming majority resulting in administrative sanctions. Only one case, from the Jordan Inland Crossing Point, in the last three years was subsequently subject to a criminal prosecution. The team carried out an onsite visit of the Jordan Inland Crossing Point to verify risk testing, the deployment of specialist resources and training provided to the staff

being deployed to enforce the declarations regime. The on-site visit also included interviews with the relevant officers.

222. Amendments to the PMLL which came into force in December 2017 significantly lowered the overall threshold for the declaration of cash at the border to NIS 50 000 (EUR 11 680). At specific designated land border crossing points, the threshold has been lowered to NIS 12 000 (EUR 2 800). This two-tier threshold reflects the risks Israel identified in its NRA. However, given the significantly lower thresholds, Israel will need to continue to ensure that sufficient resources are applied to border controls to ensure effective monitoring and compliance with the lower threshold declaration requirements.

Table 15. **Cash Declaration Detections**

Increase in activity pre- and post-PMLL amendments

Year	Jordan Crossing	National Cases	Total - Sum of seizure (NIS/EUR)	Total -Sum of financial sanctions (NIS/EUR)
2014	4	142	26 849 924 / 6 274 174	1 773 391 / 414 398
2015	6	144	15 475 387 / 3 616 221	2 230 964 / 521 322
2016	6	149	12 692 156 / 2 965 848	4 629 551 / 1 081 813
2017	4	91	5 700 000 / 1 331 951	792 000 / 185 071
2018 (to 22 March)	30	70	4 705 803 / 1 099 632	989 114 / 231 132

Source: ITA.

223. Historically the number of cases derived from cross-border cash cases demonstrates a strong effectiveness in relation to this issue and reflective of the overall threat. The drop in national performance in 2017 is due to a higher number of specialist cash dog units being replaced during that year and the need for the handler to undertake the training alongside the newly recruited K9 unit thus reducing operational deployment time. As of the time of the on-site visit, the competent authorities were taking a less punitive approach to breaches of the cash declaration procedure whilst the travelling public becomes aware of the lowering of the threshold for cash declarations. However, instances of deliberate concealment are still addressed in a robust fashion by way of financial penalties applied to the falsely and undeclared cash. There are clear information boards at border points which set out the legal obligations to declare cash and negotiable instruments. Most recent case studies already demonstrate that sanctions are likely to be effective, proportionate and dissuasive. As mentioned above, Israel will need to ensure that sufficient resources are continued to be allocated to ensure effective compliance with the lower threshold reporting requirements.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

224. Statistically there is a clear upward trend in provisional seizures in preparation for the range of confiscation outcomes in Israel. This is clearly as a result of the combined efforts of the investigating authorities and prosecutors. Confiscation is considered an integral part of financial enforcement and accordingly it is one of the issues to be promoted according to the NRA's action plan.

225. Data shows that around 70% of assets subject to provisional measures are eventually subject to confiscation (by whatever regime or process, including fines and taxes). When addressing the NRA risks the assessment team considered both predicate offending and typologies in the same manner that that NRA does but restricted the sums to those that are purely confiscation results. Data relating to confiscation arising from predicate offending is set out in table 16 below. It should be noted that some of the detail varies from similar information set out in table 14 insofar as this data is more recent and takes into account delays in finalising elements of the confiscation process due to e.g. appeals. The data available does not address the highest risk predicate offence fully, as tax offences were not classed as predicate offences until October 2016, but it is clear that all elements of predicate offending within the NRA are addressed.

Table 16. **Criminal confiscation according to risk – not including taxes and fines (2014-2016) in EUR**

	Sum Confiscated	Sum Requested	Sum Seized
S.3(b) PMLL	11 343 095	22 273 809	55 070 238
Other	690 684	4 761 429	11 719 761
Gambling	8 035 646	17 358 337	19 791 381
Fraud	61 196 454	136 973 391	173 858 372
Fictitious Invoices (and tax offences post Oct 16)	25 714 988	76 095 093	100 333 673
Extortion and Criminal Organisations	2 042 175	14 911 436	17 025 283
Drugs	5 542 600	14 900 248	15 985 248
Bribery and Breach of Trust	3 528 096	15 979 513	112 221 518
Total	**118 093 738**	**303 253 259**	**506 005 474**

Source: SAO

226. Whilst Israel positively drives forward confiscation of criminal proceeds, by whatever means is available to it within its current legal framework, it is harder, as described above, to map that effectiveness and performance across to the NRA. However, as commented upon in IO7, four out of five cases are self-laundering (see Figure 2 in IO.7) and this approach is often used to trigger value-based confiscation. Whilst this may be seen as having a negative effect on the effectiveness of IO.7, it is also a positive for IO.8 as the approach enables the range of typologies within the NRA to be addressed (see Figure 1 in IO.7). It is accepted that there is no data on the number of confiscation orders secured. However, it is a justifiable conclusion to assume that self-laundering cases do progress to confiscation when it is suggested that a primary purpose of pursuing self-laundering charges is to trigger confiscation. It is therefore concluded that Israel does produce confiscation results that are consistent with the ML NRA to a very large extent.

Overall conclusions on IO.8

227. **Israel has achieved a high level of effectiveness for IO.8**

.

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

Israel has achieved a high level of effectiveness for IO.9.

a) Israel has developed a wide range of effective instruments and mechanisms to combat terrorism and terrorist financing in all its aspects.
b) Different types of TF cases are prosecuted and offenders convicted. These cases are consistent with Israel's TF risk profile and include TF cases on the collection, movement and use of funds, as well as TF cases that did not involve terrorism charges. These cover a spectrum of TF typologies: cross-border smuggling, charities/NPOs and voluntary contributions, trade-based TF, money transfer mechanisms, and supposedly legitimate business activity. *Shin-Bet*'s and the other security agencies' proactive efforts are effective in disrupting terrorism at the early stages, which curtails a large number of TF investigations and renders prosecution for TF unnecessary.
c) Between 2013 and 2017, 37 cases resulted in convictions for one or more TF offences, involving 26 natural and legal persons. There are some delays in TF prosecutions when the defendants are not in custody.
d) TF cases are well identified and investigated, through a comprehensive legal, institutional and operational framework. Case studies also showed that Israel identifies the specific role played by the terrorist financier. *Shin-Bet* leads on counter-terrorism and TF intelligence and is the main source of TF investigations, while INP leads on formal investigations. Both have adequate resources and manpower for TF investigations, and both have designated units and teams are in place to tackle TF. IMPA also plays a key role in identifying TF cases for investigation.
e) The investigation of TF is integrated with, and used to support, national counter-terrorism strategies and investigations. This includes the designation of terrorist organisations and terrorist support networks. Counter-terrorism and CFT have been given the highest priority. The counter terrorism strategy is formulated from the highest echelons of the government, and the national policy on evolving risks is reviewed at the highest levels.
f) Israel applies criminal sanctions in criminal cases which are effective, proportionate, and dissuasive, ranging from prison sentences, to suspended

sentences, fines and confiscation. The penalty scale for the TF offence is between two to five years imprisonment.

Immediate Outcome 10

Israel achieved a substantial level of effectiveness for IO.10.

a) Israel implements targeted financial sanctions (TFS) for TF without delay. Israel has demonstrated its ability to implement TFS within the context of UN designations pursuant to UNSCRs 1267/1989 and 1988, domestic designations, and in relation to international requests.
b) The National Bureau for Counter Terror Financing (NBCTF) in the Ministry of Defence leads and co-ordinates the designation process. The Bureau has overall responsibility for co-ordinating national CFT enforcement policies, and works closely with *Shin-Bet*, who initiates most domestic designations, as well as INP, IMPA, and the security agencies. Israel has the necessary mechanisms for identifying targets through this co-operation.
c) Co-operation and co-ordination of operational matters on NPOs between authorities is strong (including sharing of the ICA's database with the ITA) but the overall jurisdictional response to NPOs is not comprehensively co-ordinated.
d) Israel has established a registration and supervision framework covering the NPOs most at risk of TF abuse.
e) The ICA is a proactive registrar and supervisor and its approach contains strong elements which mitigate the risk of TF abuse (including attention to donors). It focuses significant attention on mitigating risk in general through improving the governance, internal controls and transparency of NPOs, including financial controls on incoming funds and disbursements. On-site inspections appear to be good quality. Nevertheless, the overall volume of supervision needs to be increased (as does the use of sanctions), the approach does not include a TF focused risk-based approach and there is some shortfall in the number of staff.
f) The ITA is also proactive in relation to NPOs; it holds substantial information and has a positive role in increasing standards and preventing misuse of NPOs.
g) The positive focus and results by IMPA, LEAs and the SAO referenced in other IOs and in depriving terrorists of assets and instrumentalities also applies in relation to NPOs.
h) Israel effectively deprives terrorists, terrorist organisations, and terrorist financers of their assets and instrumentalities related to TF activities. A large amount of funds and property have been frozen, seized, and confiscated. Mechanisms include seizure and confiscation orders following domestic designations and through criminal investigations and convictions.
i) The measures taken by Israel are largely consistent with the overall TF risk profile.

Immediate Outcome 11

Israel has achieved a moderate level of effectiveness for IO.11.

a) Israel has implemented comprehensive and effective counter-proliferation finance targeted financial sanctions with regard to Iran, which are implemented without delay. The Sanctions Bureau, in the Ministry of Finance (MoF), co-ordinates efforts relating to PF sanctions and the accessibility of the information of sanctions against Iran to the public and business sector. The Sanctions Bureau works closely with Ministry of Foreign Affairs (MFA), ITA, INP, IMPA and the security agencies.
b) Legislation in March 2018 has further enhanced the technical requirements for TFS relating to PF without delay, including relating to the DPRK which was not previously covered under the PF-TFS regime. However, the legislation contains discretion for the Minister of Finance to permanently adopt the automatic designations from UN.
c) The competent authorities have taken a number of effective measures to ensure compliance from FIs/DNFBPs with regard to their PF-TFS obligations relating to Iran.
d) Up to the time of the on-site visit, Israel had not implemented specific requirements on targeted financial sanctions on proliferation financing related to DPRK since these requirements only came into force during the on-site visit. The compliance programmes for FIs, DNFBPs, and supervisors which were in place to ensure implementation of PF-TFS obligations relating to Iran, were not yet applicable with regard to DPRK. This is mitigated by the fact that most FIs and some DNFBPs screen customers and transactions against all international lists, including those relating to DPRK.
e) Given the comprehensive prohibitions against Iran, which are well understood and are a priority for FIs, and the trade restrictions and limited exposure relating to DPRK, no funds or other assets of designated persons and entities have been identified. Israel demonstrated case examples where trade sanctions and customs interventions were applied.

Recommended Actions

Immediate Outcome 9

a) Israel should implement ways to speed up the court process to prosecute TF when the offenders are not in custody.

Immediate Outcome 10

a) Although the issue does has not hindered effectiveness, Israel should address the technical gaps in the designation framework so that, in particular, Israeli citizens and residents can be designated under UNSCRs 1267 and 1373, and so that the MoD does not have discretion not to make the automatic designations from the UN permanent.
b) A mechanism should be established to increase co-ordination in relation to NPOs, including proactive and effective compliance with measures to address potential TF abuse of NPOs, on a whole-of-government basis; this should include the sharing of additional information with the ICA by those authorities most involved with criminal justice.

c) Israel should ensure that the ICA has a uniform range of powers across the range of registered NPOs.
d) The ICA should rebalance its approach so that, in addition to its other policy and operational objectives, it should undertake a comprehensive TF risk-based approach and manage the register of NPOs and the accuracy and up to date nature of information on it, comprehensively and effectively; this should include revisions to the sanctions framework to provide a greater range of sanctions and proportionate use of those sanctions. Resources should be increased to ensure this activity is effective.

Immediate Outcome 11

a) Israel should build and implement comprehensive compliance-ensuring programmes for FIs, DNFBPs, and supervisors for PF-TFS relating to DPRK. The supervisory and monitoring regime in respect of FIs and DNFBPs, in terms of frequency of outreach and inspections should be strengthened.
b) Although it has not hindered effectiveness, Israel should address the technical gaps in the designation framework so that, in particular, the MoF does not have discretion not to make the automatic designations from the UN permanent.

228. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5-8, 30, 31 and 39.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

229. Due to its geographic location and its historical and political circumstances, Israel has experienced high terror threats, and as a consequence, high TF potential threats. As a result, it has developed a wide range of effective instruments and mechanisms to combat terrorism terrorist financing in all its aspects. The authorities have a good understanding of the domestic and international terrorism threats that Israel faces, and TF risks as they are associated with those threats.

230. The assessment team based its conclusions on a variety of elements including: discussions with relevant Israeli authorities (*Shin-Bet*, INP, IMPA, the Sanctions Bureau and the National Bureau for Counter-Terrorist Financing). The team reviewed numerous cases demonstrating that the authorities to a high extent have identified, investigated, and convicted for TF offences consistent with Israel's risk profile.

231. Most TF activities that Israel faces do not originate and are not performed within the Israeli financial system, but rather emanate from sources outside Israel. However, Israeli authorities are aware of those channels that might be used within Israel, and invest great efforts to identify and prevent attempts by terrorists and terrorist organisations to misuse the Israeli financial system. Israel assesses that

the most significant terrorist financing threat to Israel emanates from (a) other countries and territories that have the organisational ability to collect and place funds and make them available for use by terrorist organisations; (b) contributions, charity organisations and donations from the general population (such as weekly donations in prayer houses, standing orders, etc.) or from individuals with money; (c) self-financing terrorist organisations by supposedly legitimate business operations, with some of the revenues or profits diverted to other purposes; (d) execution of illegal activities, the laundering of money derived from the offense, and the transfer of money, in whole or in part, for the purpose of financing the activity of the organisation. The transfer of funds to terror organisations is carried out in two main methods: the smuggling of goods, valuables and funds through border crossings, including through trading; and the use of money transfer mechanisms that include correspondent activity, currency service providers, pre-paid cards and foreign credit cards.

232. Foreign terrorist fighters do not feature significantly in Israel's risk profile, as very few have travelled to conflict zones or returned in recent years, and those who have returned have been subject to comprehensive monitoring, investigation, and in some cases prosecution and conviction. These activities were financed using only small amounts of self-funding.

233. Similarly, Israel faces terrorist activities from lone wolf actors who do not require organisational support or funding. In the last quarter of 2015, there was a wave of "lone wolf" terrorist attacks. The attacks were carried out by young lone terrorists from the relevant area, and involved mostly knife-stabbing, vehicle ramming, or shooting. In the framework of *Shin-Bet* activity, in close co-operation with the IDF and the INP, to thwart this terror, hundreds of disruption activities were conducted, including identification, arrests, investigations, indictments and convictions. Due to the efforts of the Israeli LEAs, the wave of lone wolf terrorist attacks, in which tens of people were killed or injured, was curtailed. However, some periodic lone-wolf activity does still occur.

234. Different types of TF cases are prosecuted, and offenders convicted. These cases are consistent with Israel's TF risk profile and include TF cases on the collection, movement and use of funds, as well as TF cases that did not involve terrorism charges. These involved the methods and channels of TF activities described above. These cover a spectrum of TF typologies: cross-border smuggling, Charities/NPOs and voluntary contributions, trade-based TF, money transfer mechanisms, and supposedly legitimate business activity.

235. Between January 2013 and December 2017, Israel prosecuted 77 cases involving 103 persons for one or more TF offences. During that period, 37 cases resulted in convictions for one or more TF offences, involving 39 natural and legal persons. See the following statistics on TF investigations, prosecutions, and convictions. The investigations data reflects those formal investigations conducted by the INP. They therefore do not include the significant efforts by *Shin-Bet* and other security agencies to prevent terrorist acts and their financing. Prosecutions are led by the State Attorney's Office (SAO), which co-ordinates with INP and other agencies throughout the prosecution.

Table 17. **Investigations and Prosecutions for TF**

	TF Investigations		Prosecutions Commenced		Convictions	
	Cases	Natural/ legal persons	Cases	Natural/ legal persons	Cases	Natural/ legal persons
2013	57	67	1	1	7	7
2014	81	84	3	4	3	3
2015	43	48	22	29	5	6
2016	60	78	28	37	9	10
2017	46	68	23	32	13	13
Total	**287**	**345**	**77**	**103**	**37**	**39**

Source: INP, SAO

236. In 2015, three legal entities were indicted and subsequently convicted in relation to one case; in 2017 there were two indictments; and in 2018, two legal entities were convicted in the "N" case, described below. The types of legal persons that were indicted/convicted were charitable NPOs and corporations; e.g. in the "N" case, one NPO and one corporation. The punishments included fines, confiscation and liquidation.

237. While the number of TF convictions appears low compared to the number of investigations and prosecutions, this is justified by the fact that some of the investigations did not result in prosecution due to lack of admissible evidence for TF. In these cases intelligence could not be turned into evidence due to concern of exposing intelligence sources, hence other charges were pursued. In addition, *Shin-Bet*'s and the other security agencies' proactive efforts are effective in disrupting terrorism at the early stages, which curtails a large number of TF investigations and renders prosecution for TF unnecessary. There is strong co-ordination between *Shin-Bet*, INP, and the other authorities to accomplish this.

238. Also, since prosecutions take time, the figures for convictions do not necessarily reflect the results of prosecutions initiated in the same year. Nevertheless, there are some delays in prosecutions. Where, there is a suspect in custody, cases are expedited and are usually prosecuted within a few months (by law the accused can only stay in custody for a maximum of nine months, with an option to extend for three more months). However, when there is no suspect in custody, prosecutions take longer. Terrorism and TF cases are tried at the District level Courts, wherein there is a system of trial by a bench of 3 judges. This system contributes to delays in trial as there are limited numbers of judges. The authorities apprised that there is a move to change the existing system to trial by a single judge, to expedite the cases pending trial.

239. The following cases demonstrate Israel's prosecution of, and convictions for different types of TF, including the collection, movement and use funds, as well as TF cases that did not involve terrorism charges.

Box 16. **Example of TF Activity – Collection**

The "K" Case

Background: A domestic organisation was designated as an unlawful association (hereafter; the Domestically Designated Organisation – DDO) in 2015 for its role in funnelling funds to the Hamas organisation. The organisation was a branch of the Muslim Brotherhood.

Four senior members of the DDO conspired together to continue financing the DDO's activities.

The funds were collected and transferred in various concealed ways. The first defendant collected NIS 740 00 (EUR 173 000) through the DDO network and provided it to the second defendant, in weekly meetings, which took place in different locations in Israel. The second defendant transferred those funds to DDO activists using one of two main methods: (1) via chargeable credit cards in the sums of NIS 500 or 800 using numerous branches of a financial institution in Israel to avoid detection, and (2) via two DDO activists (defendants 3 and 4) who transferred the money to other activists. A total sum of NIS 500 000 (EUR 117 000) was transferred using these methods.

Relevance to IO.9 and IO.10 (deprivation of TF assets): In 2016, the defendants were convicted for TF (s. 8 of the PTFL), money laundering, and membership in an unlawful association. Two of the defendants were sentenced (as part of a plea bargain) to 23 months imprisonment, suspended sentence and a fine of NIS 100 000 (EUR 23 400) each. The third defendant was sentenced (as part of a plea bargain) to 8 months imprisonment, suspended sentence and fine of NIS 24 000 (EUR 5 600). The forth defendant's case was still pending as at the time of the on-site visit.

Due to proceedings taken in this case and in other DDO-related cases, the DDO's activity and the funnelling of funds to it has been significantly decreased.

Box 17. **Examples of TF Activity – Movement**

Example 1: The "R" Case

Background: The defendants were under the surveillance of the INP "*Yachbal*" unit as part of the framework of activity of the DDO. They were apprehended carrying 40 cash envelopes of NIS 1 000 each (a total sum of NIS 40 000/EUR 9 350), with the intention of forwarding them to DDO activists. This case demonstrates one of the ways in which funds were transmitted, on a monthly basis, as a "salary" to DDO and /or Hamas operatives in Israel.

Relevance to IO.9: In 2016, three defendants were charged with TF (s.8(a) of the PTFL) and membership in a terrorist organisation. They were subsequently convicted and sentenced to 14 months imprisonment.

Relevance to IO.10 (deprivation of TF assets): The TF funds that were seized were also forfeited, as were vehicles used to transport these funds.

Example 2: The "I" Case (stand-alone TF)

Background: The defendant, an attorney, owned a law practice for the representation of prisoners who were convicted of security offences. She used her status as their attorney to attempt to disguise the sources and destination of funds. The defendant was arrested while carrying hundreds of thousands of USD and NIS. She and her brother were convicted for funnelling funds from Hamas to prisoners.

Relevance to IO.6: IMPA's proactive reports contributed to the intelligence gathered in the case prior to the arrest and led to the detection of new methods of activity of terrorist financiers.

Relevance to IO.9: The defendant was convicted for the TF offences (s.8(a) of the PTFL and s.85(c)(1) of the Defence Regulations) and sentenced to four years imprisonment and three years suspended sentence. Her brother was also convicted for TF offences and sentenced for eight years imprisonment and one year suspended sentence.

Example 3: The "C" Case (stand-alone TF)

Background: This case was investigated by the recently established TF Task Force and is now being prosecuted. It involves a Turkish national and a relative who was an Israeli national and businessman. The investigation uncovered a network of foreign shell corporations involved in raising funds for Hamas. The relative was in charge of transferring funds from Turkey to Hamas operatives in Israel. He received hundreds of thousands of Euros in cash from connections in Turkey, and smuggled them into Israel by wrapping EUR 500 notes in plastic food bags taped to his body. The two were subsequently arrested. The Turkish national was deported.

*Relevance to IO.*6: IMPA's intelligence reports, in response to requests that came both from *Shin-Bet* and INP, assisted in the arrest of the offenders and exposed new entities (e.g. MSBs) which were suspected to be involved in the TF activity.

Relevance to IO.9: The relative is being prosecuted for; *inter alia*, TF under s.23 and 31 of the CTL.

Relevance to IO.10 (deprivation of TF assets): Funds in a local MSB in the amount of NIS 112 000 (EUR 26 100), EUR 101 700 and USD 6 400 were seized and confiscated.

Box 18**. Examples of TF Activity - Use**

Example 1: The "A" Case – Abuse of NPO TF

Background: The case involved four defendants, who were high-ranked Hamas leaders. They were involved in establishing Hamas schools, as part of Hamas' Da'wah regime. Through this activity, they sought to raise funds to finance the organisation's terror activities against Israel. They were also involved in funnelling funds which were raised abroad for the purpose of financing Hamas activities in Israel– through various MSBs and sophisticated financial transactions.

*Relevance to IO.*6: IMPA's reports, in response to both *Shin-Bet*'s and INP's requests, exposed the offender's bank accounts used for the funnelling of TF funds.

Relevance to IO.9: In 2014, the Court convicted three of the defendants of terrorism and TF offences. Defendant 2 was convicted and sentenced to 7 years' imprisonment for terrorism and TF offences and additional 3 years suspended sentence for terrorism (membership in a terrorist organisation) and 2 years' suspended sentence for TF, pursuant to section 8(a) of the PTFL, and ML. Defendant 3 was sentenced to 42 months and 3 years suspended sentence for TF and ML. Defendants 1 and 4 were convicted of terrorism offences.

Relevance to IO.10 (deprivation of TF assets): The Court ordered the forfeiture of foreign currency seized, in the amount of NIS 300 000 (EUR 70 000).

Example 2: The "M" Case - *Hawala*-type TF

Background: Between the years 2010-2014, the defendant, an Israeli attorney at the time, used his status as an attorney to exchange and transmit messages between prisoners of the domestically designated Hamas organisation and its leaders in Gaza.

As compensation for his services, the defendant was given a total sum of NIS 1.3 million (EUR 304 000) from Hamas. The money was forwarded to him in various methods: by couriers through an attorney; and by Israeli citizens in exchange for funds transferred to a third party in Gaza in a Hawala-type transaction, thus bypassing the official financial system and controls.

Relevance to IO.6: IMPA's reports, first proactive and then responsive, led to the exposure of TF activity.

Relevance to IO.9: In 2017, the court convicted the defendant for a number of TF offences, including engagement in terror financing (sections 8 and 9 to the PTFL) and the provision of services to an unlawful association (section 85 of the Defence Regulations), as well as tax fraud and various money laundering offences. He was sentenced to 7.5 years imprisonment and a one year suspended imprisonment.

Relevance to IO.10 (deprivation of TF assets): The defendant was also penalised with a fine of NIS 50 000 (EUR 11 680). The court also ordered the forfeiture of NIS 1.2 million (EUR 280 400). In a separate proceeding, the defendant was ordered to pay amended taxes, from which he evaded, to the Israel Tax Authority, in the total sum of NIS 350 000 (EUR 81 800). Following his conviction his license to practice law was suspended.

TF identification and investigation

240. In line with the country's NRA, Israel has been successful at identifying TF in a number of ways including through its extensive and sophisticated use of financial intelligence and in the course of terrorism investigations which always incorporate a TF component. The assessment team based these conclusions on: statistics of the number of cases prosecuted and convictions achieved; discussions with prosecutors, *Shin-Bet*, INP and other LEAs, including specialised units focused

on counter-terrorism; the Intelligence Fusion Centre, IMPA, the Counter Financing Bureau and the National Cargo Targeting Centre.

241. TF cases are well identified and investigated, through a comprehensive legal, institutional and operational framework. Case studies also showed that Israel identifies the specific role played by the terrorist financier. *Shin-Bet* leads on counter-terrorism and TF intelligence and is the main source of TF investigations. *Shin-Bet* possesses a wide array of powers for the purpose of dealing with terror threats, and in practice *Shin-Bet* takes a proactive role in identifying and dealing with TF threats. The daily functions of *Shin-Bet* units are guided by classified internal work plans that are updated periodically. The work plans are then converted into tangible targets drawn out for every unit in accordance with its operational characteristics. The existence of a financial component of terrorism activity is examined in all relevant cases, in parallel to the terrorism investigation itself.

242. Several organisations (*Shin-Bet*, INP, IMPA, the Intelligence Fusion Centre, the Counter Financing Bureau and the National Cargo Targeting Centre) work in cohesion to effectively identify and investigate TF offences. While *Shin-Bet* leads on the intelligence side, INP leads the formal investigations to gather evidence, etc. Different units within the INP handle different TF cases, depending on their complexity and, occasionally, on their territorial nexus. While investigations are typically initiated by the *Shin-Bet*, the INP also initiates investigations when evidence of suspected TF arises in the course of its work.

243. Regardless of the source agency for identifying the case, INP and *Shin-Bet* closely and effectively co-operate during the investigation to secure evidence for a court proceeding, arrest suspects, and identify and confiscate funds and assets intended for TF.

244. *Shin-Bet* and INP have adequate resources and manpower for TF investigations, and both have designated units and teams are in place to tackle TF. A Terrorism Financing Task Force has also been established within INP's "*Yachbal*" unit. It is a trained, skilled and specialised financial investigation unit to assist in detecting TF activity. The TF Task Force includes specialists from INP, the intelligence community, ITA and IMPA.

245. Through the Task Force, the Fusion Centre, and IMPA's monitoring and analysis, Israeli agencies increasingly utilise financial intelligence for detection and investigation of TF cases.

246. IMPA also plays a key role in identifying TF cases. In this sense, IMPA's role in identifying TF offences has grown in recent years. This is due to IMPA's activities in identifying and monitoring signs that TF activities are being carried out, based on the financial information in its custody.

247. IMPA has the necessary resources and ability to develop initial identification of TF cases. IMPA has a dedicated team for TF, incorporating specialist TF analysts. They provide answers to requests for information sent by LEAs and security agencies, conduct proactive operational analysis and strategic analysis, support investigations conducted by the TF task force. The activity of the TF team is supported by the analysts in the Alert Centre, who monitors all suspected TF information reported to IMPA (while giving it high priority). In

addition, IMPA's Strategic Analysis Team works with the TF analysts on TF projects (both proactively and in joint projects with security agencies). The work on TF is also supported by the IT Department for special TF data mining projects. Finally, IMPA's Proactive Analysis Team conducts both ML and TF operational projects.

248. IMPA enters all UARs that it receives into its database, and their contents are monitored for the purpose of identifying entities or activities that raise TF suspicions and detecting additional entities that may be involved. IMPA uses its alerts centre, keyword searches, and analysis of every UAR received that is flagged as relating to TF (which are all analysed within one day) to further examine and confirm suspicions and identify potential TF activity. The statistics for TF UARs reported to IMPA are as follows.

Table 18**. TF UARs**

Sector	2013	2014	2015	2016	2017	Total
Banking Corporations	265	210	188	245	218	1 126
Insurers	0	0	0	0	3	3
Stock Exchange Members	2	0	0	0	1	3
MSBs	1	0	1	6	31	39
Portfolio Managers	0	0	1	0	0	1
Postal Bank	231	166	151	195	119	862
Provident Funds	0	5	0	0	0	5
Credit Cards	60	86	100	89	134	469
Trading Platforms	0	0	0	0	0	0
Precious Stones	0	0	0	0	0	0
Total	559	467	441	535	506	2 508

Source: IMPA.

249. When there is further suspicion of TF activity or a TF offence, IMPA sends an intelligence report to *Shin-Bet* and INP.

250. These intelligence reports are used to identify potential TF cases (see for example the "DDO" case and the "N" case below) or additional targets for ongoing investigations. IMPA's intelligence reports also contributed greatly to the success of a number of other TF cases. (See the case examples above, as well as IO.6.) In addition, IMPA's intelligence reports assisted in the early detection, disruption and prevention of TF in a wide range of activities, prior to these activities reaching the threshold of judicial proceedings. The following table indicates proactive and responsive intelligence reports disseminated to law enforcement, judicial proceedings (in cases) which were generated by FIU disseminations or when FIU disseminations revealed new investigation channels.

Table 19. **Judicial proceedings (in cases) which were generated by FIU disseminations or when FIU disseminations revealed new investigation channels**[28]

Year	Total FIU TF disseminations		Prosecutions		Convictions	
	Total Intelligence reports disseminated		Total number of TF cases prosecuted	TF prosecutions based on FIU disseminated information	Total number of TF convictions (final)	Convictions based on FIU disseminated information
	Proactive	Responsive				
2014	65	22	3	3	3	**2**
2015	41	18	22	3	5	**1**
2016	45	23	28	3	9	**2**
Total	**151**	**63**	**43**	**10**	**17**	**5**

Source: IMPA, SAO.

251. See Table 17 above for statistics on TF investigations. Israel's effective identification and investigation of TF cases is well demonstrated through case studies.

Box 19. Identification of TF cases

Example 1: The "DDO" Case

Background: Following years of ongoing investigation by security agencies and LEAs, surveillance was put in place in order to track down the financial activity of several entities and NPOs that were identified as belonging to the Muslim Brotherhood.

Between 2009 and 2014, 3 NPOs were identified as being tasked with collecting funds abroad and funnelling them into Israel for the benefit of the designated Hamas organisation. During this period, NIS 161 million (EUR 37.6 million) was collected by these NPOs, from sources in a foreign country. The extensive network of organisations acted with formidable sophistication, involving the fabrication of import/export transactions, the use of chargeable debit cards, fictitious "charitable donations" from multiple jurisdictions, cash transfers, and other means.

Relevance to IO.6 and IO.9: IMPA played a key role in identifying the DDO case. As part of ongoing monitoring of the unusual activity reports, IMPA identified reports indicating a diversion of financial activity from entities that had been previously designated as an unauthorised association for TF purposes. As part of the financial investigation, IMPA sent requests to receive supplementary information from abroad and from a financial institution in Israel. IMPA's monitoring and analysis resulted in the mapping of the vast and elaborate DDO network before its 2015 designation. The case was then transferred to the Fusion Centre for further intelligence analysis, which then led to the investigation by INP and *Shin-Bet*.

28. For 2017, there were 43 proactive and 44 reactive intelligence reports disseminated. Figures for resulting prosecutions and convictions were not available.

Relevance to IO.9: A number of individuals and entities identified as part of the DDO network were later prosecuted and convicted for TF. See case examples above and below.

Relevance to IO.10: Based on the intelligence collected, in 2015 the Minister of Defence designated the DDO (including sub organisations and affiliates) as an unlawful association. The designation was timed, *inter alia*, in light of the findings of the financial intelligence, in a close co-operation between all authorities involved, and the private sector, in order to provide for full seizure of the funds.

Following the designation and the mapping of the DDO network and assets, orders for seizure were issued against over 20 related entities and their assets, leading to the freezing of two bank accounts holding some NIS 300 000 (EUR 70 000), identification of dozens additional legal entities (NPOs, corporations, and financial institutions) possessing 90 separate bank accounts, 37 real estate assets, 36 vehicles, and traded stock ownership in 10 different corporations that have been seized and led to forfeiture of considerable funds in different accounts, owned by the DDO. The total value of the property of the DDO frozen/forfeited since September 2014 is estimated to be over NIS 20 million (EUR 4.7 million). The case also led to the termination of several NPOs.

Example 2: The "N" Case

Following the designation of the DDO, within the framework of the Fusion Centre it was established that additional charity organisations were operating for the DDO. The entities involved used different accounts to funnel the funds from abroad as a mechanism to conceal the fact that the funds were connected to DDO and avoid confiscation.

Relevance to IO.6 and IO.9: Financial intelligence provided by IMPA showed that foreign NPOs were funding the prohibited DDO activity. A certain charity association was traced and identified as leading and supervising the activity. The information indicated that the funds were transferred directly to DDO operatives via this association. The case demonstrates the efficient use of financial information in identifying and supporting TF investigations, and as a tool to continue monitoring TF activity after an organisation was designated for TF activity.

Relevance to IO.9: Nine individuals were indicted of offences under the PTFL and the PMLL. In February 2018 the defendants were convicted, inter alia, of TF according to section 9 of the PTFL.

Relevance to IO.10 (deprivation of TF assets): In the course of the investigation, property worth NIS 8.5 million (EUR 2 million) was seized and an application for confiscation of property worth NIS 3.7 million (EUR 864 600) was submitted. Following conviction in February 2018, NIS 740 000 (EUR 173 000) was confiscated.

TF investigation integrated with – and supportive of – national strategies

252. The investigation of TF is integrated with, and used to support, national counter-terrorism strategies and investigations. This includes the designation of terrorist organisations and terrorist support networks. The geo-political

challenges that Israel faces with respect to terrorism has made counter-terrorism and CFT the highest priority. Hence, the counter terrorism strategy is formulated from the highest echelons of the government, and the national policy on evolving risks is reviewed at the highest levels. Furthermore, financial supervisors and IMPA participate in the efforts to mitigate TF risks in their outreach activities to the private sector.

253. In its strategy to counter terrorism, Israel focuses on the financial elements of the terror activities and the methods to identify and disrupt those financial channels. The national strategy is calibrated in accordance with the evolving risks, and policy is being reviewed regularly by all relevant stakeholders. It includes the Prime Minister, Security Cabinet, National Security Council, Attorney General, Intelligence Community (*Shin-Bet*, Mossad, IDF), along with other professional and relevant authorities as needed, such as INP, Tax Authority, IMPA, and Ministry of Justice. Israel recently transferred the functions of co-ordinating policies and strategies from the Interagency Co-ordination Committee (within the NSC), established in 2003, to the National Bureau for Counter Terror Financing (NBCTF). The NBCTF has an action plan covering two main strands: i) tracing terrorists through financial movements and preventing them from moving funds or other assets; and ii) disrupting the sources of revenue used by terrorist organisations, by targeting their capacity to raise funds.

254. Accordingly, investigation of TF in Israel correlates and corresponds with the general counter terrorism strategy and investigations as demonstrated in several illustrative case studies. Israel's strong understanding of combating TF in order to prevent acts of terrorism is well supported by the adoption or application of several measures that illustrates the national policy regarding combating TF. This policy broadly includes:

a) Investigation of TF as part of terrorism investigations.

b) Designations – *Shin-Bet* and INP TF investigations also support the identification of terrorist organisations and operatives, expose terror networks and support designations of terrorist organisations as unlawful associations.

c) The establishment of TF Task Force and Fusion Centre as a part of overall CT efforts.

d) The adoption of Security Cabinet Decision B/86 regarding combating TF and the recent establishment of the NBCTF.

e) The enactment of a comprehensive Counter Terrorism Law (CTL) in 2016.

f) The supervisors of financial sector and IMPA participate in the efforts to mitigate TF risks in their outreach to the private sector.

255. The investigation of TF has also supported national counter-terrorism strategies through the designation of terrorists, terrorist organisations and terrorist support networks. See the DDO case example above.

Effectiveness, proportionality and dissuasiveness of sanctions

256. Israel applies criminal sanctions in criminal cases which are effective, proportionate, and dissuasive, ranging from prison sentences, to suspended

sentences, and fines (as well as confiscation – see IO.10). With regard to suspended sentences, in most TF cases, there is a component of additional one-two years' suspended sentence, which is added to the prison sentence. The suspended sentence is imposed to prevent repeated unlawful behaviour, and will be automatically activated in case of a repeated offence.

257. These sanctions have been demonstrated in a number of case studies. Most cases involved several charges and several defendants. And the rulings of the courts do not usually refer to the sanction assigned to a specific single offence, but rather on a punishment term which reflects all the offences the defendant was convicted of, or offences of a certain type, or specific characteristics of the offender or the activity penalised. See the case studies above for the penalties applied. However, in the "A" case, also described above, the court established a penalty scale for TF offences, separate from the other offences of participation in the activity of a terrorist organisation. The court decided that the penalty scale for the TF offence is between two to five years imprisonment.

258. In the TF convictions between 2013 and 2017, fines amounting to NIS 3 880 338 (EUR 906 740) were imposed, and 169.1 months of prison sentence imposed along with 67.5 months of suspended prison sentence. The statistics in the table below represent cases where TF was the only or the main component. In the event that there were other offenses in the conviction, they were ancillary to the TF offence.

Table 20. **Criminal penalties imposed for TF offences**

Year	Imposed prison sentence (average in months)	Suspended prison sentence (average in months)	Fines (NIS/EUR)
2013	19.4	12	2 358 825/ 551 200
2014	43.3	16	270 590/63 230
2015	54	16	558 000/ 130 390
2016	23	13.5	645 000/ 150 720
2017	29.4	10	47 923/ 11 200
Total	**169.1 (average time = 33.82)**	**67.5 (average time = 13.5)**	**3 880 338/ 906 740**

Source: SAO

Alternative measures used where TF conviction is not possible (e.g. disruption)

259. As a result of the potential destructive consequences and the risk of terrorism on the State of Israel, there is a particular focus among security agencies and LEAs, first and foremost on the disruption and prevention of the terrorist activity. Through these agencies' co-ordinated and rigorous efforts, Israel effectively combats terrorism and terrorists groups in many cases before they reach the stage of a possible TF investigation and conviction. Statistics on this are classified, but open source materials indicate that there are hundreds of such cases each year.

260. Though the criminal justice enforcement is the preferred route for enforcement and disruption of TF activities in Israel, at times the criminal

enforcement is not feasible due to lack of evidence related mainly to concerns regarding exposure of intelligence sources. In cases where criminal convictions for TF are unattainable, the authorities and LEAs use other effective, additional administrative and fiscal measures. These measures include imposition of fines, designations, administrative confiscation, suspension of professional licenses and liquidation of companies and NPOs. All these measures contribute to the effective mitigation of TF activity.

261. *Shin-Bet* for example, utilises administrative measures including initiating procedures for seizure and confiscation of assets and instrumentalities to disrupt terrorist and TF activities, before they lead to a TF prosecution. The seizure and confiscation of funds and assets is always examined in TF cases.

Box 20. **Case studies demonstrating administrative enforcement**

Example 1: A case including TF, recruitment and smuggling, in which a boat used to transfer items for the designated terrorist organisation Hamas from Egypt, was confiscated according to section 74 of the Defence Regulations (1945).

Example 2: A container aimed for Hamas, was confiscated according to regulations 74 and 120 of the Defence Regulations.

262. Israel has also prosecuted and convicted offenders for membership in an unlawful (terrorist) organisation under the Defence Regulations, Regulation 85. This legislation is the pre-cursor to the CTL adopted in 2016 (and was annulled after the CTL entered into force, although criminal activity identified that occurred while the Defence Regulations were still in force is still pursued under this legislation). The following are statistics for indicted or convicted offenders for the non-TF components of Regulation 85 (e.g. membership in an unlawful association).

Table 21. **Statistics for indicted and convicted offenders**

	2014	2015	2016	2017	Total
Regulation 85 of the Security Regulation (non-TF aspects)	8 indicted/ 6 convicted	12 indicted/ 4 convicted	6 indicted/ 2 convicted	14 indicted/ 4 convicted	40 indicted/ 16 convicted

Source: SAO

263. The ITA maintains an active working relationship with LEAs which update the ITA on investigations or convictions involving economic cases, including TF cases, where the activity has a bearing on tax assessments. The ITA examines all such cases and where appropriate issues tax requirements.

264. The Citizenship Law, as amended in 2011, provides for revocation of citizenship of a persons convicted of terrorism. In 2016, the law was updated to include revocations for violations of CTL, including acts of TF and has since been used twice by the authorities.

265. In respect of foreign terrorist fighters, the authorities are aware of approximately 70-80 Israeli citizens who have travelled to Syria for ideological purposes. However, very few have done so in the past several years. No organisational support for these individuals was identified, as those who travelled used low-level self-funding to do so. Those who have returned have faced intensive investigation and monitoring. Foreign terrorist fighters were usually caught and arrested upon their return to Israel, and some even prior to their departure, following *Shin-Bet* investigations. Approximately 15-20 were indicted. They were indicted and convicted of several counts, namely, membership in an unlawful association, supporting a terrorist organisation, conducting prohibited transactions with terrorist related property under the PTFL, participating in prohibited military training, and contacts with a foreign agent. The average sanction imposed was 20-30 months imprisonment.

Overall conclusions on IO.9

266. **Israel has achieved a high level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

267. Israel implements targeted financial sanctions (TFS) for TF without delay. Using the framework described under Recommendation 6, Israel has demonstrated its ability to implement TFS within the context of UN designations pursuant to UNSCRs 1267/1989 and 1988, domestic designations, and in response to requests from third countries to take freezing action pursuant to UNSCR 1373.

268. The assessment team based its conclusions on a variety of elements including: discussions with relevant Israeli authorities (*Shin-Bet*, INP, IMPA, ICA, ITA, the Sanctions Bureau and the National Bureau for Counter-Terrorist Financing), the financial sector and DNFBP supervisors (BoI, ISA, CMISA, the Ministry of Communication, the Ministry of Justice and the Ministry of Economy and Industry), and a wide range of entities from the private sector, including several NPOs. The team reviewed and discussed the comprehensive information, statistics and case studies provided by Israel.

269. With the amendments to the Counter Terrorism Law (CTL) in February 2018, Israel has removed the delays in the technical framework for implementation of UNSCR 1267 and successor resolutions. However, there is still a technical gap in the designation framework as Israeli citizens and residents cannot be designated under UNSCRs 1267 and 1373. In addition, the process allows discretion for the MoD not to make permanent the temporary designations from the UN, in which case the temporary designation will expire. But this is not an impediment to effectiveness, since all designations by the UN have been transposed domestically in Israel. Israel has not made any requests to the UN for designation of any individual or entity under UNSCR 1267.

270. The National Bureau for Counter Terror Financing (NBCTF) in the MoD leads and co-ordinates the designation process, including adopting designations according to UNSCRs 1267/1989, 1988, and 1373. The Bureau's functions were recently transferred from the Interagency Co-ordination Committee within the

National Security Council. This transition took place in order to further enhance inter-agency co-ordination, provide greater transparency to the designation process, and also provide the new bureau greater authority that the Committee. In addition to co-ordinating the designation process, the Bureau has overall responsibility for co-ordinating national CFT enforcement policies. The Bureau works closely with *Shin-Bet*, who initiates most domestic designations, as well as INPA, IMPA, and the security agencies. Israel has the necessary mechanisms for identifying targets through this co-operation.

271. Israel has received requests for designation of a terrorist organisation or individual from two countries, and has designated them in both cases. Israel has not formally requested any other country to make a designation. However, Israel has made requests to three countries, using an informal process of contacts between security agencies.

Box 21. **Illustrative examples of designations under UNSCR 1373**

1. Hamas: On 22 September 1989, the Minister of Defence designated Hamas as an unlawful association, due to its terror attacks it has launched against Israel and its civilians, and due to its efforts to finance and support acts of terror. In following years, additional organisations affiliated to the Hamas were also designated.

2. See the DDO case in IO.9 above, which was a large TF investigation that led the designation of the DDO and numerous sub-entities.

3. On 12 August 2014, the Minister of Defence designated an organisation AMART AL-AQSA as an unlawful association. As part of the activity against the organisation, money was confiscated and its offices closed.

4. On 19 June 2014, the "W" Foundation was designated as an unlawful association in Israel, due to its affiliation with the Muslim Brotherhood and being a significant part of the Hamas fundraising network abroad.

5. In March 2017, the Palestine National Fund was designated as terrorist organisation in Israel. The designation was based on the ongoing and continuous activity of the funds, which includes financial support for those responsible for carrying out serious terrorist activity against Israel. This served as a significant financing route for transfer of funds, amounting to tens of millions NIS each month, for Palestinian terrorists activists who are imprisoned in Israel or who were imprisoned in Israel, as well as to the families of terrorist activists who were injured or killed as part of terrorist acts that were carried out.

272. By virtue of Resolution 1373, 314 entities have been designated as terrorist organisations. Other examples of such designations were also provided in the submissions made.

273. Once the designation is made, it is published on the same day on the MoD's website and enters into force. It is also published in the Official Gazette (*Reshumot*) and in the daily newspapers.

274. The obligation to freeze applies to all natural and legal persons. Supervised entities must immediately suspend any activity in the customer's account or

transaction, and submit a report to the INP and IMPA regarding suspicious or unusual transactions and to wait for the INP instructions concerning the continuation of the activity. The INP checks all such reports against the lists of designations and if needed uses its databases and co-ordinates with *Shin-Bet* to verify whether they are true matches. In the affirmative, the case is further co-ordinated with the IFC or the TF Task Force. These agencies then liaise with the MoD, which issues administrative seizure orders and forfeiture orders.

275. To facilitate supervised entities' compliance with the obligations, IMPA also disseminates the designations to FIs and covered DNFBPs (via email fax, or registered mail). This is usually done the same day of the UN designation. Moreover, in July 2017, IMPA published guidelines regarding the legal requirements for the prevention of TF. These guidelines emphasise and clarify the obligations of the supervised entities to fulfil their TFS obligations.

276. Financial institutions have a strong understanding of their TFS obligations. Financial institutions adequately implement their obligations on targeted financial sanctions and most make use of external software providers to perform automatic screening against the updated UNSCR lists. However, smaller firms and some MVTS institutions depend on a manual screening process (due to limited available resources), which does not always allow timely checking of their customer and transaction database with the updated UNSCR lists.

277. Covered DNFBPs have a good understanding of their TFS obligations through the websites of the IMPA or the MoD, and screen their customers appropriately. They verify new clients during the on-boarding stage against these lists and undertake subsequent actions should there be a match.

278. The following table indicates the numbers of initial freezes by financial institutions (i.e. possible matches that were then reported to INP for further instructions) as well as confirmed hits (which resulted in seizure orders) from 2013 – 2017. See Table 22: for statistics on the amounts frozen, seized, and confiscated. All of the freezes and seizures related to domestically designated entities – no matches were identified in relation to UNSCR 1267/1989 and 1988.

Table 22. **Initial freezes and confirmed hits by financial institutions**

	Number of Initial Freezes Taken by FIs	Confirmed hits regarding domestic lists
2013	178	6
2014	125	1
2015	99	5
2016	105	3
2017	78	2

Source: INP, MoD

Targeted approach, outreach and oversight of at-risk non-profit organisations

279. NPOs in Israel are structured as either legal persons or legal arrangements. Registered NPOs include 41 653 *amutot*, 3 200 public trusts and 1 240 charitable companies. *Amutot* are the most common and best-known type of NPO. *Amutot* and charitable companies are both corporate entities but with slightly different corporate structures and governance, and the choice between them is dictated by

the preferences of the founders. Public trusts are legal arrangements, which do not have statutory governance structures and are therefore unsuitable for complex activities; they do not tend to receive new funds but typically disburse benefits by, e.g. scholarships. There would appear to be some 20 000 registered NPOs which are dormant.

280. There are other types of NPO (which have been assessed and which are considered to present a negligible TF risk (which assessment is accepted by the evaluation team)), which have not been subject to the ICA's registration framework. Ottoman associations, a predecessor structure of the *Amuta* were brought within the framework at the time of the onsite element of the assessment. It is also planned to bring the other major type of NPO, *gemachim*, within the framework; these NPOs are established by orthodox Jewish individuals and groups. According to the Central Bureau of Statistics the total income for all NPOs in 2016 was NIS 144.3 billion (EUR 33.7 billion).

Risk

281. As indicated in IO.1, the NRA process has considered the ML and TF risks of NPOs. It is understood that the sector is prone to abuse by terrorists and their financiers. The ML assessment is not sufficiently comprehensive and this might have an implication for understanding TF risk (in terms of whether sufficient information is known about NPOs and whether ML might be carried out for TF); any effect would not appear to be significant in practice. Use of cash appears to be relatively common and, other than for *amutot* or charitable companies (see below for information held on substantial donors), donations can be made anonymously.

282. Donations and charities are considered in the public TF risk assessment material. The greatest risks presented by NPOs are seen as donations made by wealthy individuals and charity organisations not always being aware of the final destination of their disbursements. It is considered that the financial system is rarely used for TF and that alternative methods of transferring funds are used. Relatively little information about TF risk has been placed in the public domain; this does not assist NPOs or others to understand risk and establish appropriate counter-measures.

283. The assessment team had discussions with the authorities on the non-public assessment report and the assessment itself. The features and types of NPOs most vulnerable to abuse for TF purposes have been assessed and there is a very good understanding of these factors by IMPA, LEAs, the SAO and the security services. (See IO.1). TF risk is concentrated in foreign NPOs active in Israel and in domestic NPOs with international activities. Within these NPO subsectors, the major threat appears to be from foreign donors. The types of NPO identified as more vulnerable to abuse are included within the registration and supervision framework of the ICA.

NPOs met by the team

284. The assessment team met several NPO associations with a mix of domestic and foreign donors. The latter are usually wealthy individuals or associations/federations, often also members of the global Jewish community, and known to the NPO and professional advisers in Israel. Some foreign NPOs (also

known to the NPOs and professional advisers) also donate funds. Most foreign donations originate from the US, Europe, the UK and a scattering of other countries such as South Africa, with a significant volume of funding being generated as a result of donors being interested in contributing to a particular project. Grant committees established by NPOs on the allocation and use of funds appear to be common.

285. NPOs take comfort from the CDD undertaken by Israeli banks on overseas donors remitting funds to Israel, with there being a concern that banks' controls are overly strong. Banks undertake CDD on the controllers of NPOs and it is common for them to visit their premises to understand management structures. Audit committees provide a structure for governance; internal controls are common and these include controls over the use of funds. Larger NPOs appear to have more effective audit committee structures with there being some room for improvement in the medium sized and small NPOs. It appeared that both names of donors and beneficiaries are checked against lists of designated persons. *Amutot* and charitable companies must also provide the ICA with a list of the names of both Israeli and foreign donors who donate more than NIS 20 000 (EUR 4 700). The ICA is considered to have a good standard of regulation and its guidelines on internal controls and the requirement for audited financial statements for larger NPOs are considered to be beneficial in addressing risk. There appears to be reasonable interaction by the ICA (but see below with regard to outreach). The assessment team was also advised that, when the ITA audits an NPO, it checks payments made by the NPO with the recipients. The risk of financial crime and ML is seen as low. The ICA had alerted the sector to the existence of some frauds.

286. TF was not seen as a risk except by one NPO. With this one exception, CFT controls are limited to checking designations. This exception was the only NPO met active in a high risk area but it was very cautious within that context and appeared to have good controls to ensure that the benefit it provides is not used for TF. The NPO works with known local authorities; cash payments are not made to beneficiaries, payments to beneficiaries must be specifically allocated, MSBs are not used, medical supplies are provided only to persons known to the NPO and checks are undertaken so as to know the backgrounds of beneficiaries. Banks in Israel appeared to engage in much stronger controls for this NPO than for the other NPOs and associations met, which had different risk profiles.

287. It was felt that training of new members of audit committees and the audit committees of less than large NPOs by the ICA should be increased.

ICA and ITA

288. The ICA has some 180 staff, of which some 50 deal with registration and the day to day supervision of NPOs; these are divided into three divisions (religion, culture and sport; social and education; and welfare) so as to enable staff to focus on the differing characteristics of each sector. Separate teams deal with registration and enforcement of NPOs and other entities. The latter team has some 15 staff (some two thirds of the time of which is spent on applications by the ICA to the court to liquidate NPOs). All staff receive training on changes to legislation relevant to NPOs. There has been some training on ML (although this is not a focus of the ICA). In the second half of 2017 IMPA provided two lectures to ICA staff on

TF red flags. Staff would benefit from the establishment of a systematic, comprehensive, training programme on ML and TF (including TF risk based approaches), especially in light of the very recently acquired responsibility for ottoman associations and as it is proposed to bring more types of NPO within the registration framework and increase the ICA's powers. It is intended to upgrade the IT system in 2019.

289. Officers met by the assessment team were well versed and confident in articulating the ICA's responsibilities and functions. Nevertheless, the number of supervisory staff will need to be increased to undertake a formal risk based approach to supervision, to remove what appears to be over reliance on third party consultants to undertake in-depth inspections and to address the incorporation of ottoman associations and *gemachim* within the registration framework satisfactorily. In addition, the enforcement team will need additional resource so as to allow the proposed increased focus on managing the register and enforcement measures to be effective. The assessment team notes that the ICA has been particularly proactive in the last two/three years, that it has commendably taken sound steps to supervise registered entities rather than only to register them.

290. As a result of the emphasis it places on governance and internal controls and the overall mitigation of risk, the ICA considers that its approach addresses TF risk even if it was not specifically structured for that purpose. The ICA is proactive in combating the potential abuse of NPOs for TF in practice, as it registers and supervises the NPOs most at risk of abuse and it has a range of supervisory tools, including attention on donors (including foreign donors) and donations (including transfers). The ICA also plans outreach programmes targeted directly at donors, and is in the process of developing a new IT system to improve transparency and facilitate supervision through more structured information. However, its approach is not in itself a TF risk-based approach. The additional resources required for a formal TF risk based approach to supervision would not appear to be significant.

291. There have been no discussions between the ICA and the BoI on risks perceived by the BoI or banks or on the adequacy of or lessons that can be learned from the controls by the banks. The ICA was not in a position to comment on text in the TF NRA report that NPOs involved with international funds transfers are considered to be higher risk for abuse by terrorists. It does not see a fundamental difference in risk between the types of registered NPO and supervisory approaches are the same subject to the differing requirements of legislation with public trusts having a different supervisory focus in light of their activities compared with corporate NPOs. Individual NPOs are not rated for risk purposes.

292. The ICA has issued good quality guidelines on the conduct of amutot and charitable companies. This guidance provides information to NPOs promoting a sound governance, control and transparency framework, including financial controls, the issue of audited financial statements, and the appointment of audit committees and internal auditors. The guidelines also reflect the importance the ICA attaches to proper financial controls and that NPOs should use their funds to provide disbursements in accordance with their specified purpose. The ICA undertakes outreach to representatives of NPOs and their advisers. Its approach

changed in 2016 from one of participation at events organised by third parties to one which focusses much more on organising events hosted by the ICA so as to reach a wider audience of NPOs. The ICA has also published ten "golden rules" for donors and met donors on several different occasions. There are benefits in the ICA's overall approach to risk and its emphasis on governance, controls and transparency but outreach to NPOs and the donor community on TF and related risks are not yet systematic, and the assessment team supports the proposed approach of the ICA to take more responsibility for outreach.

293. The ICA receives a good level of information for active NPOs. Prior to registration, information is required on the founders and directors, all of whom must sign the application form in front of an Israeli lawyer; this information includes a confirmation from each of them as to whether he/she has a criminal record (also signed in front of the lawyer) and a signature by the lawyer identifying each founder and director and verifying each of their declarations that they can act in that capacity. The ICA checks its NPO database (but not its other databases) to ascertain if the application information triggers any cause for concern, the name and purposes of the applicant NPO are consistent, the purposes of the NPO are clear and whether there is any indication that the NPO might operate in breach of the law (which would include ML or TF by extension). A number of founders have withdrawn or nor progressed an application due to the response by the ICA on the basis of information it holds about the founder's fitness and propriety in relation to his/her involvement with other NPOs. In rare cases, it has been necessary to formally reject an application. Some applications have been withdrawn or rejected for other reasons, mainly due to the purpose of the applicant not being consistent with the public purpose of an NPO or to the purpose being unfeasible. Some 1 500 applications are made by *amutot* each year with withdrawals or rejections as follows: (2014: 116; 2015: 111: 2016: 124; and 2017: 96). For public trusts the figures are much smaller with 80 applications being made in 2016 and 2017 combined and 64 certificates being granted. The approach by the ICA is positive but would benefit from refinement (for example, checking other ICA databases and open source material and, at least on a risk basis, the confirmations of non-conviction it receives).

294. With regard to day-to-day supervision, the ICA pays close attention to an NPO's annual turnover; risk characteristics of a particular area or sector; any indications of improper conduct from financial statements, complaints or other sources; and tracking the remediation of breaches. The approach seems to be well thought out. The ICA's powers are not uniform across all NPOs.

295. It is mandatory for all *Amuta*, charitable companies and public trusts to provide the ICA each year with financial statements, which are available for public scrutiny. In addition, each Amutot and charitable company with an annual turnover of more than one million NIS and public trusts with an annual turnover of more than NIS 80 000 (EUR 18 700) must provide the ICA with audited financial statements. For *amutot* and charitable companies information on donors is required, if the donation exceed the amount specified in the regulations, including the name (which would identify whether it is a legal person) and the amount donated. Upon receipt of a request by one or more donors and subject to receipt of additional information on the donors, the ICA can grant an exemption from the publication of this information although it still needs to be disclosed to the ICA.

The ICA does not carry out any specific checks on donors. Seventy-seven exemptions for privacy reasons were granted for *amutot* for the period 2015 to 2017; requests are not granted for corporate donors.

296. An NPO which does not provide its financial statements will not receive a certificate of proper conduct from the ICA, which is a condition of receiving government funds. A request for a certificate triggers a check as to whether or not financial statements have been received The ICA intends to put in place a system for routinely checking whether financial statements have been received. Financial statements received by the ICA are examined, inter alia, to ascertain to what extent financial activities are transparent, whether disbursements are consistent with the purposes of the NPO, whether there are any unexplained loans or money transfers, or whether there are any conflicts of interest. Most active *amutot* and charitable companies have filed financial statements. Approximately 2 200 financial statements are received from public trusts (out of a total of 3 200) each year.

297. Certificates of proper conduct are not provided during the first two years of an NPO's operation. NPOs which have not been provided with certificates are mostly newly established or inactive, although some have sufficient funding not to need government support. They are issued only after the ICA has assessed the file and financial statements to ascertain whether: all reporting requirements have been satisfied satisfactorily; the guidelines are met and appropriate governance structures are in place; the financial statements do not indicate any breaches of law, any unexplained transfers or improper financial activity or any ambiguity in the activities carried out or any other irregularity; and that any queries have been addressed. If concerns arise from the review, or prior to the review of annual reports, additional information and explanation as may be required or an inspection may be carried out by the ICA to make sure the guidelines are met, including the financial provisions regarding the payment of expenses to the payee only and not using of cash. There are examples of the checks also involving liaison with the ITA, the NPO and on-site inspections to the NPO. The large number of failed applications demonstrates that the ICA is proactive. It sees the certification process as a proven incentive for NPOs to raise their standards and remedy any deficiencies. Several dozen times a year the ICA revokes a certificate or refuses to renew it on the basis of significant breaches of its standards. These cases must be remedied, in which case a certificate can be renewed, or the ICA applies to court for the NPO to be liquidated; in severe cases the ICA makes an application to the court for liquidation without providing an opportunity for failings to be remedied.

298. Inspections have been undertaken of *amutot* and charitable companies since 2014. There are two types of inspection, namely on-site inspections (commenced in 2016: 25; 2017: 39) and in-depth inspections (2014: 190; 2015: 119; 2016: 100; 2017: 84). The former are inspections carried out without notice to the NPO undertaken by ICA staff. The annual plan is agreed in the last quarter of each year; scope is left for ad hoc inspections. The programme is guided by a range of factors, including whether there are issues which need clarification following a complaint; follow up to remediation from an in-depth inspection or a complaint; or whether a particular concern has arisen. Priority is given where the NPO has a public interest and it has a turnover of at least NIS 1 million (EUR 234 000) (with NPOs with very low turnover being inspected only in special

circumstances). The type of service it provides and the amount benefits provided are also relevant factors.

299. Inspections by the ICA appear to be of good quality, with coverage including sources of funds, misuse of assets, expenses and use of cash and disbursements. Disbursements are a focus. In-depth inspections are undertaken by third party firms of accountants, typically in response to complaints (or where a response from an NPO does not address a complaint satisfactorily), the ICA's review of financial statements, where the supervisory divisions identify NPOs which justify more focussed attention and situations where a NPO is not co-operating well with the ICA. A series of published focal points are used to guide in-depth inspections. They do not address TF risk explicitly but the process targets the proper conduct of NPOs, sources of funds, use of funds, expenses, and disbursements, and the selection of NPOs and the selection of particular focal points indicates elements of risk based supervision in practice. In some cases the third party is appointed to monitor remediation of deficiencies by the NPO. The trend of a reducing number of in-depth inspections, together with the overall number of inspections, suggests a shortfall of resources in the ICA. In addition, the average one and a half year length of in-depth inspections is overly long.

300. Applications for government funding are made by an NPO to the Office of the Accountant General. The Office, which was not met by the assessment team, conducts its own off-site inspections of NPOs to ascertain whether government funding would be or is secure. There has been recent liaison between the ICA and the Office to maximise the efficiency of each organisation. The two authorities have co-ordinated their activities to agree which authority will undertake an inspection and which follow up actions will be carried out by which authority; the inspection report is shared between the two authorities. In addition, the two authorities are carrying out a pilot project in which they are undertaking joint in-depth inspections using accountants. Further information has not been provided on the Office's supervision.

301. While the ICA has power to refuse to issue certificates of proper conduct and to request remediation of failings pending liquidation proceedings, the only administrative sanction available to it is the power of strike off. It has been used rarely, where a NPO is dormant. It is planned to begin a programme of strike off of dormant NPOs during 2018. The ICA has cross referenced some of its records with those of the ITA, which support the ICA's views on which NPOs are inactive as they have never had files at the ITA, or files opened have been closed, or existing files show no assets are held. In addition, the ICA has sought and obtained information from the Ministry of Transportation on whether these NPOs own vehicles and from the land registry in relation to rights over assets.

302. The ICA makes some 70-80 applications to court each year for NPOs to be put into liquidation. These are NPOs which have been acting in breach of legislation or the ICA's standards. Cases are initiated as a result of inspections, absence of financial statements, reviews of financial statements, complaints or other third party information provided to it. The pattern of the last year is different in that it has involved three cases involving TF. Most cases are successful with the court agreeing to liquidation or a resolution is agreed. It appears to the team that there is some delay in the period of time for the court process to be completed.

303. The ICA is effective in co-operating and exchanging information with other authorities and using information provided by other authorities. There is quite substantial liaison with the Office of the Accountant General. The ICA spontaneously provides information in dozens of cases each year regarding concerns in relation to particular NPOs to IMPA, *Shin-Bet*, the INP and the ITA. It does not receive feedback on outcomes from IMPA and *Shin-Bet* due to the classified nature of the cases. It would be beneficial for a mechanism to be found to provide a few individuals in the ICA with at least basic feedback so that it can understand the risks presented by the NPOs in question and the sector as a whole.

304. Nevertheless, these two authorities, the INP and the *Shin-Bet* (as well as other authorities) spontaneously provide information to the ICA and which benefit its supervision and prevention of misuse of NPOs. On the basis of information provided by *Shin-Bet*, a successful application was made to the court in 2017 to liquidate a NPO acting in breach of its purposes and raising funds by misleading foreign governments and entities (legal proceedings are pending). Another potential case involving TF is being investigated by the INP after contact by the ICA. In addition, in another ongoing case, following designation of theseNPOs by the Minster of Defence, the ICA has made applications to court for the liquidation of 13 NPOs, seven of which have been subject to a liquidation order. The ICA has also demonstrated that it is working with a range of authorities on fourteen other cases in which there have been or are criminal proceedings.

305. There are some fifty requests for assistance made to the ICA by the INP each year. In some cases, this information has allowed the INP to commence investigations. There are also approximately 50 requests a year for assistance from the ITA in relation to non-public information held by the ICA. The ITA in any case receives a copy of the ICA's public database at the end of each day. IMPA also receives a copy of the database. Requests from IMPA and *Shin-Bet* are less common. The ICA has never refused a request for information, although there have been occasions when it has not possessed the precise information requested. On these occasions a judgment has been made whether to contact the NPO or undertake an inspection to obtain the information. Reasons for requests are not provided; Israel has suggested that the ICA's co-operation at the investigation and prosecution stages of cases provides it with sufficient information to understand TF risks of registered NPOs. The assessment team considers that more can be done to provide information relevant to risk to the ICA.

306. The ITA is also proactive with regard to NPOs and has a positive role in increasing standards and preventing misuse of NPOs. It has substantial records on 23 000 NPOs which have applied for exemption from VAT and other tax. NPOs pay tax to the ITA where they pay salaries and in some cases pay income tax as they undertake business. Subject to a risk based model introduced by the ITA (which is useful *inter alia* in addressing TF risk), where an application for exemption from tax is made (which exemption should be sought annually), the ITA reviews the purpose of the NPO, its by-laws, its book keeping, to what extent financial transactions match the purpose, whether the NPO appears to be well managed, the source of donations, and the identity of donors; it also liaises with the ICA where it considers that there might be non-public information of relevance to its checks. It also checks its records with the ICA database, and, therefore, the accuracy of information it receives.

307. Notwithstanding strong bilateral relationships Israel's responses as a whole to the abuse of NPOs for TF are co-ordinated to some extent through the operational activities of the Task Forces mentioned elsewhere in this report and the Fusion Centre. Work is being undertaken to introduce enhanced "whole-of-government" co-ordination mechanisms.

Other preventive measures

308. CDD by reporting entities can provide valuable risk mitigation in relation to NPOs. IO.4 notes the adequacy of CDD, including in relation to beneficial ownership, by FIs (see IO.4 for details). The BoI includes consideration of banks' standards in relation to transfers and NPOs as part of its supervision.

Further actions

309. The positive focus, co-ordination and activities described in other IOs for IMPA, LEAs and the SAO also apply in relation to NPOs (also see the case studies e.g. the "A" Case; the "R" Case; the "N" Case; the "W" Case in IO.9 of the report).

Deprivation of TF assets and instrumentalities

310. Israel effectively deprives terrorists, terrorist organisations, and terrorist financers of their assets and instrumentalities related to TF activities. Israel uses a variety of tools in this respect.

311. Following designation and positive matches against the lists, the MoD issues administrative seizure orders and forfeiture orders pursuant to the CTL and Defence Regulations. Final forfeiture orders are also issued following criminal conviction for terrorism or TF. (See TC annex, R.6 and R.4). The table below shows the amounts seized and forfeited following a designation or through another administrative seizure process, and through criminal procedures in TF cases.

Table 23. **Property seized and confiscated following designations or in TF cases**

	Administrative seizures		Criminal seizures**		Property forfeited***	
	Cases	**Amount**** (expressed in EUR)**	**Cases**	**Amount**** (expressed in EUR)**	**Cases**	**Amount**** (expressed in EUR)**
2013	10	155 180	13	503 630	15	265 020
2014	2	1 205 480	83	1 452 810	2	1 205 480
2015	40	518 610	54	4 663 470	47	558 340
2016	42	48 230	134	1 877 160	45	314 620
2017	21	62 060	85	2 337 780	27	467 630

Note: This includes the amounts frozen/seized following designation (and confirmed hits) under the Defence Regulation or the CTL, or and seized using another administrative seizing process under the CTL e.g. seizure of property of an organisation prior to its designation, seizure of property connected to a grave terrorist offense, or seizure of property discovered after a sentence has been delivered.*
*Note**:This includes the amounts frozen/seized in criminal terrorism and TF proceedings according to the various laws (at the outset of the criminal process).*
*Note***: This includes final forfeitures/confiscations following a conviction or an administrative freezing decision that has been made final.*
*Note****: The figures do not include various assets that were also seized/confiscated, but have not been estimated. This includes real estate, vehicles, industrial and agricultural equipment, mechanical equipment, communication equipment, jewellery, different tools, and computers.*
Source: MoD, SAO.

Box 22. **Case examples of seizures and confiscations following designations and TF investigations/prosecutions**

The "DDO" Case (see case example in Immediate Outcome 9 above):

Following the designation and the mapping of the DDO network and assets, orders for seizure have been sassed against over 20 related entities and their assets, leading to the freezing of two bank accounts holding some NIS 300 000 (EUR 70 000), identification of dozens additional legal entities (NPOs, corporations, and financial institutions) possessing 90 separate bank accounts, 37 real estate assets, 36 vehicles, and traded stock ownership in 10 different corporations that have been seized and led to forfeiture of considerable funds in different accounts, owned by the DDO. The total value of the property of the DDO frozen/forfeited since September 2014 is estimated to be over NIS 20 million (EUR 4.7 million).

"W" Foundation Case:

In June 2014, the "W" Foundation was designated as an unlawful association in Israel, due to its affiliation with the Muslim Brotherhood and being a significant part of the Hamas fundraising network abroad. Following the designation, NIS 3.5 million (EUR 818 000) were seized and confiscated.

The "N" Case (see case example in Immediate Outcome 9 above):

In the course of the investigation, property worth NIS 8.5 million (EUR 2 million) was seized and an application for confiscation of property worth NIS 3.7 million (EUR 864 600) was submitted. Following a conviction in February 2018, NIS 740 000 (EUR 173 000) was confiscated.

The "M" Case (see case example in Immediate Outcome 9 above):

In April 2017, the court convicted the defendant for a number of TF offences. He was sentenced to 7.5 years imprisonment, one year suspended imprisonment, and ILS 50 000 fine. In addition, the court ordered the forfeiture of NIS 1.2 million (EUR 280 400). In a separate proceeding, the defendant was ordered to pay amended taxes, from which he evaded, to the Israel Tax Authority, in the total sum of NIS 350 000 (EUR 81 800).

The "L" Case:

The defendant was recruited to a domestically designated terrorist organisation, which had contacts with Hamas, and was asked to deliver funds from the terrorist organisation, or on behalf thereof, to prisoners in Israel. These funds, estimated in tens of thousands of NIS were paid as a reward to these prisoners and their families for committing terrorist activities. The funds were transmitted to the defendant through unrelated middlemen (some of which were Israeli citizens), on several different occasions and in a variety of locations.

The defendant was convicted of several TF offences, including, pursuant to the section 8(a) of the PTFL. He was sentenced to 27 months imprisonment, 8 months suspended sentence, and a fine of NIS 5 000 (EUR 1 168). A sum of NIS 113 000 (EUR 26 400), which was related to his unlawful actions, was confiscated.

Consistency of measures with overall TF risk profile

312. The measures taken by Israel are consistent with the overall TF risk profile – targeting groups operating in Israel and abroad attempting to fund terrorist

groups and activities against Israel. Israel has sophisticated and effective mechanisms to identify and impose TFS on terrorists, terrorist organisations, and their supporters. TFS restricts terrorist groups and their facilitators from accessing the Israeli financial system and contribute to preventing designated persons from accessing Israel's financial system. TF legislation considers domestic risks and also applies to satellite organisations which are not involved in terrorism but provide support to terrorist organisations. Multiple statutes and processes are used effectively to freeze and deprive terrorist organisations of Israel based funds and assets. The types of NPO identified as more vulnerable to abuse are included within the registration and supervision framework of the ICA. It is a proactive registrar and supervisor. Its approach contains strong elements which mitigate the risk of abuse of NPOs for TF purposes (including attention on donors) although it does not have a comprehensive risk-based approach.

Overall conclusions on IO.10

313. **Israel has achieved a substantial level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

314. Israel has implemented comprehensive and effective counter-proliferation finance targeted financial sanctions with regard to Iran, which are implemented without delay. These are part of Israel's broader and comprehensive counter-proliferation efforts in relation to Iran.

315. The assessment team based its conclusions on a variety of elements including: discussions with relevant Israeli authorities (*Shin-Bet*, INP, IMPA, the Sanctions Bureau and the National Bureau for Counter-Terrorist Financing), the financial sector and DNFBP supervisors (BoI, ISA, CMISA, the Ministry of Communication, the Ministry of Justice and the Ministry of Economy and Industry), and a wide range of entities from the private sector.

316. *Government Decision no. 3160 (2011)* was followed by the government's sanctions policy against Iran of 13 July 2011, which set out broad goals to strengthen counter-proliferation and proliferation finance measures. Accordingly, Israel established a Committee on Sanctions Policy against Iran, in 2011, and as per the recommendations of the said committee, implemented sanctions against Iran through administrative, regulatory and legislative actions. These measures include the *Trading with the Enemy Order 2011* which clarifies that Iran is designated as an enemy of the state and implemented PF-TFS sanctions for Iran.

317. The Sanctions Bureau in the Ministry of Finance (MoF) was established pursuant to the *Combat of the Iranian Nuclear Program Law* (CINPL) in August 2012. The Bureau co-ordinates all efforts relating to counter-proliferation and PF, and the accessibility of the information of sanctions against Iran to the public and business sectors. The Sanctions Bureau has a central committee consisting of the MoD, the NSC, and the INP, but also works closely with all other agencies – e.g. MFA (and its sanctions headquarters, which deals with all UN sanctions), ITA, IMPA, and the other security agencies – to enforce trade sanctions and targeted financial

sanctions with regard to Iran. The Sanctions Bureau has a co-ordinator who is responsible for co-ordinating the Bureau's operations. With the law *Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof*, which entered into force on 11 March 2018, the Bureau also now deals with all proliferation and proliferation finance co-ordination, including with regard to DPRK.

318. The law automatically incorporates all proliferation and PF-related UNSCRs (including PF-related UNSCRS on Iran and DPRK) on a temporary basis, to be reviewed and designated permanently by the Minister of Finance. Therefore, all designations required under Recommendation 7 were in force during the on-site visit. However, the legislation gives discretion to the Minister as to whether to make these designations permanent.

319. Prior to this law, Israel had not implemented specific requirements on targeted financial sanctions on proliferation financing related to DPRK. Israel had relied on the *Import and Export Order (Control of the Export of Goods to the Democratic People's Republic of Korea)*, which requires licences to export to DPRK, and *General Direction No.2.4* of the Ministry of Economy and Industry, which requires licenses for imports. No requests for import from, or export to, DPRK, have ever been received.

320. IMPA disseminates the updated UN designations of individuals and entities, usually the same day of their designation, to all supervisors and supervised entities subscribing to its mailing list. These include PF designations of Iran and DPRK, and reminds them of their obligations to freeze and report transactions pursuant to the CINPL and the Trading with the Enemy Ordinance. (This dissemination of lists took place even before the new law imposing TFS-requirements for DPRK). These did not create enforceable PF-TFS obligations with regard to DPRK, although in practice there have never been any "hits". Additionally, the Sanctions Bureau and the Ministry of Foreign Affairs (MFA) publish explanations on their website regarding Iranian and DPRK TFS obligations from the UN, and provide a link to the lists on the UN's website as well as links for delisting requests to the UN Security Council.

Identification of assets and funds held by designated individuals/entities and prohibitions

321. Most supervised entities (and all the banks) use software for identifying and finding a match between their customers and designated entities. Those using such software include screening against the Iran and DPRK lists. Despite the elaborate legal framework as described above no individuals or entities involved in PF related to WMD have been identified. Given the comprehensive prohibitions in place against Iran, and the trade restrictions and limited exposure to DPRK, funds which may be directed to PF have not reached the financial sector whether their origins are from designated entities or not. Hence no funds or other assets of designated persons and entities have been identified with regard to either country. Nor have there been any false positives. The screening against the various lists, the verification of beneficial ownership requirements, and the priority given to prevent any financial transactions involving Iran all contribute to ensuring that designated persons and entities (and those acting on behalf of or at their direction)

are prevented from operating or executing financial transactions. Israel did provide case examples of customs interventions relating to Iran, and authorisations refused by the Ministry of Finance relating to imports and exports. The Israeli authorities have also confiscated assets pursuant to the Trading with the Enemies Ordinance. For DPRK, the evaluation team was presented with a case concerning a shipment involving the DPRK that was intercepted by the Israeli authorities, demonstrating good co-operation and awareness of proliferation issues generally

FIs and DNFBPs' understanding of and compliance with obligations

322. A number of measures have been adopted to enhance the understanding of the FIs/DNFBPs with regard to PF-TFS relating to Iran, which appear to be sufficient. To explain the sanctions regime and ensure compliance, there is substantial outreach to the supervised entities as well as to the business sector (with the assistance of the Manufacturers' Association and the Chambers of Commerce). The Department of the Chief Economist - International Affairs within the MoF is responsible to provide information and guidance related to sanctions for potential transactions. In addition, the Sanctions Bureau maintains a database on information related to sanctions and designations in respect of Iran and DPRK. The Sanctions Bureau's website also refers to websites of countries and organisations that maintain sanctions regime against Iran and DPRK, and also refers to designated entities in the Iranian and DPRK context.

323. The IMPA, BoI, ISA and CMISA have issued a number of guidelines, circulars and updated directives to enhancethe supervised bodies understanding of their obligations under the PF regime and obligations. The circulars also require financial institutions to adopt policies to evaluate and manage their PF risks. These all refer specifically to Iranian sanctions. Since the enforceable TFS obligations regarding DPRK only came into force during the mutual evaluation on-site visit, the guidelines and circulars did not refer directly to measures on DPRK. However, they do refer to the need to refer to the UN lists on PF (and for banks, non-bank stock exchange members, and trading platforms, screen against these lists) and take this into account into their AML/CFT programmes. As with TF-related TFS, these financial institutions are required to check their customers – including account holders, authorised signatories, beneficial owners, controlling shareholders, and the persons performing the transaction or parties to the transaction – against the designation lists. Prior to the new legislation, the MFA had also met with representatives of all the banks to ensure that they were aware of the UN obligations on DPRK and that their screening systems were up-to-date and include DPRK listings.

324. Financial institutions have a strong understanding of their TFS obligations with regard to Iran, and applied systems to comply with them. All the institutions have screening systems for customer on-boarding as well as account monitoring. Financial institutions were also aware of the international TFS obligations with regard to DPRK. Most of these use automatic screening systems (i.e. the ones purchased from outside vendors, and international lists from other countries) which include both the Iran and DPRK lists, so financial institutions also screen for the latter. However, some smaller firms and MSBs depend on manual screening processes.

325. In the event of a match with the DPRK list, financial institutions indicated that they would contact the INP or *Shin-Bet* for advice (who would likely block the transaction). Some financial institutions had internal policies blocking any financial transactions involving DPRK.

326. The DNFBPs under AML/CFT supervision also have a good understanding of, and implement measures to comply with, the PF obligations with regard to Iran. Most also check the lists distributed by IMPA, which include DPRK.

327. Since the PF-TFS requirements for DPRK only came into force during the on-site visit, FIs and covered DNFBPs compliance programmes in place for Iran did not specifically cover implementation of these measures.

Competent authorities ensuring and monitoring compliance

328. The competent authorities have taken a number of measures to ensure compliance from FIs/DNFBPs with regard to their TFS obligations relating to PF, particularly with regard to Iran. The BoI monitors banks' compliance with TFS requirements on-site when it conducts a thematic CFT inspection, which will be determined by information received through the off-site process or when other indicators reveal that such an inspection is necessary. The ISA and CMISA regularly check TFS obligations during on-site visits. Financial supervisors check not only that supervised entities are complying with the Iran prohibitions, but also that they have proper screening systems in place and that they are screening against the wider list circulated by IMPA (which includes DPRK designations). However, the PF-TFS requirements for DPRK only came into force during the on-site visit and the comprehensive compliance programmes which were in place to ensure implementation of PF-TFS obligations regarding Iran, were not yet in place with regard to DPRK. For example, it is unclear what sanction authority they would have had in the event of finding a DPRK list violation.

329. Supervision by the DNFBP supervisors was more varied – the MoJ (which supervises lawyers and accountants) monitors for compliance for all lists during its inspections, while the MoE (which supervises diamond dealers) has not yet incorporated this into its compliance programme.

330. No violation of the PF-TFS obligations that were in place has been detected.

Overall conclusions on IO.11

331. **Israel has achieved a moderate level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

Israel achieved a moderate level of effectiveness for IO.4.

Financial Institutions (FIs)

a) FIs generally have a good understanding of their ML/TF risks and obligations. Such understanding is more sophisticated in the banking sector and to a lesser extent the credit service and MSB sectors. As a whole, they have developed appropriate AML/CFT controls and processes, including CDD and transaction monitoring, to mitigate risks. Such controls, again, are less developed among MSBs. Cross-checking, verification, and periodic review of CDD information are not widely practised among MSBs.
b) FIs generally applied EDD measures satisfactorily in relation to higher-risk areas such as PEPs, higher-risk countries, and new technologies. They adequately implement their obligations for TFS.
c) The level of suspicious transaction reporting (defined as UARs in Israel) is commensurate with the level of ML/TF risks faced by and the size of the financial sector. There is a sharp increase in the level of reporting by MSB providers in the past two years, which could be due to recent introduction of licensing regime and changes in regulatory regime as well as outreach and training by authorities. IMPA provides helpful guidance to FIs in terms of red flags and quality feedback and there is good interaction between financial supervisors and IMPA in this regard.
d) FIs generally have sufficient internal controls (including at financial group level) to ensure compliance with AML/CFT requirements. They also provide AML/CFT training to facilitate compliance and early detection of suspicious transactions, though not necessarily providing supervised entities with the latest typologies.

Designated Non-financial Businesses and Professions (DNFBPs)

a) Covered DNFBPs have a moderate, though reasonable, understanding of ML/TF risks and obligations, noting that the sectors have been recently incorporated in the AML/CFT regime.
b) Regarding AML/CFT controls and processes, risk mitigation programmes are generally not advanced. Most relied on limited source of information

(i.e. only those obtained from CDD processes, instead of specific ML/TF risk assessment) to mitigate risks.
c) The application of EDD measures among covered DNFBPs varied, with no requirements in respect of domestic PEPs.
d) Not all DNFBPs are required to file UARs and no UARs have been filed by the DNFBPs.
e) Level of internal controls adopted by covered DNFBPs is not comprehensive and covered DNFBPs do not carry out frequent AML/CFT-specific training.

5

Recommended Actions

Israel should take actions to:

Financial institutions (FIs)

a) Enhance the understanding of evolving ML/TF risks and latest obligations (particularly in respect of CDD, higher-risk customers, and domestic and foreign PEPs) among financial institutions, and especially by those MSBs with retailed-focus; and to update all supervised entities on how their sectors could be misused for ML/TF purposes on a regular basis.
b) Ensure that financial institutions continue to, and smaller FIs and MSBs, verify customers and transactions information in a timely manner and on a regular basis.
c) Promote financial institutions' application of EDD in higher risk situations in relation to targeted financial sanctions and PEPs (both domestic and foreign), especially smaller FIs and the MSB sector.
d) Ensure that financial institutions, especially in the MSB sector, file UARs when CDD processes cannot be completed; and continue to provide feedback and guidance to all their entities especially in the areas of UARs in view of the recent introduction of regulatory regime and large number of UARs filed by the sector.
e) Ensure all financial institutions, especially smaller firms and MSBs, apply adequate background checks when hiring new employees, instead of just relying on applicants' self-assessment.
f) Encourage financial institutions to continue providing up-to-date and AML/CFT-specific training to staff, especially on latest typologies.

Designated Non-financial Businesses and Professions (DNFBPs)

a) Extend AML/CFT obligations to all DNFBPs that are currently not covered in the national AML/CFT regime.
b) Develop and enhance DNFBPs' understanding of ML/TF risks and obligations (especially in respect of CDD, higher-risk customers, and domestic and foreign PEPs). and update supervised entities and self-regulatory bodies (SRBs) on how their sectors could be misused for ML/TF purposes.
c) Ensure that DNFBPs verify customers and transactions information in a timely manner and on a regular basis.

d) Promote DNFBPs' understanding and application of EDD in higher risk situations, especially in relation to targeted financial sanctions and PEPs (both domestic and foreign).
e) Extend UAR obligations to all DNFBPs; and provide feedback and guidance to reporting entities especially in the area of the importance of submitting UARs.
f) Ensure diamond dealers apply adequate background checks when hiring new employees.
g) Encourage DNFBPs to continue providing up-to-date and AML/CFT-specific training to staff (e.g. latest typologies).

332. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF risks and AML/CFT obligations

Financial Institutions

333. Most financial institutions generally demonstrated a good understanding of their exposure to ML/TF risks (particularly on domestic clients or those with an Israeli linkage). They developed and implemented internal procedures and programmes to identify, assess, and document these risks on a regular basis (usually annually). The results of these internal risk assessments allowed supervisors and regulators to have a better understanding of the operational ML/TF risks faced by supervised entities, and in turn develop and refine their regulatory approach. Overall, the level of understanding of ML/TF risks and application of internal risk assessments are most sophisticated in the banking sector, followed by the securities and insurance sectors, and then the credit service and MSB sectors. The methodologies of such risk analysis and classification of risk factors are also more developed in the banking sector.

334. Financial institutions interviewed participated in the NRA exercise mostly through answering questionnaires prepared by the NRA's regulators working group and through discussions with their supervisors. In addition, financial institutions participated in outreach activities organised by the IMPA. As such, they were aware of the results of the ML NRA and sectoral risk assessments. Nevertheless, not all financial institutions agreed with the findings. Some of them considered that the NRA might have overestimated the ML/TF risks that their sectors faced.

335. Most financial institutions also have a good level of understanding of AML/CFT obligations in general and the need to implement internal systems and controls. They were aware of the various regulatory instruments, circulars, and guidance issued by regulators. They were also aware of the different AML/CFT measures which were recently introduced by the authorities.

5

DNFBPs

336. As mentioned in Chapter 1 and IO.3 analysis, in Israel, lawyers and accountants providing the services included in the FATF Recommendations - defined in Israel as "Business Service Providers" (BSPs) - are covered for AML/CFT obligations regarding, e.g. CDD and record-keeping but not for UAR. Dealers in precious stones are covered for the range of AML/CFT measures. Dealers in precious metals, trust and company service providers (TCSPs), and real estate agents do not have any AML/CFT obligations. Casinos are illegal in Israel and hence not considered in this report.[29] Notaries were not considered separately in this report, as they are regulated as lawyers when they carry out the activities of R.22 in Israel.

337. In general, most DNFBPs (including those not covered for AML/CFT supervision) have a reasonable understanding of both ML and TF risks faced by their sectors, as well as those faced by Israel as a whole. Among them, BSPs (i.e. lawyers and accountants) demonstrated a clearer understanding of risks, and the diamond sector to a lesser extent. Accountants belonging to international groups benefit from group policy and resources, and have developed ML/TF risk assessments.

338. All covered DNFBPs had some involvement in the NRA process, e.g. sharing their institutional risk assessments with IMPA, but were not involved in determining final sectoral risk ratings. Lawyers and accountants providing BSP services, and diamond dealers considered that the risk rating has not taken into account the mitigation measures and controls in place in determining the level of risk in these sectors. Most entities recognised the potential ML/TF threats in DNFBP sectors that are not subject to AML/CFT supervision, such as real estate, especially in terms of volume of transactions and transaction amount. This echoes the moderate-high ML risks as identified in the NRA (see also IO.1).

339. For those sectors under AML/CFT supervision (i.e. lawyers and accountants providing BSP services and diamond dealers), the supervised entities were generally aware of their obligations under the PMLL and other sectoral legal instruments.

Application of risk mitigating measures

Financial Institutions

340. Financial institutions have generally established internal systems and controls to mitigate ML/TF risks. When it comes to smaller market players outside the banking sector, such measures and controls are less sophisticated and more manual-based (depending on the availability of resources). Based on internal risk analysis, financial institutions generally assign risk rating to their clients and transactions. These ratings could be numerical scores, or risk levels of low, medium, or high. They then implement different internal monitoring procedures according to the identified risk profiles. Most financial institutions have also made use of monitoring mechanisms to mitigate risks. For example, transactions

29. Israel has taken action to set up a task force to consider bringing investigative and prosecutorial action against illegal gambling and on-line casinos.

involving those clients of higher risks require approval from more senior personnel in the compliance department and closer ongoing monitoring at the back office.

DNFBPs

341. The ML/TF risk mitigation programmes implemented by covered DNFBPs are generally not advanced, with the exception of accountancy firms belonging to international groups – as they apply group programmes (including risk assessment). Most other DNFBPs mainly rely on information obtained from CDD to mitigate ML/TF risks. Based on on-site interviews, lawyers and accountants providing BSP services tend to de-risk by rejecting clients and transactions deemed to have medium/high risks (e.g. coming from a higher risk jurisdiction) by following the approach required by Israeli authorities and applied by the Israel Bar Association and the MoJ. However, it does not appear that covered DNFBPs have conducted systematic and regular risk assessments, and applied corresponding risk mitigation measures.

Application of CDD and record-keeping requirements

Financial Institutions

342. Financial institutions generally have put in place adequate risk-mitigation measures in relation to CDD and record-keeping measures. They obtain all the required CDD information, and refuse business relationships or transactions if the CDD process cannot be completed. They were also able to demonstrate that they took measures to monitor and verify information obtained, and conduct periodic review of customer identification data. To achieve this purpose, institutions generally use other established sources to verify clients' identity, e.g. national registries and third-party screening or beneficial owner providers. However, such cross-checking, verification, and periodic review are not as widely practiced among smaller firms, especially in the MSB sector. These MSB service providers rely more on data provided by the client. As for more established financial institutions, they have also made use of information obtained from CDD process to develop a customer risk assessment matrix, which in turn enhance their internal risk assessments and application of other risk mitigation measures. Deficiencies regarding CDD process were noted by financial supervisors such as BoI and MoC (in relation to Postal Bank). All institutions appear to apply adequate record-keeping requirements.

343. Regarding the identification of beneficial owners, financial institutions rely on information available from the Companies Registry maintained by the ICA for verification on an ongoing basis. This is demonstrated by how financial institutions in the banking sector noticed that certain identification information on the Registry might not be most up-to-date or available in some cases.

DNFBPs

344. Covered DNFBPs generally apply the CDD requirements and refuse clients or transactions when the process cannot be completed. However, as lawyers and accountants are not subject to Unusual Activity Report (UAR) requirements, they

will not file any reports to IMPA even in situations where the CDD process cannot be completed. Dealers in precious stones are obliged to submit UARs but have not done so to date. Covered DNFBPs are also aware of the need to verify information collected (either manually or electronically). During the CDD process, if clients are found to fall within a higher risk category (e.g. foreign clients, NPOs, PEPs), covered DNFBPs will also have enhanced procedures or require additional information. Overall, the conduct of the CDD process is not comprehensive among lawyers and accountants providing BSP services, as well as diamond dealers. All DNFBP entities met keep records for a period of five years and apply adequate record-keeping requirements.

345. Regarding the identification of beneficial owners, covered DNFBPs were aware of the requirement to understand who was behind each transaction and ensure that appropriate CDD was conducted on the beneficial owner.

Application of EDD measures

a) Politically Exposed Persons (PEPs)

346. Financial institutions across the board screen for local and foreign PEPs (including family members and close associates). The banking sector generally relies on commercial providers for automatic screening. As for other financial institutions (especially smaller ones), they often conduct their own research (e.g. internet search). PEP customers are subject to EDD, placed into the highest client risk category, and enhanced monitoring.

347. Among covered DNFBPs, the understanding of EDD obligations in relation to PEPs varies. There is no requirement to conduct specific measures in respect of domestic PEPs. Lawyers and accountants providing BSP services screen only for foreign PEPs. They will apply EDD if there is a match of the PEP criteria. Based on interviews conducted during on-site, the legal profession generally underestimate the risks associated with domestic PEPs. While diamond dealers indicated checking of client profile for PEP match, they have not encountered any PEPs so far. The assessment team therefore was not able to form an assessment on how well they apply EDD involving PEPs. The team is also uncertain whether the absence of PEP match is consistent with the business and trade profiles of the sector.

b) Correspondent banking and wire transfers

348. Financial institutions (mainly banks) with direct correspondent banking relationships were able to demonstrate a good understanding of the risks involved in such transactions, and apply EDD and additional controls required to mitigate relevant risks. Regarding wire transfers, the understanding of MVTS providers (especially those of a smaller scale or with a retail focus) on EDD obligations are not as strong as other financial institutions (e.g. banks). This could be due to the limitations of the CDD/EDD requirements as mentioned under the analysis of R.16.

349. DNFBPs do not have relationships similar to correspondent banking, and do not conduct wire transfers.

c) Targeted financial sanctions

350. Financial institutions have a strong understanding of their obligations on targeted financial sanctions and adequately implement those obligations. Most FIs make use of external software providers to perform automatic screening against the updated UNSCR lists. However, smaller firms and some MVTS institutions depend on a manual screening process (due to limited available resources), which does not always allow optimal timely checking of their customer and transaction database with the updated UNSCR lists.

351. Covered DNFBPs are aware of the various UNSCRs either through the websites of the IMPA or the MoD, and screen their customers appropriately. They verify new clients during the on-boarding stage against these lists and undertake subsequent actions should there be a match.

d) Higher-risk countries identified by the FATF

352. Financial institutions are aware of the obligations to apply EDD to higher-risk countries, and assign a higher-risk rating to customers or transactions associated with those countries for ongoing monitoring. They obtain the lists of higher-risk countries from IMPA, though they may not necessarily understand why some of those countries are classified as having higher risks, or may not be fully aware of the relevant FATF public statements.

353. Lawyers and accountants providing BSP services apply the EDD obligations for customers and transactions associating with the higher-risk customers. They take additional steps to understand the nature of the business and source of funds. While it is unclear as to whether diamond dealers conduct all necessary EDD to customers/transactions associated with higher-risk countries, they generally monitor transactions involving those countries more closely.

e) New technologies

354. Financial institutions apply EDD in relation to the use of new technologies, e.g. alternative payment services and digital customer identification. Financial institutions usually conduct a designated risk assessment before launching a new service and engage with the supervisor pro-actively in a timely manner. Financial institutions, especially those in the securities sector or those with a business model involving the use of face-to-face communication and IT interaction, are aware of the supervisory advice issued by the Bank of Israel (BoI) regarding virtual currencies and do not usually conduct business in this area. The use of new technologies is less common among covered DNFBPs.

Reporting obligations and tipping off

355. As elaborated in Chapter 3 (IO.6) and R.20, Israel has wider reporting obligations, which start with unusual activities. Unusual Activity Reports (UARs) for non-bank sectors do not only capture suspicious activities, but also those transactions with potential connections to ML/TF, e.g. transactions which are not in line with the client's profile, large transactions or higher-risk recipients, or suspicions of predicate offences (e.g. tax evasion and fraud). TF issues are also covered in UARs. As also explained in the TC analysis and above, reporting obligations are not required for lawyers, accountants, and non-covered DNFBPs. As such, the large majority of the UARs come from the financial sector. Similar to the trends in many jurisdictions, there has been an increasing number of UARs

filed in recent years (a 75% increase in the past five years). Of which, about 70% of the UARs are from the banks. The Israeli authorities attributed the increase in the level of reporting is due to increase awareness of the reporting obligations.

Financial Institutions

356. Financial institutions generally seemed to have a good understanding of, and sufficiently apply, their reporting obligations to IMPA. The use of automated monitoring systems by most FIs also points to a relatively high level of sophistication and awareness of reporting obligations. The filing pattern is generally in line with the sectoral risk profile (see table below). Until 2016, MSBs submitted relatively low number of UARs as corresponding to the level of sectoral risks, types of transactions (e.g. cash-based, cross-border nature), as well as the number of transactions involved, despite the outreach conducted by IMPA since 2013. Since 2015, there has been a substantial increase of UARs, which could possibly be explained by the stronger supervisory focus in this area and outreach to this sector (e.g. issuing red flag publications for BSPs by IMPA in 2015 and conducting training sessions for over 700 MSBs).

357. Supervisors have detected some deficiencies in entities' UA reporting and imposed sanctions (mostly fines). They indicated that the level of compliance and quality of reporting has improved over the last few years. IMPA is also active in engaging the industry on UA reporting and provides guidance, for example in the form of red flags, which should trigger a report.

358. Financial institutions generally have measures in place to prevent tipping off. For example, front-office employees are not made aware of investigations/filing report of certain customers.

Table 22. **Number of UARs filed by Financial Institutions**

Sector	2013	2014	2015	2016	2017	Total
Banks	41 384	48 512	57 596	54 255	53 637	**255 384**
MSBs	435	2 333	5 047	12 904	23 278	**43 997**
Credit Cards Companies	1 734	2 184	3 067	4 254	4 744	**15 983**
Trust Companies (of Banks)	96	110	52	19	6	**283**
Insurance Companies	3 135	4 198	4 610	4 035	4 080	**20 018**
Stock Exchange Managers	778	740	695	364	380	**2 957**
Portfolio Managers	290	244	298	298	356	**1 486**
Trading Platforms	0	0	0	0	25	**25**
Postal Bank	1 817	2 012	2 079	1 890	1 454	**9 252**
Provident Funds	129	252	419	404	483	**1 687**

Source: IMPA.

DNFBPs

359. Among covered DNFBPs, only diamond dealers are subject to reporting obligations, and they have not submitted any UARs to date.[30] This does not appear to be consistent with the size and ML/TF risks profile identified in the NRA (i.e. moderate high).[31] In addition to the red flags published by the IMPA, DNFBPs would benefit from targeted outreach from competent authorities/SRBs, particularly on sharing concrete examples of suspicious transactions. This would allow them become aware of how their sectors could be misused for ML/TF purposes.

360. Given that there are no UARs filed by covered DNFBPs, the assessment team is unable to draw conclusions as to whether any available tipping-off preventive measures are effective.

Internal controls and legal/regulatory requirements impending implementation

Financial Institutions

361. In general, financial institutions have adequate staff to ensure compliance with AML/CFT requirements. The staffing appears to be proportional to their size, business profile, and the ML/TF risks they face. They have also put in place internal controls and procedures corresponding to their risk levels. All FIs met also have compliance programmes and are subject to internal audits. Most firms have incorporated AML/CFT elements in their general and regular training programmes for employees, and have made use of online programmes for this purpose – though not necessarily focusing on the most updated typologies. A number of FIs, mainly in the banking and securities sectors have also provided designated person-to-person training sessions for staff involving in front-line operations, sometimes with the involvement of the supervisor. The manner in which employees are screened regarding their reliability varies. Some firms have rather strict checks, including polygraph tests, whereas others rely on the applicant's self-assessment and the impression of staff responsible for hiring new staff. Such measures tend to be more developed in the banking and parts of the securities sector, whereas especially smaller or specialised firms in the MSB sector often conduct less robust screening procedures for new employees. Controls and trainings seemed to be slightly less sophisticated for smaller firms, especially in the MSB sector.

DNFBPs

362. All covered DNFBPs are recently incorporated in the AML/CFT regime. Though they generally understand the need for internal controls and procedures, the level of such controls is not maintained as comprehensively as is desired. Lawyers and accountants providing BSP services mainly rely on their stringent

30. Diamond dealers are required to report unusual transactions that are conducted in cash which exceed NIS 50 000 (EUR 11 680) or NIS 5 000 (EUR 1 170) if the customer is from a high-risk country, including attempts to conduct such transactions.
31. P.31 of Israel's AML NRA (unrestricted version).

profession-specific entry (though not AML/CFT-focused) requirements to ensure fit-and-proper of employees. Accountancy firms belonging to international groups rely on group policy for internal controls and procedures. For diamond dealers, it is unclear whether their firms have set up compliance or internal audit departments for AML/CFT purposes. Nevertheless, all supervised entities will check job applicants against criminal record. Covered DNFBPs do not provide as many and frequent AML/CFT-specific trainings to their employees – even though employees' general AML/CFT understanding may not be as advanced.

5

Overall conclusions on IO.4

363. **Israel has achieved a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

Israel has achieved a moderate level of effectiveness for IO.3.

Financial Institutions (FIs)

a) Financial supervisors, and to a lesser degree the CMISA regarding the MSB sector, have a good understanding of ML/TF risks in the sectors they supervise.
b) For financial supervisors which have prudential supervisory duties, they generally rely on their available prudential supervisory programmes for AML/CFT purposes. Financial supervisors generally have not yet developed a full risk-based AML/CFT-specific supervision, although the degree to which supervisors follow a risk-based supervision approach varies, and is rather low for the MSB sector. Most of them have not conducted their own AML/CFT institution-specific risk assessments.
c) As a result, the supervision programme, including on-site and off-site inspection, general monitoring, follow-up measures, have mostly not been entirely planned and undertaken according to the identified ML/TF-specific risk level of individual supervised entities.
d) Generally, financial supervisors implement robust market entry controls. However, the CMISA has only recently introduced a licensing regime for the MSB sector (fully in force by October 2018) and has not taken any measures in targeting unauthorised financial services providers and its understanding of the size of the unauthorised sectors of credit and MSB services is currently limited.
e) Though sanctions and remedial actions are applied across the financial sectors, the number is limited and the severity of these is not strong enough to allow promptly identifying, remedying, and sanctioning violations of AML/CFT requirements. Although relatively high fines were issued to non-compliant MSB entities, their deterrent effect could not be fully established. The current level of supervision in the MSB sector is also not adequate.
f) Financial supervisors are generally successful in promoting a clear understanding of AML/CFT obligations, although the banking and securities supervisor tend to be more active in this area.

Designated Non-financial Businesses and Professions (DNFBPs)

a) Not all DNFBPs under the FATF definition (including real estate agents, precious metal dealers, and TCSPs) are within the national AML/CFT regime.
b) DNFBP supervisors do not have a strong understanding of the potential ML/TF risks faced by the entities they supervise. Not all public authorities met demonstrated a clear understanding of the size and potential vulnerabilities of DNFBP entities which have not yet been incorporated in the AML/CFT regime (e.g. TCSP).
c) DNFBP supervisors and SRBs do not conduct risk-based supervision, and are at an early stage in the development of a risk-based model.
d) DNFBP supervisors (who have recently taken up the AML/CFT supervisory role) have failed to implement effective and dissuasive sanctions where entities have failed to meet required AML/CFT obligations – especially when all DNFBP supervisors identified a significant range of deficiencies. In some instances, supervisors rely on supervisory follow-up actions instead of imposing sanctions to create deterrent and to promote compliance. It is too early in the supervisory process to assess if this approach is effective.
e) DNFBP supervisors have started to pursue AML/CFT obligations awareness raising initiatives.

Recommended Actions

Israel should ensure that:

FIs

a) Priority actions should be taken in developing and consolidating supervisors' understanding of ML/TF risks, especially CMISA in relation to its supervision on credit service providers and MSBs.
b) All financial supervisors should fully conduct, or continue to conduct risk-based AML/CFT supervision and monitoring instead of relying on any available prudential supervisory programmes. Specifically, the supervision programme, including on-site and off-site inspection, general monitoring, follow-up measures, should be planned and undertaken according to the identified ML/TF-specific risk level of individual supervised entities.
c) All financial supervisors should take immediate steps to conduct, or continue to conduct institution-specific risk assessment by analysing the risk factors faced by and mitigation measures adopted by supervised entities, and categorising entities according to different ML/TF-specific risk level/rating, such that sufficient resources could be proportionately adjusted and supervisory activities (in terms of number of inspections and intensity) could be focused on those entities and thematic issues facing the highest ML/TF risks.
d) The CMISA should implement the MSB licensing regime early to prevent unfit individuals from entering the market, or unauthorised and ML/TF

activities in the sector. In view of the higher ML/TF risks exposed to a large number of supervised entities in the MSB sector, the CMISA should therefore consider making broader use of the sanctions to increase deterrence.

e) All financial supervisors should actively make full use of available dissuasive sanctions against non-compliant FIs to promote AML/CFT compliance.
f) Financial supervisors, especially the CMISA, should consider making more frequent use of interactive channels, such as training and seminars, to promote understanding of AML/CFT obligations and risks.
g) The CMISA should be provided with sufficient resources to allow increasing the frequency and depth of inspections.

DNFBPs

a) Priority actions should be taken to incorporate all DNFBP sectors under the FATF definition (including real estate agents, precious metal dealers, and TCSPs) within the national AML/CFT regime, including the introduction of licensing/registration/other controls to prevent potential market entry abuse of ML/TF purposes by criminals, implementation of all preventive measures, and suspicious transaction reporting requirements.
b) Priority actions should be taken in developing and consolidating DNFBP supervisors' understanding of ML/TF risks, especially MoE in relation to precious stones sectors.
c) DNFBP supervisors should take immediate steps to conduct institution-specific risk assessment by analysing the risk factors faced by and mitigation measures adopted by supervised entities and categorising entities according to different ML/TF-specific risk level/rating, such that sufficient resources could be proportionately adjusted and supervisory activities (in terms of number of inspections and intensity) could be focused on those entities and thematic issues facing the highest ML/TF risks.
d) DNFBP supervisors should fully conduct risk-based AML/CFT supervision and monitoring. Specifically, the supervision programme, including on-site and off-site inspection, general monitoring, follow-up measures, should be planned and undertaken according to the identified ML/TF-specific risk level of individual supervised entities.
e) All DNFBP supervisors should actively make use of available dissuasive sanctions against non-complying DNFBPs to promote compliance.
f) DNFBP supervisorsshould continue to pursue awareness raising initiatives on AML/CFT obligations.
g) DNFBP supervisors should be provided with sufficient resources to allow expanding the frequency and depth of inspections.

364. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.26-28, R.34, and R.35.

365. The number of market players in the banking system of Israel is small (20). Banking businesses are concentrated in five largest domestic private banks representing a total of 96% of market share. The Bank of Israel (BoI) is the banking sector supervisor. The government-owned Postal Bank provides basic banking services to low-income non-bank clients through its 650 branches throughout the country, and the Ministry of Communications (MoC) is the relevant supervisor.

366. Other non-bank financial institutions under the AML/CFT system include credit service providers and Money Services Businesses (MSBs), which were newly subject to licensing requirements in June 2017 and 2018 respectively. They provide a variety of services: credit and lending services to retail and corporate clients, wire transfers (especially focusing in cross-border transfers by foreign guest workers) and currency exchange. The Capital Markets Insurance and Savings Authority (CMISA) was recently independent from the Government and resumed the role of supervisor for these two sectors, in addition to the insurance and pension funds. During the transitional period from 2015 to 2017, the Israel Tax Authority (ITA) was responsible for MSB supervision.

367. The AML/CFT supervision in relation to securities activities conducted on trading platforms and by non-bank stock exchange members and portfolio managers are handled by the Israel Securities Authority (ISA).

368. As for DNFBPs, there are two supervisors, namely the Ministry of Justice (MoJ) for Business Services Providers (BSPs) of lawyers and accountants and the Ministry of Economy and Industry (MoE) for dealers in other precious stones (covering both diamond dealers and jewellers). Israel has not assigned any AML/CFT supervisors for real estate agents, dealers in precious metals, and trust and company service providers (TCSPs). Operations of casinos are illegal in Israel.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

Financial institutions

369. Financial supervisors including the BoI, ISA, and CMISA apply robust and effective processes to prevent criminals and their associates from holding, or being the beneficial owner of a significant function in FIs in the banking, securities, insurance, credit service and MSB sectors. They do not allow individuals having financial, tax, and fraud-related criminal record to hold significant functions. They also consider reputation, integrity, as well as financial reliability of applicants before granting of permit. For example, the BoI has not yet approved one bank holding permit application due to pending results of integrity check; and the ISA denied five securities trading platform licensing requests in 2016 due to applicants' failure of reliability test. Four other applicants withdrew their trading platform licensing requests upon ISA's reliability checks in the same year.

370. Supervisors screen applications and verify submitted information using a number of sources, including open-source materials (such as news articles and online resources), third-party screening providers (particularly on beneficial ownership information), as well as government departments or law enforcement

agencies (especially for identification and criminal records). If applicants have business or hold significant or management positions in institutions of other financial sectors, supervisors will also check with relevant regulators during the fit-and-proper process. In case of non-Israeli applicants, supervisors will check with overseas regulators on the suitability of applicants. While the BoI has not rejected any recent applications, it explained that the publication of relevant requirements and forms on its website has likely led to withdrawals by applicants (e.g. one withdrawal in 2017). Withdrawals were often due to lack of sufficient equity or financial strength, or lack of business or personal integrity of applicant. Depending on the reasons of withdrawals, the BoI will develop corresponding follow-up measures. The ISA and CMISA also concurred on this (e.g. three withdrawals by portfolio manager applicants in 2015, four withdrawals by trading platform applicants, and one withdrawal by an MSB applicant). Overall, supervisors apply adequate measures to prevent criminals from holding a significant or management positions in financial institutions.

371. Regarding the Postal Bank, the MoC appoint civil servants as senior staff based on merits, and government recruitment processes apply. As for agent staff at local branches, the MoC conducts vetting such as criminal records, financial integrity, and (financial) reliability checks.

372. Upon granting licences, financial supervisors rely on the approved applicants' obligations to inform them of any changes which could affect the licensing conditions. Failure to do so could lead to sanctions. Supervisors also make use of their on-site and off-site inspections to identify and detect any breaches to market entry requirements, or to verify and confirm suitability of approved applicants.

373. On shell banks, BoI regulations prevent such operations by requiring a physical presence of the bank before granting any licence. Prior to granting the licence, BoI will verify and confirm the address provided.

374. While unauthorised activities are less common in the banking, securities, and insurance sectors, Israel has recently strengthened measures to prevent unauthorised activities in the MSB sector by introducing a licensing scheme to all credit service providers by June 2017 and all other MSBs including financial service providers by June 2018 (after the on-site).[32] Licensing requirements are similar to those implemented in the banking and insurance sectors, e.g. fit-and-proper, capital, and liquidity requirements. According to the former supervisor (i.e. ITA and the former CMISA under MoF), this involves the licensing of some 2 000 entities. However, during the on-site interview, the newly independent CMISA, which was responsible for MSB supervision prior to May 2016, did not have a clear estimate of the total number of MSB entities to be licensed, or the extent to which the introduction of a licensing regime would help remove non-qualifying market players. Generally speaking, financial supervisors rely on complaints, intelligence from other law enforcement agencies and supervised entities in detecting unlicensed activities.

32. The licensing scheme will be fully in force in October 2018 (after on-site).

DNFBPs

375. A number of DNFBP sectors, namely real estate,[33] precious metals, and TCSPs, are not covered for AML/CFT in Israel. Covered DNFBPs including lawyers, accountants, and diamond dealers are subject to licensing controls, with the exception of precious stones dealers. Specifically, the Bar Association, Council of Certified Public Accountants under the Ministry of Justice (MoJ), and Ministry of Economy and Industry (MoE) administer the licensing regimes for lawyers, accountants, and diamond dealers[34] respectively. Providing legal or accounting services without a licence is an offence. To be professionally accredited as lawyers and accountants, candidates are required to undergo admission exams with satisfactory results. As for diamond dealers, applicants are required to have at least four years' industry experience, and demonstrate financial and business viability. All supervisors/SRBs do not allow individuals with criminal records to enter the market. While lawyers and accountants rely on candidates' self-declaration, MoE arranges interviews with applicants to facilitate its consideration of granting of licences. However, supervisors/SRBs have not been able to demonstrate that they have taken additional measures to verify individuals being the beneficial owners of a significant or controlling interest or holding a management function in covered DNFBPs. It is noted that a licence is personal to lawyers and accountants, hence impossible to have other individuals that are beneficial owners.

376. In case of breaches of licensing requirements (including compliance with ethical rules), the Bar Association and the MoJ make use of its sanctions power to suspend or revoke the licences, or to issue written warnings. An additional AML-related ethical rule was introduced in September 2015. In the past five years, 358 and ten licences for lawyers and accountants have been suspended or revoked respectively. However, all these suspensions/revocations are not related to AML/CFT as AML/CFT-focused inspections have only commenced since February 2016.

377. As mentioned, real estate agents, dealers in precious metals, as well as TCSPs that are not lawyers or accountants are not included in the Israeli AML/CFT regime. While real estate agents are required to undergo non-AML/CFT industry exams and criminal record checks, it is unclear if Israel has implemented any other types of market-entry controls. Israel was also unable to successfully demonstrate a full understanding of the estimated size of unauthorised activities which might be subject to AML/CFT abuse. Israel should accord priority to incorporating all DNFBPs under the FATF definition into AML/CFT supervision, and introduce licensing, registration, or other controls to prevent potential market entry abuse of ML/TF purposes by criminals.

33. About 20 000 registered real estate agents by the end of the on-site.
34. The MoE grants three types of diamond-related licences namely a licence to trade in diamonds (1 500); a licence to produce polished diamonds (700); and a licence to be a jeweller (250).

Supervisors' understanding and identification of ML/TF risks

Financial Institutions

378. Financial supervisors rely on the NRA co-ordinated by IMPA as the main source of national and sectoral ML/TF risk information. Some of them have in recent years made use of information obtained from their supervisory activities and private sector input to further develop their understanding of ML/TF risks. All financial supervisors were able to point out the main risks, typologies, and common instrumentalities for ML/TF abuse in Israel, e.g. the use of cash, money service businesses, and real estate transactions.

379. However, financial supervisors are in the process of developing their own methodologies for understanding and identifying the ML/TF risks faced by their sectors and individual supervised entities. For those supervisors which have prudential supervisory duties, instead of developing a dedicated ML/TF risk assessment methodology, they rely on existing prudential risk assessment tools for understanding and identifying ML/TF risks of the relevant sectors. So far only the ISA and the Postal Bank have developed a methodology (including risk model for individual securities sector) to conduct institution-specific ML/TF risk assessment.

380. The BoI has since the end of 2017 expanded its institution-specific prudential risk assessment (originally 16 prudential risk parameters such as credit, liquidity, and conduct risks) to incorporate AML/CFT as two additional parameters. Supervised entities are required to submit information, such as the number of accounts involving offshore destinations, MSB businesses and PEPs, as well as group-level information, on a semi-annual basis or upon request by the BoI. With information received, BoI will determine a general and consolidated prudential risk rating of each supervised entity. Although the BoI conducts thematic AML/CFT supervision since 2009, the risk assessment methodology has only been further developed since 2017, a process which is still ongoing. Whilst the BoI has a preliminary understanding of ML/TF risks, it is too early to conclude that the updated methodology is effective in identifying ML/TF risks faced by individual supervised entities.

381. Among the financial supervisors, the understanding of and ability to identify ML/TF risks is not as strong at the CMISA, as far as the credit service and MSB sectors (classified as moderate-high risks in the NRA) are concerned. This is because the licensing regime was only recently introduced and the CMISA is at the beginning of collecting more entity-specific data in this process. The CMISA, nevertheless, has an understanding through the NRA and the exchange with IMPA about general risks exposed to these sectors. The recent focus of the CMISA was to introduce the licensing regimes for MSBs. It has therefore not yet developed any comprehensive methodology to assess ML/TF risks for both the sector and individual supervised entities. The aforementioned unclear understanding on the extent of informal activities and number of registered entities in the sector does not allow it to fully understand how the sectors might be subject to ML/TF abuse. As far as the insurance sector is concerned (classified as low risk in the NRA), the CMISA has not conducted any stand-alone sectoral and institution-specific ML/TF risk assessments.

382. The services provided by and clients of the Postal Bank are exposed to a lower level of ML/TF risks due to lower transaction amounts, limited and basic banking services offered. That said, MoC considers inherent risks and mitigating measures identified in the risk surveys conducted by the supervision department of the Postal Bank, and advises on residual risks faced. In addition, based on monthly transaction reports, the MoC will update the level of ML/TF risks faced by individual branches (650), and especially on the 21 targeted branches, and update frequency, content, and intensity of supervisory activities (including on-site visit) accordingly.

383. Nevertheless, a few supervisors (e.g. BoI and ISA) have increasingly made use of thematic ML/TF risk assessments to improve their understanding of potential ML/TF abuses. Such themes include accounts with intensive cash activities and cross-border wire transfers for banks; and closed-circuit accounts at trading platforms and their ML/TF risks for the securities sector.

DNFBPs

384. The level of understanding of and the ability to identify ML/TF risks varies among the two DNFBP supervisors, with, the MoJ (BSP services) having a better understanding. While both DNFBP supervisors are aware of the NRA results, not all of them were fully involved in the process. For the MoJ, this is because it has only taken up the AML/CFT supervisory role since 2015, when the NRA was being conducted.

385. Though the MoJ has not conducted any sectoral and entity-specific risk assessments, it was able to identify that smaller to medium-sized entities may be exposed to higher ML/TF risks, as those entities often have not established compliance programmes or hired compliance officers. The MoJ also explained that entities which handle occasional transactions and do not have close interaction with the financial sector may also be exposed to higher ML/TF risks. The MoJ should still take steps to develop more systematic sectoral risk assessments.

386. Regarding the MoE, it has a low level of understanding of and ability to identify ML/TF risks, though the diamond sector is exposed to a medium to high risk under the NRA. The MoE has not conducted and does not have plans to develop sectoral and institution-specific risk assessments. Greater efforts need to be made in this regard and the MoE would benefit from closer interaction with other supervisory authorities for the purposes of sharing experiences, knowledge and procedures.

Risk-based supervision of compliance with AML/CFT requirements

Financial Institutions

387. As mentioned, the financial sector in Israel (with the exception of the MSB sector) is relatively homogeneous. For those supervisors that have prudential supervisory responsibilities (e.g. BoI, ISA in relation to trading platforms and portfolio managers, CMISA in relation to insurance), they mostly rely on and extend their prudential supervisory programmes (with tools including on-site and off-site inspection, ongoing monitoring, meetings with senior management, training, policies and procedures, etc.) for AML/CFT purposes. AML/CFT

supervision of most financial supervisors is housed within the compliance departments, with some supervisors (e.g. BoI and ISA) assigning staff exclusively for AML/CFT purposes (see table below). Financial supervisors, with the exception of the ISA do not assign ML/TF risk rating to individual institutions (e.g. high/medium/low or numeric scores) and therefore do not determine their supervisory programme (in terms of timeliness, frequency and intensity) according to the level of ML/TF risks faced by individual institutions. Rather, financial supervisors will focus on the higher risk activities or businesses of the institutions (e.g. cash-intensive or MSB activities) or higher risk customers (e.g. non-Israeli customers) when conducting their on-site and off-site inspections. Generally, the application of risk-based AML/CFT supervision has not yet been fully developed. Financial institutions confirmed that supervisors generally rely on the comprehensive and, where applicable, intensive prudential supervisory programmes for AML/CFT purposes.

388. The BoI relies heavily on prudential on-site inspections for supervision, which work in close co-operation with the off-site supervision department. It generally spends three months for prudential inspection at the five major banking groups and two commercial banks, and conduct an average of 30 on-site inspections each year. Five of these inspections are wholly AML/CFT-thematic inspections. The annual work plan for on-site inspections, however, was based on the overall prudential risk profile of the respective FI. As mentioned in previous paragraph, the methodology and the priority of the annual inspection plan is not determined by the ML/TF risk rating of individual institution. While the BoI indicates that an ML/TF risk identified as high for a particular FI usually triggers in advance immediate supervisory action in a flexible and timely manner, its supervision does not appear to be fully based on a stand-alone ML/TF risk assessment. It remains unclear in which way how the BoI uses institution-specific ML/TF risk considerations and assessments in order to determine which particular banks and in which depth they are inspected.

389. In addition, the BoI has conducted thematic off-site AML/CFT inspections in the five major banks, for example on MSB accounts with intensive cash activity and cross-border transfer or correspondent banking services to banks in disputed territories. The BoI relied on these ad-hoc thematic inspections for checking mainly these five banks' compliance on TFS-related obligations, while also checking compliance with TFS-related obligations on-site when it conducts a thematic CFT inspection (which will be determined by information received through the off-site process or whether other indicators reveal that such an inspection is necessary). Separately, it met regularly with the management and Board members of supervised banks to promote compliance with banking regulations. It also has wide access to financial institutions' computer systems (including CDD and transaction information) for desk-based data risk analysis.

390. For the securities sector, the number of AML-specific inspections by the ISA is relatively low particularly for portfolio managers, which have been identified as having lower risks. The ISA started in 2015 conducting risk assessments, assigning risk rating to its supervised entities in the form of a risk assessment matrix with various parameters, as well as incorporating risk-based elements in supervision (e.g. making use of a Prohibition of ML Forum, which meet frequently and regularly among senior management, to determine the inspection focus on higher

risk brokerage activities involving nostro accounts). As an example, the Prohibition of ML Forum decided to conduct an inspection of one non-bank stock exchange member as that member received the highest risk rating and largest volume of activities. On-site inspections review compliance for TFS-related obligations. Apart from on-site inspections, the ISA also uses other tools such as off-site questionnaires, training of staff or lateral correspondence inspections. Based on identified risk rating, it conducted off-site inspections covering 45 portfolio managers in 2018, which constitutes about one third of the sector.

391. For the CMISA, the priority of its supervisory focus up to June 2018 is on implementing the new licensing regime for the MSB sector and has not yet mapped out the types of supervised entities which should be accorded with supervision priority. CMISA is still in the process of developing a concrete plan for completing the sectoral or institution-specific risk assessment. It takes into account ML/TF risks only in a general, but not institution-specific manner. In view of the broad range of activities in the credit services and MSB sectors (from credit service provider to corporate clients to retail-oriented MSBs engaging in cross-border wire transfers), and the limited manpower available to the CMISA at the time of the on-site visit, it is imperative for CMISA to assess higher risk entities (such as those engaging in retail-oriented MSBs, or cross-border wire transfers) for fully prioritised on-site and off-site inspections. Although CMISA is in the process of increase supervision staff, and has already done so, the concern remains whether or not these resources will be adequate for the high number of supervised entities. The current number of inspections is considered too low, especially against the background of the higher risks associated with this sector in the NRA.

392. The Supervision Department of the Postal Bank relies, to a large extent, on its desk-based monthly review on customer and transaction profiles prepared at headquarter, to plan and apply risk-based supervision programme. Some of the risk factors include nature (e.g. cash-based, MSB-related) and amount of transactions, as well as profile of customer (e.g. profession). Based on the analysis, the Postal Bank has identified 21 out of 650 local branches for handling transactions that are of higher ML/TF risks. The Supervision Department of the Postal Bank has conducted more frequent on-site visits to these branches to check the quality of services offered, and provided more AML/CFT-specific training to staff of these branches. It has also made use of other supervisory measures like trainings, guidelines and information requests for AML/CFT monitoring purposes. Based on the external commissioned AML/CFT risk report (which took two years to finish), the Postal Bank has recently adopted thematic monitoring focusing on special scrutiny of MSB accounts. The Supervision Department also initiate thematic reviews occasionally.

393. Most financial supervisors have not fully implemented AML/CFT-specific supervisory programmes. Save for the banking sector, the numbers of dedicated resources for AML/CFT supervision and AML/CFT-specific inspections are generally low. The number of AML/CFT inspections also is not commensurate with the size of the sector. (See table below). Resources allocated, with the exception of the banking sector, do not appear to be adequate for AML/CFT purposes, though the financial supervisors did not consider it necessary to increase manpower resources.

Table 24. **AML/CFT Manpower Resources Available to Financial Supervisors**

Supervisor	Number of Supervised Entities		Number of Full-time AML/CFT Staff	Number of AML/CFT inspections	
BoI	Banks (incl. commercial banks)	20	8 (140 in compliance department)	On-site (2017)	5
				Off-site (2017)	0
CMISA (note 1)	MSB (note 2)	1 689	9 (30 in compliance department)	On-site (2016)	20 (ML only)
				Off-site (2016)	0
	Insurers	22	8 (110 in compliance department)	On-site (2016)	20 (ML only)
				Off-site (2016)	0
ISA	Trading Platforms	6	4 (3 additional staff in compliance department)	On-site (2017)	6
				Off-site (2017)	6
	Exchange Members	6	3 (3 additional staff in compliance department)	On-site (2017)	0
				Off-site (2017)	4
	Portfolio Managers	125	9 (part-time) (9 in compliance department)	On-site (2017)	7
				Off-site (2017)	1
MoC	Postal Bank	1 (650 branches)	3 (supported by 4-6 external consultants)	On-site (2017)	0
				Off-site (2017)	7

Note 1: ML on-site inspections on MSBs were conducted by the ITA in 2016-17. CMISA has not yet started any investigation since resumption its supervisory role.
Note 2: MSB staff was also responsible for prudential and AML/CFT duty in relation to the credit service providers. However, Israel does not keep separate breakdowns on inspection statistics.
Source: BoI, CMISA, ISA, ITA and MoE.

Table 25. **AML/CFT Supervision Conducted by Financial Supervisors**

Number	2013	2014	2015	2016	2017
Banks					
Supervised entities	22	22	22	19	20
Off-site Inspections	0	3	0	1	0
On-site Inspections	4	2	2	3	5
MSBs (*Note 1*)					
Supervised entities	2 219	1 820	1 726	1 818	1 689
Off-site Inspections	0	0	0	0	0
On-site Inspections	25	23	25	20	11
Credit Service Providers					
Supervised entities	N/A	N/A	N/A	N/A	958
Off-site Inspections	N/A	N/A	N/A	N/A	0
On-site Inspections	N/A	N/A	N/A	N/A	0
Insurance					
Supervised entities	8	9	10	10	9
Off-site Inspections	0	0	0	0	0
On-site Inspections	1	1	2	2	1
Trading Platforms					
Supervised entities	N/A	N/A	N/A	N/A	6
Off-site Inspections	N/A	N/A	N/A	N/A	6
On-site Inspections	N/A	N/A	N/A	N/A	6
Exchange Members					
Supervised entities	9	9	8	6	6
Off-site Inspections	1	2	0	3	4
On-site Inspections	2	0	1	1	0
Portfolio Managers (*Note 2*)					
Supervised entities	120	122	124	125	126
Off-site Inspections	34	27	46	0	45
On-site Inspections	11	23	4	8	7
Postal Bank					
Supervised entities	1	1	1	1	1
Off-site Inspections	12	12	12	12	12
On-site Inspections	1	1	0	0	7

Note 1: MSB-related inspections in 2016-2017 were conducted by the ITA, and those prior to 2015 by the MoF. Portfolio managers-related inspections in 2017 were on ML only.
Note 2: On-site inspections of portfolio managers are integrated inspections, i.e. both prudential and AML/CFT.
Source: BoI, CMISA, ISA, ITA, and MoE.

DNFBPs

394. DNFBP supervisors have recently taken up AML/CFT supervision, i.e. MoE for dealers in precious stones in September 2016 and MoJ for BSP providers (i.e. lawyers and accountants) in September 2015. The number of inspections carried out in 2016 and 2017 remains low (see table below). Less than 1% of lawyers and less than 2% of diamond dealers have received an on-site inspection in the past two years. Accountants and non-diamond precious stones dealers received no on-site inspections, as MoE conducted inspections only to entities having higher

ML/TF risks; and MoJ conducted inspections only when there are concerns arising from off-site inspections or a concern raised by an inspection of non-compliance with relevant legal provisions by a BSP. However, as both supervisors have not conducted a sectoral or an institution-specific risk assessment of the supervised entities, this was not demonstrated to be an appropriate application of risk-based approach of supervision (on-site inspections).

Table 26. **Inspection Conducted by DNFBP Supervisors**

Covered DNFBPs	Number	2016	2017
Lawyers	Supervised entities	62 000	63 782
	Off-site inspections	623	2 137
	On-site inspections	0	6
Accountants	Supervised entities	18 678	18 472
	Off-site inspections	142	120
	On-site inspections	0	0
Dealers in Precious Stones	Supervised entities (diamond)	2 348	2 457
	Supervised entities (non-diamond)	250	182
	Off-site inspections	0	0
	On-site inspections	0	35

Note: With the exception of BSPs and non-bank stock exchange members, off-site inspections conducted by supervisors are not AML/CFT-specific, but cover other regulatory issues as well.
Source: MoE and MoJ.

395. At present, the MoJ relies heavily on off-site inspections for monitoring supervised entities' compliance with AML/CFT obligations (focusing on CDD processes). The criteria used in determining the priority of which supervised entities will receive off-site inspection first, or whether supervised entities are selected for off-site inspections based on ML/TF risks, are unclear. That said, during the off-site inspection process, supervised entities are requested to provide documentation of risk assessment and risk mitigation measures undertaken. The MoJ will follow up with entities if it has identified any gaps in such measures. In 2017, a total of 27 follow-up off-site inspections took place. While the MoJ does not appear to make use of the information received to conduct any risk mapping of the sector, such information forms the basis for the six on-site inspections in relation to lawyers providing BSP services in 2017. In addition, the MoJ has taken into account the outcome of off-site inspection, information from the INP, and suspected breaches of AML/CFT obligations when determining the scope and depth of on-site inspection.

396. In the absence of institution-specific and by extension sectoral risk assessment, MoJ has made reference to the NRA in identifying supervised entities which may be subject to higher ML/TF risk (e.g. those lawyers involved in real estate transactions). It has also made reference to information from other public authorities (e.g. such as the Land Registry and Regulation Department and Corporation Authority) to identify supervised entities that are more often involved in real estate transactions for on-site inspections. The Israel Bar Association is

allowed to be present at the on-site inspections, which is conducted without prior notice.

397. A range of significant deficiencies were identified during the inspections. These include the failure to undertake risk assessment; conduct adequate CDD procedures; verify customers against designated UN lists; conduct EDD on foreign PEPs; obtain beneficial ownership information of legal persons and arrangements; and provide guidance/internal procedures manual for employees as to their AML/CFT obligations. At present, UAR requirements only apply to the dealers in precious stones sector (not the BSP sector) and the relevant supervisor has not identified any non-compliance in this regard to date.

398. Despite the broad range of identified deficiencies, the MoJ, which has recently taken up its supervisory role, is not equipped with sufficient resources (with four full time and two part-time staff) to follow up with those entities in a more focused manner. It is unclear as to whether the MoJ has planned specific follow-up monitoring or supervisory measures with these entities. The MoJ has only taken early steps of implementing a risk-based supervisory approach, which has to be further developed and significantly strengthened.

399. Similarly for the MoE, certain risk-based elements were adopted when identifying supervised entities for inspections. For example, diamond dealers having inconsistent transaction profile (e.g. substantive difference between estimated and actual trade value), involving underground banks, having connections with criminal records, problematic records, etc. The MoE has also selected certain entities for inspection on a random basis, and has made use of both scheduled and unannounced inspections. Prior to the scheduled inspections, MoE also conducts desk-based reviews on CDD procedures and documentation of supervised entities – which is required for cash transactions equivalent to or above NIS 50 000 (approximately EUR 11 680). Follow-up inspections are on-site or off-site, depending on the findings.

400. Following preliminary desktop review, on-site inspections generally last for about an hour on average and involve one staff member of the MoE and one other contractor from an accounting firm who is responsible for conducting the inspection. It does not appear that such on-site duration could allow the MoE to conduct a thorough inspection, especially on more complicated transactions e.g. that involve PEPs and beneficial owners. The MoE is planning to add more risk factors, e.g. company data, export data and companies involved in counter-party to the transaction, when planning the next 320 inspections over the next 18 months. New entities will also be a focus of future inspections. For this purposes, the MoE will allocate significant resources (11 staff and 29 out-sourced persons on contract to end 2019). Consultants recruited for this purpose have been subject to a vetting process and provided with training.

401. Overall, the level of both on-site and off-site AML/CFT-specific inspection (in terms of number, frequency, duration, scope and depth of inspection) is low. Risk-based approach of inspection has not been consistently applied by all DNFBP supervisors (particularly for MoE). DNFBP supervisors also have not adjusted the subsequent monitoring programmes according to the inspection results, or risk level identified to correct the significant deficiencies identified.

Remedial actions and effective, proportionate, and dissuasive sanctions

Financial Institutions

402. Financial supervisors have a wide range of supervisory and enforcement measures at their disposal, ranging from warnings, imposing fines, to revocation of licences. The most common breaches of AML/CFT obligations include incomplete CDD information or procedures, and failure to report unusual transactions. With the exception of the MSB sector, the overall level of remedial and sanction actions imposed on supervised entities is rather low, i.e. the severity of sanctions and level of fines imposed (especially in the securities and insurance sectors). For instance, the BoI did not impose administrative sanctions in 2016 and 2017. That said, it applies other types of sanctions, for example requirements for additional capital, limitations on dividend allocations, requiring the closure of activities abroad and personal sanctions to supervised entities, on 14 occasions in 2013-2017 on breaches of AML/CFT and prudential requirements such as failure to complete CDD processes. The BoI considers these measures very effective and deterrent. The Postal Bank has imposed fines in case of non-compliance with UAR requirements, and occasionally applies other types of sanctions such as termination of the business relationship and the confiscation of deposited guarantee funds.

403. For the MSB sector, the MoF/ITA had actively made use of high fines, licence suspension, and initial of prosecutions against non-compliance with AML/CFT obligations. That said, such measures do not appear to have created sufficient deterrence, as the supervisor continues to identify multiple deficiencies in each inspection.

404. Supervisors generally rely on communicating supervisory messages to supervised entities directly and issuing corrective action plans, aiming at preventing potential/further ML/TF abuse. In a few cases, supervisors (e.g. ISA and Postal Bank) have recommended that the supervised entity concerned introduce manpower changes (e.g. suggesting removal of a compliance officer from office). Given few remedial and sanction actions and low level of sanctions imposed (see table below), it is difficult to conclude that such measures are effective, proportionate, and dissuasive.

Table 27. **AML/CFT Remedial and Sanction Actions Imposed by Financial Supervisors**

	2014	2015	2016	2017
BoI on Banks				
Warnings	0	1	0	0
Referral to Sanctions Committee	2	2	0	0
Fines	2 (NIS 3.1m/ EUR 724 400)	2 (NIS 5.35m/ EUR 1.25m)	N/A	N/A
- Range of Fines	NIS 0.8 m – NIS 2.3m	NIS 1.15m – NIS 4.2m	N/A	N/A
Reprimands	N/A	N/A	N/A	N/A

	2014	2015	2016	2017
Corrective Actions	2	1	1	1
Suspension of Licence	0	0	0	0
Revocation of Licence	0	0	0	0
Financial sanctions	2	2	0	0
Capital sanctions	1	3	3	3
Dividend allocations	0	2	3	3
Personal sanctions	0	1	0	5
Requirement to close activities abroad	0	0	1	3
ISA on Trading Platforms				
Warnings		N/A		2
Referral to Sanctions Committee		(as ISA first started inspection in 2017)		N/A (Note1)
Fines				
- Range of Fines				
Reprimands				N/A
Corrective Actions				6
Suspension of Licence				0
Revocation of Licence				0
ISA on Stock Exchange Members				
Warnings	0	3 (2 verbal & 1 written)	0	1
Referral to Sanctions Committee	1	1	0	0
Fines	1	0	1 (Note 2)	N/A
- Range of Fines	EUR 21 176	0	EUR 59 701	N/A
Reprimands	0	0	0	0
Corrective Actions	0	4	2	1
Suspension of Licence	0	0	0	0
Revocation of Licence	0	0	0	0
ISA on Portfolio Managers				
Warnings	0	0	0	0
Referral to Sanctions Committee	1	0	0	0
Fines	1	0	N/A	N/A
- Range of Fines	NIS 41 000 (EUR 9 600)	N/A	N/A	N/A
Corrective Actions	0	0	0	0
Suspension of Licence	0	0	0	0
Revocation of Licence	0	0	0	0

	2014	2015	2016	2017
CMISA on MSB Providers				
Warnings	2	1	0	0
Referral to Sanctions Committee	15	10	9	11
Fines	15 (NIS 510 000/ EUR 119 200)	10 (NIS 1.038m/ EUR 242 600)	9 (NIS 900 000/ EUR210 352)	11 (NIS 2.475m/ EUR 578 300)
- Range of Fines	NIS 7 500 – NIS 900 000 (EUR 1 752 – EUR 210 352)			
Reprimands	0	0	0	0
Corrective Actions	0	0	0	0
Suspension of Licence	4	6	5	3
Revocation of Licence	0	0	0	0
CMISA on Insurance Companies				
Warnings	3	1	1	0
Referral to Sanctions Committee	0	1	0	0
Fines	0	1	N/A	N/A
- Range of Fines	0	NIS 406 000/ EUR 94 900	N/A	N/A
Reprimands	0	0	0	0
Corrective Actions	1	2	2	1
Suspension of Licence	0	0	0	0
Revocation of Licence	0	0	0	0
MoC on Postal Bank				
Warnings	0	0	0	0
Referral to Sanctions Committee	0	1	0	5 (ongoing)
Fines	N/A	1	N/A	N/A
- Range of Fines	N/A	NIS 24 000/ EUR 5 600	N/A	N/A
Reprimands	N/A	N/A	N/A	N/A
Corrective Actions	0	0	0	0
Suspension of Licence	N/A	N/A	N/A	N/A
Revocation of Licence	N/A	N/A	N/A	N/A

Note 1: Pending the Sanction Committee to convene, the ISA will refer one case for its consideration.
Note 2: This refers to the inspection concluded and referred to Sanctions Committee in 2015, but the fine was imposed in 2016.
Source: BoI, CMISA, ISA, and MoC.

DNFBPs

405. DNFBP supervisors/SRBs are provided with enforcement powers ranging from written warnings, imposition of fines, to revocation of licences. Enforcement is mainly related to non-compliance with CDD processes (e.g. inadequate documentation), probably due to unfamiliarity with new AML/CFT obligations. Given the very few inspections conducted to date, it is difficult to draw conclusions on the effectiveness of remedial actions and the dissuasiveness of sanctions.

406. Since the commencement of AML/CFT supervision in 2016, MoJ relies on a written follow-up process to correct non-compliance actions and has issued

11 warning letters to five accountants and six lawyers, and referred two cases to the Sanctions Committee (established in 2017). The number of enforcement actions issued does not correspond to the number of supervised entities. The level of fine imposed is also considered not dissuasive and proportionate. Only one entity was imposed with a fine of NIS 2 000 (EUR 467) for not performing proper CDD, and another entity was imposed with a fine of NIS 20 000 (EUR 4 670) - contrary to maximum fine of up to NIS 2.260 million (EUR 528 100).

407. The MoE also did not demonstrate that it has taken remedial actions following inspections and the Sanctions Committee is still in the process of being set up. It is not possible to draw conclusions on the effectiveness, proportionality and dissuasiveness of enforcement and sanctions. That said, the MoE has started to prepare for case referrals to the Sanctions Committee.

Table 28. **AML/CFT Remedial and Sanction Actions Imposed by DNFBP Supervisors/SRBs**

	2016	2017	2018 (until March)
Accountants (total supervisory population of 18 432; 0 on-site inspections conducted)			
Warnings	5	0	0
Referral to Sanctions Committee	0	0	0
Fines	N/A	N/A	N/A
Reprimands	0	0	0
Corrective Actions	0	0	0
Suspension or Revocation of Licence	0	0	0
Lawyers (total supervisory population of 63 782; 6 on-site inspections conducted)			
Warnings	84	22	0
Referral to Sanctions Committee	0	0	2
Fines	0	0	1 (NIS 2 000/ EUR 467)
Reprimands	0	0	0
Corrective Actions	0	0	0
Suspension or Revocation of Licence	0	0	0
Diamond Dealers (total supervisory population of 2 348; 18 on-site inspections)			
Warnings	0	0	0
Referral to Sanctions Committee	0	0	1
Fines	N/A	N/A	N/A
Reprimands	0	0	0
Corrective Actions	0	0	0
Suspension or Revocation of Licence	0	0	0

Source: MoE and MoJ.

Impact of supervisory actions on compliance

Financial Institutions

408. There are indications that supervision does have a positive impact on overall compliance levels, although this varies from sector to sector.

409. The BoI has a close supervisory relationship with banks, and has made use of intensive prudential inspections for AML/CFT purposes. The BoI observed a decrease in non-compliance in number and severity in recent years, which it attributes to its wide range of supervisory measures. The BoI also stressed the importance of other communication channels with the industry (e.g. Compliance Officers' Forum and regular visits with senior bank management). Such contacts enable the BoI to better assess the culture and level of compliance and address issues in a preventtive and proactive fashion. The BoI also considers that the growing number of UARs points to an increased level of awareness for AML/CFT issues among FIs. Nevertheless, the number of enforcement actions is generally low.

410. The ISA considers its increased use of automated software for monitoring and publication of sanctions results in an increased level of AML/CFT compliance among some of the supervised entities. The ISA added that applied sanctions ultimately resulted in improved risk rating for the respective supervised entities, after the deficiencies were resolved. (See table below).

411. Regarding MSBs, the limited supervisory measures undertaken by the new supervisory framework of CMISA does not seem to have brought positive effect on compliance yet. Against the background of the high number of heterogeneous supervised entities, the fact that in every recent inspection deficits were found and the classification of this sector as higher-risk in the NRA, more inspections have to be performed and stronger sanctions be applied in order to create a stronger supervisory impact. Regarding the insurance sector, the number of inspections and the number of supervisory measures are rather low, which are not incommensurate with the ML/TF risk profile of the sector.

412. The Supervision Department of the Postal Bank also considers its enforcement actions have a positive impact on the local branches, as illustrated by a reduction in the number of UARs (unlike BoI's interpretation) and cross-border transactions. For the latter, enforcement actions appears to have the unintended effect of de-risking instead.

DNFBPs

413. DNFBP supervisors commenced AML/CFT supervision only in 2016 and 2017. As their supervisory programmes are at a very early stage of development, the number of sanction measures imposed is very low and supervisors have not yet started a second-round/subsequent follow-up visits. It is therefore difficult to draw conclusions on the impact of the supervisors' actions on compliance.

414. Nevertheless, the MoJ considers that its inspection regime useful in raising AML/CFT awareness among supervised entities. The MoE approach to supervision in the diamond industry would benefit from the implementation of an inspection plan based on risks. Over the next 18 months, the MoE plans to conduct some 320 inspections and will be based on risk factors (e.g. the scope of trade, type of trade – import, export, or local trade, and number of years in business). Noting that its current on-site inspection generally lasts only one hour for each supervised entity (diamond dealer), it is questionable whether such inspection is sufficient in creating any supervisory impact on the dealers. The MoE should accord sufficient

resources (e.g. time) for inspection and make reference to actions made by other supervisors to increase supervisory effect on supervised entities.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

Financial Institutions

415. Generally, financial supervisors promote a clear understanding of AML/CFT obligations and risks, but the extent of this varies. While all supervisors have issued AML/CFT regulations and circulars, only some supervisors (e.g. BoI and ISA) have issued guidance documents to promote, mainly, the understanding of AML/CFT obligations. Separately, IMPA publishes risk typologies-related information to supervised entities.

416. Supervisors such as the BoI and the ISA have a range of different communication channels that they use, namely formal guidance like circulars, Q&As and guidance documents, conferences, training and seminars and other regular fora or informal contacts with supervised entities. They generally prefer formal documentary channels to disseminate regulatory messages. Though the level of interaction is frequent and intensive, the materials and interaction are generally well received by supervised entities. As for the CMISA, it also conducts outreach and issues guidance to facilitate supervised entities' understanding of AML/CFT obligations and risks – especially in the MSB sector, which should continue and be strengthened. This is particularly essential as MSBs are being incorporated in the AML/CFT licensing regime. While the Supervision Department of the Postal Bank does not have an intensive engagement programme, it has engaged with responsible persons and branches of Postal Bank, to some extent, to promote understanding of ML/TF risks.

DNFBPs

417. DNFBP supervisors have mainly made use of training seminars to raise supervised entities' awareness of AML/CFT obligations and ML/TF risks in the sector, allowing interaction between supervisors and supervised entities in the early incorporation of DNFBPs in the AML/CFT regime. In addition to the above approach, increased on-site inspections would serve to enhance an understanding of ML/TF in the DNFBP sector and of their obligations. Statistics on training seminars are as follows:

Table 29. **Training Courses Delivered from 2015 Q4 to 2018 Q1**

Supervisor	Sector	Number of Courses	Estimated Attendance
MoJ	Lawyers	15	736
MoJ	Accountants	12	520
MoE	Precious Stones Dealers (Diamonds only)	3	500

Source: MoE and MoJ.

418. Specifically, the MoJ has invited an overseas AML/CFT expert to give a seminar to the Israel Bar Association (an SRB) and Council of Certified Public Accountants under the MoJ, and BSP providers. The MoE, in collaboration with the

IMPA, arranged two conferences for diamond dealers on AML/CFT obligations in the past two years. The issues covered included AML/CFT legislative requirements such as CDD and record keeping. While supervisors should continue these efforts they should also consider making a wider range of training materials available to the DNFBP sector such as publishing good/best practices, and other supervisory documents, in addition to red flags, Q&As and guidelines. This will further promote an understanding of AML/CFT obligations and the different ML/TF risks faced by the sector and Israel as a whole.

Overall conclusions on IO.3

419. **Israel has achieved a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

Israel has achieved a substantial level of effectiveness for IO.5.

a) Information on the creation and types of legal persons is publicly available.
b) Israel has undertaken a risk assessment of legal persons and arrangements. Understanding of risks is substantially more developed in practice than the risk assessment suggests but assessment and understanding of vulnerabilities and misuse are not yet comprehensive.
c) The ICA maintains registers of companies, partnerships and public trusts, which are publicly accessible. For the vast majority of legal persons, registered information also constitutes beneficial ownership information. Some steps are taken to manage the adequacy, accuracy and currency of data on companies but these are not yet comprehensive. Nevertheless, based on feedback provided by the ICA, other authorities and banks (which have access to almost all information by the ICA on companies) registered information is reliable.
d) The ITA maintains a register of Israeli resident trusts and holds information on the beneficial ownership of companies and trusts. It is an important source of beneficial ownership information; validation of the adequacy, accuracy and currency of this information is undertaken on the basis of significant sampling and is comprehensive. The high quality of information supports a significant number of cases against legal persons by the ITA and by other LEAs and the SAO.
e) All legal persons and trustees of legal arrangements which make filings with the ITA must have a bank account.
f) Other mitigating measures have also been taken to support transparency of beneficial ownership framework (e.g. the addition of a provision in company legislation in 2016 preventing the issue of bearer securities and controlling existing bearer securities).
g) Banks are the main source of beneficial ownership information. Banks understand risk and have high standards of CDD in relation to beneficial ownership, consistent with the risks identified. Beneficial ownership information for legal persons and legal arrangements is available promptly. Very good quality beneficial ownership information is also available from other FIs and DNFBPs. Information held by banks is the highest quality among all supervised entities, and supports the large number of cases against

and involving legal persons and arrangements by LEAs and the SAO in light of the adequacy, accuracy, and currency of such information.

h) There is a range of effective mechanisms which lead to beneficial ownership information for legal persons and legal arrangements being held in Israel; empirical data would be required to confirm whether this covers all persons/arrangements.

i) The ICA has taken some substantial steps to impose sanctions. However, the range of sanction powers available to it and its overall use of sanctions are not comprehensive. The approaches to sanctions applied by the ITA and supervisors of FIs and DNFBPs varies are not sufficiently effective.

Recommended Actions

a) A more in-depth analysis of the risks of legal persons and legal arrangements involving all relevant authorities should be conducted as planned.

b) A co-ordinating mechanism should be established so as to ensure adequate mitigating measures are put in place in response to the assessment, and that the effectiveness of use of the measures is monitored and changes made to the framework where appropriate. This should include mechanisms to ensure that Israel can demonstrate that it obtains and retains adequate, accurate and current beneficial ownership information on all legal persons and arrangements.

c) The ICA should adopt a more proactive approach to managing the information on its registers and also adopt risk based approaches to ensuring that data is adequate, accurate and current.

d) The ICA should be provided with additional powers of sanction (e.g. power to strike off companies subject to a notice period) with a view to cleaning the register, and enhancing its approach to the application of sanctions.

420. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.[35]

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

421. Information on the creation of companies and partnerships is publicly available on ICA's website[36], which includes procedures, guidelines, required documentation, application forms and applicable legal provisions, as well as the list of registered companies and partnerships. The website also specifies the information and procedures involved for making changes to the registered

35. The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

36. http://www.justice.gov.il/units/RasutHataagidim/Pages/default.aspx

information held by the ICA after incorporation. Information regarding legal persons (NPOs) is also publicly available (see R.8 and IO.10). As for legal arrangements, ITA's website separately provides information regarding the reporting obligations to the ITA in relation to trusts.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities created in the country

422. Israel has articulated a separate risk assessment of legal persons and arrangements and those businesses/professions which provide services to them. All relevant authorities were involved in the exercise, which was co-ordinated by IMPA. In order to understand the different degree and pattern of ML/TF threats, vulnerabilities and risks posed in relation to the various structures, the authorities sought to estimate the asset size of various types of legal persons and arrangements, and made use of UAR findings and case examples (e.g. companies issuing false invoices, tax avoidance through the use of trusts). There are differences in the level of threat emanating from different types of legal persons and arrangements. Control measures with regard to Israeli companies were also considered. Overall, the threat of ML by using legal persons and legal arrangements was rated as medium-high with, respectively, companies and trusts presenting the highest threats. The risks associated with legal persons and legal arrangements were concluded as being moderate-high.

423. The NRA also identified that there was insufficient information available on the scale of ML through legal persons and arrangements, and that further analysis should be conducted. This conclusion contributing significantly to the rating, which is considered appropriate. Measures to remediate the gaps were included in the NRA action plans.

424. Examples where the analysis included in the risk assessment was not comprehensive include: various characteristics of legal persons and arrangements (such as the possibility of cross-border activity, and the use of nominees and of TCSPs were examined at a theoretical level. Services provided by BSPs and TCSPs were not assessed comprehensively. The ITA's system was referenced as needing to provide easier search capability and additional information.

425. The Israeli authorities have, based on the NRA results, implemented measures which have developed their understanding of ML risks posed by legal persons and arrangements substantially. The ICA has started to make use of a new IT system to allow better understanding of ownership information and to co-ordinate the exchange of further information between the ICA and LEAs. The ITA has developed and uses a new IT system which has addressed the deficiency identified in the NRA. IMPA is working with the ISA to identify suspicion of ML involving public companies. Cases involving legal persons and legal arrangements undertaken by LEAs and SAO have also led to increased understanding. FI supervisors appear to have enhanced their understanding of beneficial ownership breaches in their sectors. IMPA, LEAs and SAO, and to some extent the ICA, understand better the TCSP sector (which mostly includes lawyers and accountants) and the way they operate, and the limited use of nominees. All LEAs indicated that they continue to identify the ML risk from legal persons and legal arrangements as moderate-high.

426. Due to its geographical location, relatively small turnover in Israel's stock exchange market, domestically-focused financial sector, lack of government-led incentives for foreign investment through legal persons or legal arrangements, and active notification by the banking sector to ICA and ITA in relation to foreign ownership, the Israeli authorities do not see the country as a natural target for foreign money launderers. This assessment is commensurate with the number of foreign corporate owners in the country. Of some 11 000 companies with foreign ownership, only 4 500 have corporate owners. Asset holding companies for foreign persons are not a material feature of the system. There are only 2 429 Israeli resident trusts (with some 2 000 beneficial owners). The vast majority of beneficial owners have financial activity in Israel and are monitored by the ITA and banks.

427. The NRA also identifies TF threats and risks posed by legal persons and arrangements, though considering that these structures are not a significant source of TF (see IO.10).

428. Israel plans to undertake a more detailed risk assessment with regard to legal persons and legal arrangements. The action plans include recommendations to establish an inter-ministerial committee to deepen the analysis of the risks and to examine mitigation measures such as the establishment of a trust registry and a database of beneficial owner information for companies.

Mitigating measures to prevent the misuse of legal persons and arrangements

429. Israeli authorities (incl. ICA, ISA, ITA, and financial/DNFBP supervisors) implement a number and range of long standing measures and controls to mitigate risks of misuse by both legal persons and legal arrangements for ML and TF. While it cannot be certain that the entirety of legal persons is covered by the measures and controls in relation to beneficial ownership substantially all legal persons which have financial activity or assets are subject to the mechanisms. See also c.24.6 and c.24.7.

ICA

430. The ICA has adopted transparency measures on basic information during company and partnership formation. Applicants are required to use prescribed forms, which require the basic information specified at c.24.3 and 24.4, as well as the contact details of the company in Israel. Information on the purpose of the legal person is provided by way of narrative (as well as by way of the contents of the constitutive documents). The online form, which constitutes 85% of applications, requires each shareholder to confirm whether the shares are held as trustee. Both the online process and the paper form application for registration involve an Israeli lawyer. The by-laws and a declaration of willingness to be a shareholder must be signed by each of the founding shareholders in the presence of an Israeli lawyer; the directors must also sign the application in front of a lawyer and confirm their willingness to be directors. The lawyer must obtain identification information on each signatory. This is usually an identification card for Israeli citizens and a passport for foreign individuals.

431. In addition to the mandatory involvement of an Israeli lawyer for both the online and paper registration process to verify the signatures of shareholders and directors, the vast majority of applications made in paper form are submitted to the registry by lawyers who are subject to CDD obligations, including an obligation to obtain and retain beneficial ownership information. The ICA confirmed that the vast majority of all registered company applications are submitted by Israeli lawyers. These lawyers are subject to CDD obligations on beneficial ownership. The MoJ is in charge of verifying compliance with these CDD obligations.

432. The ICA has implemented additional mitigation measures in relation to potential abuse by use of online applications. Such applications must be submitted by a lawyer subject to AML/CFT obligations, who is identified by an electronic certificate. The identity details of that lawyer are checked against the Bar Association's register to confirm he/she is a qualified lawyer and that his/her licence has not been suspended or revoked. There is one exception, which is rarely used, when the application is submitted by a shareholder who is the sole shareholder and a director of a company. Such applications require the identification of that shareholder on the online system by an electronic certificate (which is issued only after a face-to-face meeting with the shareholder/director concerned). In addition, the ICA requires the applicant (i.e. the lawyer or shareholder) to upload a copy of the by-laws, signed in the presence of a lawyer required to verify the signature of the shareholder on the articles of association – hence, sole shareholders making online applications are also subject to identification measures.

433. Where a shareholder/director is not an Israeli citizen, the ICA requires the applicant to provide a certified copy of the passport for individuals and a certified certificate of incorporation for legal persons. Instead of according resources to conduct verification to this group of foreign shareholders, which only constitutes 1.2% of the companies, the ICA relies on the certification conducted by an Israeli lawyer, by a foreign notary, or by an official representative of Israel in the foreign country where the passport or certificate was issued. This appears to be a proportionate approach adopted by Israel in preventing the misuse of legal persons.

434. Directors can be individuals or legal persons but, if the director is a legal person, it must also appoint an individual director to act on its behalf.

435. In addition to the foregoing, the ICA adopts a number of measures at the application stage to validate reliability of company information to be included on the register. These include: checking its existing records in the register of the relevant type of legal person (there would be merit in extending this to cover other ICA registers), the register of bankrupt individuals and the population register. The ICA emphasised that the population register is of very high quality and that, in light of the high proportion of companies owned by Israeli residents, this validation check is particularly useful. The ITA also confirmed the accuracy and value of the population register in validating its information. Company formations have been refused by the ICA e.g. in cases of a similar, confusing or potentially misleading company names. More than 20% of applications are refused, which helps the management of a higher quality register.

436. Additional measures include: requiring companies to provide updated information within fourteen days of the change; requiring companies to provide an annual report confirming the basic information previously provided to the registry by the end of the calendar year and making such annual reports publicly available so that the public can see when a report was last submitted and its contents; and introducing legislative amendments to make it mandatory for companies to report to ICA on whether shares are held in trust.

437. The ICA's experience is that routine updates of changes to information are nearly always provided in a timely manner and are accurate – although it does not maintain statistics or undertake specific validation of the information. It also noted that the banking sector is vociferous in demanding accuracy from the database and the importance to companies of updating information at the registry in order for the changes to be recognised and effective from the perspective of third parties dealing with the companies.

438. The ICA uses the annual reports provided by companies as a back-up and periodic verification of the adequacy, accuracy and currency of the changes to the information required to be reported to it. The ICA checks every annual report submitted against the information in its database. The reports support the ICA's view that the information in the registry on financially active companies is accurate and up to date. The ICA has taken proactive steps to minimise any delay in providing the report by issuing an alert to companies which have not filed the report in a timely manner (within 30 days of the end of the year); this is followed by a subsequent check on compliance (in about March of the following year). All companies that do not submit annual reports (including inactive companies) are declared to be "violating companies", a status which is publicly accessible and which allows the ICA to refuse to register charges and to delete charges previously registered. This significantly limits the ability of companies to obtain credit, change the company name or purpose, and register mergers. The ICA can also deny the controlling shareholder and any director who has not paid a fine imposed by the ICA from registering new companies. In addition, since 2016 the ICA has imposed fines against some companies which have not submitted their annual reports. The measures being taken by the ICA appear to be well known.

439. The measures taken have increased the compliance rate of filing annual reports by financially active companies from 10% (some 20 000 annual reports) in 2010 when the sanction was introduced to 85% (some 160 000 annual reports) in 2017. Inactive companies (i.e. companies which have closed their files/books with the ITA but have not yet been dissolved or companies that have never opened a file with the ITA) which have not submitted their annual report are declared to be violating companies.

440. The ICA advised that the use of its published information by banks, the ITA and other authorities contributes to the high degree of accuracy of information and to the timely updates of changes by companies. In practice, FIs and DNFBPs such as banks and lawyers, as well as the ITA, are cross-checking the basic and beneficial ownership information provided to them by companies with the information available at the registry. Banks are also continuously monitoring changes in the registries, including designations of violating companies (through

automated computerised interfaces) and inquire with their customers with regard to any potential discrepancies.

441. Overall, therefore, the ICA sees the ongoing requirement to file changes to basic ownership information on companies as providing reliable basic ownership information; and that its view is validated by the checks undertaken by the private sector, the confirmations provided in annual reports and the successful use of the information by the private sector and the authorities. Registered information also comprises beneficial ownership information where the legal owners are individuals or where the ownership chain comprises only of registered Israeli companies/partnerships.

442. Regarding partnerships, the ICA requires the notification of updated information within seven days of the change. As with companies, specific checks are not made but the ICA's experience is that changes are mostly notified to it on time as there are civil mechanisms in place to provide incentive to do so. The ICA relies on partners' understanding of their liabilities and the demands of the banking sector as the motivating forces for managing partnerships and therefore to keep information provided to the ICA up to date. There is no requirement for partnerships to provide annual reports. A number of changes are planned to partnership legislation in the short term, including an annual reporting obligation.

443. Turning to the registration of public trusts (i.e. charities – also see IO.10), applications are made on a prescribed form, which includes the name of the settlor, the trustee, the purpose of the trust, and the trust assets. There are no checks on the information provided. Annual financial statements are also required but provision of these is not verified by the ICA. The information at the registry is publicly available. The vast majority of these trusts, as with other types of trust, are created by lawyers or accountants subject to AML/CFT obligations. The ICA intends to promote greater transparency in relation to public trusts.

ISA

444. Companies which have listed their shares, or which have issued bonds listed, on the Tel Aviv Stock Exchange (TASE) are under the supervision of the ISA and are subject to disclosure requirements. These "TASE companies" are required to disclose information to the ISA and the public, inter alia, on the identity and holdings (number of shares and voting power) of persons holding more than 5% of the issued share capital/voting power), and the identity of senior officers such as directors and persons entitled to appoint such senior officers (principal shareholder).

445. In addition, companies are subject to ongoing disclosure requirements when specific events and material events occur. This includes certain changes to information provided (date and manner of change, and the number of shares and voting power held before and after the change). Depending on the nature of the event, changes to information must generally be advised to the ISA and to the public within 3.5 to 24 hours. TASE companies also include information on shareholders in periodic reports to the ISA and to the public and this will include beneficial ownership where the beneficial owner is a "principal shareholder". TASE companies are also required to keep their registers up to date.

446. The ISA conducts audits of companies and information held where an issue triggers its attention.

447. Both the ISA and the ITA consider the information held by the ISA on TASE companies is reliable. This is borne out by the investigations undertaken by these authorities.

ITA

448. The ITA holds basic and beneficial ownership information on all legal persons which have an income, which own real estate, which buy/sell real estate, which have any employees in Israel, which have any assets in Israel or which undertake any financial transactions. All legal persons making disclosures to the ITA are required to have a bank account and are subject to banks' CDD requirements, including those on beneficial ownership.

449. The definition of beneficial ownership which applies to disclosures to the ITA is the same as that which applies to FIs. The ITA, therefore, holds information on the directors, shareholders and beneficial owners of companies and partnerships (which information is updated annually). It is proactive in checking relevant parties, including beneficial owners. It routinely uses information from the ICA and is provided with the ICA's public records at the end of each day. The validation checks include making enquiries of third parties such as banks and other authorities. Some 5% of its files of legal persons (both active and inactive) are selected on a sample basis to a full audit and validation each year to ascertain the accuracy of information provided and tax payable. These audits cover a five year period. All legal persons have been covered by these checks and a substantial number have been subject to audit more than once.

450. Legal arrangements are subject to the same requirements and approach as that articulated above for legal persons except that 45% of trust files (including beneficial ownership) have been subject to a full audit and validation of information in recent years so as to ascertain and ensure the accuracy of information and tax payable. Information provided includes names and residency of settlors, trustees, protectors and beneficiaries. The ITA also maintains a database of Israeli resident trusts (and foreign resident trusts which have assets in Israel).

451. Based on its validation activity and case experience, and the experience and information held and used by other authorities and FIs, the ITA is confident that legal persons and trustees of legal arrangements provide accurate and updated information for the annual filings and that any inaccuracy would be very rare. It could not remember any omissions or inaccuracies. The ITA has found the basic and beneficial ownership information provided to it for legal persons and legal arrangements for its own purposes to be adequate, accurate and current. This view is supported not just from its own validation and case activity but also use of the ITA's information by other authorities and its ability to successfully address foreign requests for information.

Requirements on legal persons and trustees

452. C.24.4 and 24.5 address the requirements for legal persons to hold information. The registered office of a company is also required to hold information when shares are held by a trustee. LEAs confirmed that companies required to provide information to them are meeting this obligation.

453. The Trust Law provides that trustees must keep account of all the affairs of a trust. LEAs confirmed that trustees (e.g. lawyers, accountants and banking group trust companies) required to provide beneficial ownership information in relation to trusts have provided correct, up to date information to them.

FIs and DNFBPs

454. The AML/CFT framework which applies to FIs and DNFBPs includes mitigating measures and controls relevant to legal persons and arrangements. C.10.10 and 10.11 specify the extent to which the various supervisory orders satisfy the requirement to verify the identity of beneficial owners. In addition, other documentation has been issued by way of mitigating measures. In particular, this includes questions and answers issued by the BoI, which address the identification of controllers of legal persons with complex structures; and questions and answers issued by the ISA, risk management circulars for stock exchange members, trading platforms and portfolio managers and a Know-Your-Customer model form for trading platforms; and questions and answers published by the supervisor of BSPs. In addition, IMPA has published a red flags document for BSPs which covers the establishment of legal persons and accounts for trusts. In light of the ability of LEAs generally to obtain high good quality information from banks without recourse to other means, the impact of the deficiencies identified throughout R.10 is not significant.

455. Over the last few years, the BoI has made use of its intensive on-site and off-site inspections to identify whether there are deficiencies in relation to the quality of beneficial ownership information held by banks. Deficiencies have, for example, included not using additional sources of information on a risk based approach to verify beneficial ownership information provided by customers; breaches in the collection of declaration forms for beneficial owners and therefore in recording information; and not recording the individual at the end of the chain of ownership. Overall, the deficiencies have not been material, have been remedied and mostly date to 2013. The level of deficiencies now identified is low and the deficiencies themselves are not significant. Banks understand risk and have high standards of CDD in relation to beneficial ownership, consistent with the risks identified.

456. Legal persons with foreign beneficial ownership are subject to enhanced due diligence by banks, which includes both additional customer take on checks and ongoing monitoring. With reference to trusts, in light of banks' concerns about the high level of risk and the cross-border nature of trusts, most banks impose additional controls during on-boarding stages for applications submitted by BSPs for trusts. They are also subject to enhanced monitoring.

457. The Supervision Department of the Postal Bank found a total of 17 breaches of beneficial ownership CDD requirements with regard to legal persons during an extensive audit process conducted between the years from 2013 to 2017; the

breaches were minor in nature. The picture found by the ISA since 2013 is more positive. Generally, stock exchange members comply with the requirements while only a few deficiencies were identified at portfolio managers (including deficiencies in completion of the beneficial owner declaration). On the basis of its off-site and on-site supervision, as well as its investigations, the ISA considers that its licensees hold high quality (adequate, accurate and current) beneficial ownership information on their customers. The supervisor of MSBs has found that failings comprise gaps in obtaining CDD on the person acting on behalf of a legal person and incomplete beneficial owner declarations (missing signatures). Gaps found by supervisors have been remediated. The CMISA has found no violations of beneficial ownership requirements by insurance companies, which seems to be commensurate with the overall low ML/TF risks faced by this sector.

458. Strawmen not detected by FIs or DNFBPs, have been used by criminals but LEAs and prosecutors confirmed that these cases have been very rare (perhaps five cases in the last decade). No other failings in relation to nominees have been noted by the authorities.

Other measures

459. Regarding measures to mitigate potential abuse brought by bearer shares, Israel passed an amendment to the Companies Law in 2016 to specify that a company may not issue or allot any type of bearer security, and that no rights attaching to bearer securities issued prior to that time could be exercised. The authorities have not observed any use of bearer securities either in on-site inspections by supervisory authorities or in investigations by LEAs. In addition, the ITA is not aware of any bearer securities within its files on legal persons.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons created in the country

460. In respect of legal persons, access to the registers of companies and partnerships held by the ICA is simple and fast, and have been routinely used by other authorities (e.g. ITA), as well as FIs (especially banks). Registered information is generally adequate, accurate and current, as confirmed by ITA, IMPA, and LEAs. Although banks had commented that they had not always found the information to be reliable, the ICA explained that this was a short term issue, lasting a few months, resulting from an overhaul of the ICA's IT systems near the end of 2017. This was an exception and, as explained in IO.4, is not considered a major deficiency. The ICA also explained that it engages in routine dialogue with the banking association and the matter had already been raised in that forum. At the time of the onsite, the ICA was comfortable that the issues had been resolved. It was also of the view that, where a bank had any doubt about the accuracy of information, it would check the matter by contacting ICA staff.

461. Banks met appear to obtain all required CDD, including in relation to beneficial owners of legal persons. Covered DNFBPs met (including lawyers and accountants) are aware of the requirement to understand who is behind each transaction and appear to ensure that appropriate CDD is conducted on the beneficial owner. Information from banks, lawyers and accountants is available promptly. Supervisors have timely access to information held by FIs and DNFBPs.

462. The ISA and the ITA have worked closely together on cases of fraud and market manipulation (a few cases each year); obtaining good quality beneficial ownership information has been a vital part of achieving success in these cases. The combination of tools used by the two authorities appears to be sophisticated, including detailed analysis of transactions and trading patterns, leveraging of IP addresses and use of telephone system information. Both authorities focus significant effort on looking for connections between beneficial owners and they have been able to find them.

463. In addition to the joint cases with the ISA mentioned above, the ITA undertakes investigations for its own tax purposes or it needs to obtain beneficial ownership information to meet a TIEA request. It succeeds in obtaining adequate, accurate and timely information on beneficial owners promptly and which meets operational needs. Checking overseas ownership is the main concern and quite significant checking is involved in relation to non-Israeli residents who are included in ownership structures of Israeli companies and where offshore finance centres feature in those structures. Joint ventures between Israelis and non-Israelis used to present issues but this is no longer the case. The ITA considers information from Israeli banks to be accurate and complete in virtually all cases; it also matches the information it holds with the databases provided by the ICA. If necessary, in order to check data, bank staff are interviewed, security camera film is reviewed, other parties to transactions are met, information is obtained from IMPA, as well as other parties contacted. The ITA has responded successfully to TIEA requests for both civil and criminal cases.

464. Access to basic and beneficial ownership information held by BSPs who are lawyers is feasible and prompt upon use of a court order. Client privilege is not considered as a hurdle by the authorities. Authorities (e.g. INP and ITA) also confirm the reliability and good quality of information obtained from lawyers, which includes all necessary records, including agreements, transaction details, invoices and emails, as well as beneficial ownership information.

465. More generally, IMPA, LEAs and the SAO have confirmed that beneficial ownership information is available within Israel; that they have timely access to the information; that it is adequate, accurate and current; and that it supports the large number of successful cases against legal persons or which otherwise include legal persons. The assessment team also notes that individual authorities have significant information available as a result of the proactivity discussed in other IOs and that this is leveraged by close co-operation and sharing of intelligence. As part of this pattern of connectivity between authorities, IMPA, like the ITA, has direct access to the ICA's updated database. In addition, LEAs have access, upon request, to IMPA's database, which contains information on beneficial owners that was received from FIs as part of their reports (both UARs and CTRs), as well as information received from foreign FIUs. LEAs can also receive beneficial ownership information through their foreign counterparts, as elaborated under IO.2.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

466. The ICA maintains a database of some public trusts (also see IO.10), which includes information on settlors; trustees; beneficiaries; any other beneficial owners; and the types, purpose and establishment date of the trust. In addition, the ITA holds significant information on trusts including the purposes of the trusts and the beneficiaries in a single database, which is available to its investigators and for sharing with other authorities upon request.

467. The text above on timely access to basic and beneficial ownership information for legal persons applies equally to trusts with the exception that the ITA has devoted greater focus on trust structures.

468. IMPA, LEAs and the SAO also have had timely access to basic and beneficial ownership information, and therefore have been able to pursue investigation involving trusts.

Effectiveness, proportionality and dissuasiveness of sanctions

469. Although Israel is one of very few jurisdictions which has proactively charged and convicted legal persons of financial crimes or ML, the range of sanction powers available to the ICA is not comprehensive. It is not empowered to strike off a company or to approach the court to apply this remedy (although legislation has been issued for consultation). There are a significant number of inactive companies and the power of strike off would be beneficial in dealing with these.

470. The ICA has taken some substantial steps in relation to the imposition of sanctions. In 2010, the ICA began to implement the violating company provisions of the Companies Act. Additional steps have been taken in the last two years to escalate enforcement of failure to provide annual reports (i.e. a fine of NIS 7 800 (EUR 1 800) unless the requisite report was provided within 45 days and further daily fine of up to a maximum fine of NIS 250 000 (EUR 58 400) in 2016 and 2017). The initial emphasis has been on financially active companies and the ICA serves, on average, notices to 500 non-compliant companies (and their directors) each year, upon crosschecking their active status with information provided by the ITA. More than 80% of these companies responded by providing the report subsequently, and the remaining companies were all subject to fines. While the ICA is provided with powers to impose fines on company directors or to collect outstanding fines through the MOJ's collection unit with effective measures including seizing bank accounts, it has not imposed any fine on company directors or seized any bank accounts to date. The ICA considers that the existing sanctions, warnings about use of them, and use of them have been highly dissuasive and effective as they have resulted in the 85% compliance rate for submission annual reports (for financially active companies). The assessment team agrees the approach has had a substantial degree of effectiveness but also considers there is scope for increased dissuasion and effectiveness by a more comprehensive approach. The ICA also indicated that it has further plans to impose higher levels of fine, impose the fines on directors and step up its stakeholder education efforts.

471. The ITA mainly relies on the imposition of administrative fines against those individuals and corporations who have failed to file tax reports (NIS 3 595 in 2016 and NIS 3 399 in 2017) (approximately EUR 840 and EUR 794 respectively). It does not impose fines specifically against individuals/corporations which fail to provide basic or beneficial ownership information (although there appear to be no cases known to the ITA where this might have been necessary).

472. Regarding financial supervisors, as discussed in IO.3, they have a wide range of supervisory and enforcement measures available to them. However, with the exception of the MSB sector, the overall level of remedial and sanction actions is low. The BoI has not imposed AML/CFT financial sanctions since the beginning of 2016 although it has levied other types of sanctions. The MoF has made active use of high fines in the MSB sector and created some deterrence, although there appears to be scope for continuing improvement. Regarding the Postal Bank, there were 17 cases of breaches between 2013 and 2017 in relation to basic and beneficial ownership issues for corporate accounts. None of these has been referred to its sanctions committee for determining the application of fines. Overall, the sanctions framework for FIs needs further focus. As for sanctions against lawyers or accountants providing BSP services, two cases of fines were imposed.

Overall conclusions on IO.5

473. **Israel has achieved a substantial level of effectiveness for IO.5**

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

Israel achieved a substantial level of effectiveness for IO.2.

a) International co-operation is particularly important for Israel given that most of the domestic large ML cases have international links (e.g. laundering of foreign predicates, activities of trans-national organised crime groups). Inherent to its geographic location, Israel also faces a high TF threat emanating from sources abroad.
b) Israel has a sound legal framework for international co-operation and has mechanisms in place for providing it. The quality of the assistance provided is good.
c) Israel exchanges and seeks information, both through the use of formal and informal channels. Israel also facilitates action against criminals and their assets, as demonstrated by a number of successful ML and TF cases.
d) Israel provides and seeks constructive mutual legal assistance (MLA) to a large extent. Although some problems have arisen in the context of identified delays in responding to MLA and extradition requests, Israel has taken steps to improve its response time, by allocating more resources to the Legal Assistance Unit (LAU) of INP and directly engaging with the central authorities of requesting countries. While there is no central authority per se (i.e. incoming MLA requests that do not involve service of court documents are handled by INP/LAU, and all outgoing MLA requests are handled by the Department of International Affairs of the State Attorney's Office / MoJ), these arrangements do not appear to have led to significant delays.
e) Authorities are committed to providing assistance to all MLA/extradition requests, and can do so without the prerequisite of a treaty. However, the lack of value-based confiscation system in incoming MLA request sometimes inhibits the ability of Israel to pursue international assistance measures in relation to assets held overseas or within Israel.
f) Authorities use informal channels (e.g. FIU to FIU and police to police) before seeking co-operation through formal channels. ITA and ISA also appear to have good co-operation with their foreign counterparts on their respective predicate offences (i.e. tax and VAT frauds, and securities related offences). IMPA has also allocated more resources to handle international requests.

g) Supervisors co-operate with their counterparts on the basis of MoUs (e.g. ISA/IOSCO). BoI also has MoUs with other banking regulators for the exchange of information.

Recommended Actions

a) To continue the planned increase in human resources to INP/LAU to assist in the timely execution of MLA requests.
b) Israel should improve its response time for incoming extradition requests, whether through additional resources or having dedicated staff within SAO/DIA to handle such requests or through enhanced engagements with foreign counterparts.
c) Israel should streamline the process for handling incoming MLAs requiring investigative action, for example, by designating INP and ITA to be the recipients for such requests.
d) To address transnational ML/TF risks, IMPA should increase the number of spontaneous disclosures arising from its operational and strategic analysis to foreign counterparts.

474. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

475. Israel relies extensively on international co-operation given the inherent ML/TF risks it faces due to its geographical localisation. Assessor's findings are based on the review of a number of case studies with elements of positive co-operation experiences; statistics on the volume of MLA and extradition requests; feedback from the global network of FATF and FSRBs countries; and discussions with the relevant authorities.

Immediate Outcome 2 (International Co-operation)

Providing constructive and timely MLA and extradition

476. Israel is generally active and constructive in responding to formal requests for MLA and extradition. Feedback received from the global network indicates that Israel generally provides constructive MLA and extradition, and that responses are of good quality. A few countries however identified problems in the context of delays in responding to MLA and extradition requests.

Mutual Legal Assistance

477. Israel does not have a central authority dealing with both incoming and outgoing MLA requests. The official mechanism for the transmission and execution of incoming MLA requests is as follows:

a) The Directorate of the Courts (the Directorate) serves as first gate for receiving and registering all incoming legal assistance requests (except ISA requests). Requests relating to civil legal assistance (e.g. service of court documents) and criminal requests that can be dealt by the courts themselves (e.g. request for testimony via video-conference) are executed by the Directorate.

b) The Legal Assistance Unit (LAU) of the INP receives all other MLA requests relating to legal assistance in criminal matters from the Directorate. LAU has seven staff. If the request concerns tax-related matters, LAU will redirect it to ITA

c) The ISA receives MLA requests directly from its counterparts.

478. The Department of International Affairs (DIA) in the State Attorney's Office (SAO) of the MoJ (see R.37) is the authority for incoming extradition requests. DIA receives extradition requests formally through MFA's diplomatic channel and in practice also receives informal requests directly from its counterparts. The DIA is also the authority for all outgoing MLA and extradition requests (see below). The DIA unit on international co-operation has approximately 25 staff – 18 attorneys, 5 interns/clerks and 3 administrative support staff.

479. It can take several weeks to a month for LAU to receive requests from the Directorate. This is due to the initial filtering by the Directorate of incoming requests. Requests requiring civil or non-investigative procedures are handled directly by the Directorate, while MLA requests relating to investigative matters will be forwarded to INP. In practice, the Directorate does not reject any MLA requests, on the basis of formal deficiencies, and rather leaves the review to the INP. While this may impede the timely provision of legal assistance by Israel, the delay does not substantially impact operations. In practice, LAU usually starts executing the request without waiting for the formal written request to be forwarded by the Directorate.

480. INP also pro-actively reaches out to the Directorate when they are aware that an urgent request is coming. LAU for example makes arrangements with foreign counterparts to receive soft copies of urgent incoming MLA requests to as soon as possible. These proactive measures are mostly based on the close co-operation between authorities domestically (police/justice), but also on the numerous informal networks that INP has abroad – e.g. INP attachés and liaison officers, CARIN network, Interpol channels (see sections below on "Providing and seeking other forms of international co-operation for AML/CFT purposes").

481. Upon receipt of the request, LAU performs its own technical review to verify whether the request satisfies the legal requirements. LAU takes whatever action it deems necessary to seek supplementary information, clarification or supporting evidence, by directly liaising with the competent authorities in the requesting country. LAU assigns the requests that meet the legal requirements to the appropriate INP unit for execution, monitors the case and sets the timeframe for the response. For complex and/or sensitive cases, if LAU believes the request cannot be processed, it first consults with the SAO, which then takes the final decision.

482. Requests for MLA may be refused on certain grounds, which were not found to be unreasonable (see R.37). Whilst a request may in principle be refused if it is of fiscal nature, in practice, LAU has never refused a request on this basis. The execution of an incoming MLA may be deferred to a later date if the immediate execution is likely to interfere with a pending criminal matter (including an ongoing investigation by the INP).

483. Between 2013 and 2017, Israel received 743 MLA requests relating to ML and predicate offences. Israel has also received one MLA request related to TF. The low number of incoming TF-related requests is explained by the reliance on a well-established informal co-operation between LAU and other relevant law enforcement and security agencies. This includes the exchange of information via highly secure channels. As mentioned in IO.9, Israel provided a number of successfully investigated and prosecuted TF cases, some of which involved foreign countries.

484. The number of MLA requests received since 2013 that specifically relate to ML is increasing – from 24 in 2013 to 48 in 2017.

Table 30. **MLA requests received by INP from 2013 to 2017**

	2013			**2014**			**2015**			**2016**			**2017**			**Total**
	ML	TF	Pred. Off	ML	TF	Pred. Off	ML	TF	Pred. Off	ML	TF	**Pred. Off**	**ML**	**TF**	**Pred. Off**	
No. of incoming Requests	**24**	**-**	**121**	**17**	**1**	**120**	**21**	**-**	**161**	**42**	**-**	**178**	**48**	**-**	**162**	**743**
Pending	5	-	16	2	-	17	9	-	64	18	-	85	32	-	115	297
Refused	0	-	0	0	-	0	0	-	0	0	-	0	0	-	0	0
Acceded	19	-	105	15	1	103	12	-	97	24	-	93	16	-	47	446

Source: INP

485. International feedback provided by the FATF/FSRBs countries is generally good, but indicated some delays in responding to MLA (and extradition) requests. MLA requests can take from a couple of weeks for a court order to be issued to 4-8 months when the case is assigned to a police unit for execution. In very urgent cases, an MLA request is executed within a matter of days. However, as the table shows, a number of requests are pending since 2013, mostly due to pending clarifications from the requesting countries.

486. Timeframes also inevitably vary based on the complexity of the case and the assistance sought. Israel formally accepts MLA requests and supporting documents submitted in English or French. However, Hebrew being the official language, it takes time to translate documents before sending responses. Israeli authorities explained that some of the delays are caused by differences in evidentiary standards in different countries (especially civil law jurisdictions), whereby Israel must request additional information to satisfy its domestic standards. Delays can also be attributed to the existence of legal conflicts or of ongoing domestic proceedings, but also to requests being of continous nature and prioritisation of cases *de minimus*.

487. Israel is mindful of these delays, and is making efforts to improve its response time by raising awareness proactively on the requirements for legal assistance. Since 2015, LAU's staff has been increased to seven officers, which enabled the sharing of the work load and reduce officers' backlog. Authorities

indicated that the intent is to further increase staffing within LAU to eleven officers, over the course of the next four years.

488. Domestically, LAU developed a number of SOPs and guidelines on the prioritisation and the timely execution of incoming requests. LAU officers frequently provide guidance to foreign partners on the Israeli legal requirements through INP representatives located abroad or other police channels. The guidance includes specific templates and forms for requesting particular assistance, including requests for evidence, search, and confiscation.[37]

489. The LAU maintains its own case management system to manage and prioritise the processing of incoming MLA requests. Under LAU's prioritisation framework, urgent requests are given higher priority. LAU also prioritises requests on the basis of the subject matter (e.g. OECD/FATF related matters) and/or if it was made through an Israeli police attaché. In practice, MLA requests that could result in domestic ML/TF investigation, seizure and/or eventual confiscation would be accorded higher priority.

490. Israel provides a range of assistance to MLA requests relating to asset recovery, including the identification, tracing and freezing of proceeds from foreign predicate offences in Israel. To prevent the dissipation of assets, Israel will initiate domestic investigations to enable the full range of freezing and confiscation powers available domestically. Israel's MLA law does not at present allow for value-based confiscation38. That said, Israel manages its way around it by opening a domestic self-laundering investigation. As a result, this limitation does not impact negatively on its effectiveness. Challenges in relation to the freezing and confiscation of assets were also noted by a few countries in the global network responding to the survey on international co-operation.

Box 23. **The "BI" Case**

Example of a successful response to an MLA request, involving investigative measures and assets confiscation

Background: A predicate offence was committed in Country A, and its proceeds were laundered in Israel.

Relevance to IO.2: The MLA request received in October 2012 asked for investigative activities to be undertaken by Israeli authorities as well as the restraint of funds in one of the bank accounts. INP's domestic investigation (with assistance of IMPA and ITA) provided Country A with the requested evidence, which led to the securing and seizing of criminal assets (approximately USD 1.25 million were confiscated in country A as part of the overall confiscation of USD 1.9 million).

See IO.7 for more information.

37. Israel is about to complete the amendment process of the ILAL, which would streamline the country's freezing and confiscation process and enable value-based freezing and confiscation.

38. A draft amendment is currently being considered to enable this type of assistance.

491. When the requests come from foreign securities regulators, ISA provides the MLA and its Department of International Affairs (IDIA) reviews requests to make sure they meet the legal requirements. All requests are maintained electronically, categorised, and archived, as per IDIA's internal procedures. Each request is followed up until it is fully addressed. An investigator is assigned an incoming request and will be responsible for any necessary actions required, including investigatory actions, issuing court warrants, search and seizures and conducting frontal investigations. The IDIA in general executes requests in order of receipt. Urgent requests are prioritised. Some requests require additional information from the requesting supervisor. During that time, ISA acts on parts of the request which do not require additional information. Between 2013-2017, ISA provided MLA to 13 countries (see table below). The usual response time varies between a few weeks to ten months, depending on the complexity of the request.

Table 31. **MLA requests received and sent by the ISA from 2013 to 2017**

	2013	2014	2015	2016	2017	Total
Incoming Requests	**13**	**13**	**34**	**34**	**26**	**120**
**** related to ML***	0	0	0	1	1	**2**
Req. executed	7	10	23	19	15	**74**
Req. pending	6	3	11	15	11	**46**
Req. refused	0	0	0	0	0	**0**
Outgoing requests	**20**	**13**	**2**	**21**	5	**61**
**** related to ML***	18	7	2	19	1	**47**
Req. executed	20	7	1	7	2	**37**
Req. pending	0	6	1	11	3	**21**
Req. refused	0	0	0	3	0	**3**

Source: ISA

492. The ITA executes an MLA request once it has been authorised by the INP, as per the provision of the ILAL. INP will do so when the request relates to fiscal matters. Once executed by ITA's investigative units, the information is sent to INP for final transmission to the requesting country. Since the inclusion of tax offences to the list of predicate offences under Israeli law in 2016, the ITA received 11 MLA requests, and executed ten of them (one request was withdrawn by the requesting country). ITA indicated that the average response time is four months.

493. Israel receives incoming MLAs directly from its foreign counterparts, whereas INP receives incoming MLAs from the Directorate. ITA receives incoming MLAs that are tax-related through both the Directorate and the INP. This process appears to involve unnecessary steps and parties, and could be further streamlined to enable INP and ITA to receive relevant MLA requests directly from their foreign counterparts rather than through the Directorate.

Extradition

494. Israel's law enables extradition in respect of all offences for which the punishment is imprisonment of one year or more, and even in the absence of any treaty or convention, on the basis of an ad hoc agreement (see R.39). Israeli citizens can also be extradited under stringent requirements.

495. Unlike MLA requests, all incoming extradition requests are sent via diplomatic channels to the MFA. They are then forwarded, along with an MFA cover letter, to the DIA of the SAO for action. Requests for extradition are transferred from the MFA to the DIA within a number of days. Urgent requests are forwarded immediately via a messenger on the day of receipt.

496. There were five ML-related incoming requests for extradition, out of the 35 received that year (which is an increase from 2013, which had only one ML request). Three of these fives requests are still being considered, two have submitted to the Israeli court. A large number of the pending cases are those that contain evidentiary gaps and thus require additional information. DIA needs for instance to request supplementary evidentiary information to satisfy a *prima facie* evidence of the basic element of the offence (e.g. *mens rea* in fraud cases). The non-receipt of this supplementary information is the main reason leading to refusal. DIA may also request supplemental guaranties. This is the case when DIA awaits the receipt of the undertaking (guarantee of transfer) stating that the extradited person will serve its sentence in Israel after completion of the judicial proceedings in the requesting country.

Table 32. **Outcomes of Extradition Requests received by Israel from 2013 to 2017**

	2013	2014	2015	2016	2017
Requests received*	21	44	20	31	35
Requests granted	4	3	6	7	4
Requests refused	6	14	1	1	1
Requests withdrawn	0	1	0	0	0
Requests pending**	11	18	11	24	29
*** Data included in this table is based on the actual submission of the request (as opposed to the opening of a file, the which can be done on the basis of an informal communication and before the receipt of a formal request **Pending includes requests opened in previous years which have not yet been executed. Source: SAO.**					

497. For urgent cases or where there is a risk to public security, Israel orders the provisional arrest of a requested person, even prior to the receipt of the extradition request. This is conditioned upon receiving assurances that an extradition request is forthcoming shortly and that it will be supported by the necessary supporting documents (e.g. a detention warrant and *prima facie* evidence or a judicial conviction decision). To facilitate the processing of urgent cases, the requesting country is invited to send a draft request to the SAO by fax or email, in parallel to the submission of the actual request via diplomatic channels. This enables to DIA to immediately initiate preparatory work while waiting to receive the formal extradition request.

498. Israel faces occasional challenges in executing requests for extradition in a timely fashion. These delays were noted by some countries in the international co-operation feedback received from the global network (4 out of 14 countries which provided inputs on MLA/extradition).

499. Israeli authorities acknowledged these delays, which they attribute to a large extent to a lack of familiarity or understanding of Israel's evidentiary requirements. For countries with established or frequent co-operation, Israel offers to raise counterparts' understanding of the evidentiary requirements by

directly communicating and providing clarifications to the requesting authorities. Where possible, SAO conducts meetings with counterparts (in the margins of international events or bilateral meetings), and regularly communicates by telephone to ensure incoming requests meet the evidentiary requirements. Authorities explained they prefer to avoid refusing requests at first instance. Where minor evidentiary gaps have been identified, and if the case presents some merit, Israel works with requesting countries to address the legal gaps. This approach takes more time and effort, as opposed to a prompt refusal to execute the original request. Requests however can be (and have been) refused due to clearly identified legal obstacles (e.g. insufficient elementary evidence, no dual criminality). The absence of a treaty in itself is not a ground for refusal, because Israel allows extradition by way of an ad-hoc agreement (e.g. for fugitives' extradition requests). Israel only encountered very few instances in which received requests for extradition on ad-hoc basis were ultimately refused. This has been the case when an ad-hoc agreement could not be finalised because the requesting country was not a signatory to relevant bilateral or multilateral conventions.

Box 24

The "GS" case

Two Israel suspects were wanted by Country A for securities fraud, aggravated identity theft and money laundering, among other offences. An extradition request was submitted to Israel in September 2015. Israel successfully executed the request for provisional arrest of two suspects as demanded in the extradition request. The fugitives were extradited to Country A in June 2016.

The "SK" case

In November 2013, Israel arrested the head of a syndicate suspected of smuggling over EUR 500 000 into the European Union and defrauding suppliers and customers. A petition to declare him extraditable was filed in Israel's District Court in late 2013. The suspect was eventually declared extraditable in September 2015 and extradited to Country A in January 2016.

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

500. As demonstrated in a number of cases, Israel seeks MLA and extradition in any ML, TF or predicate offence cases that have a transnational element. Feedback received indicates that Israel generally seeks legal assistance, especially with countries it has established co-operation with.

Mutual Legal Assistance

501. Outgoing legal assistance requests are handled by the IDIA in the SAO. The unit consists of eighteen attorneys and five legal interns responsible for the drafting and sending of MLA requests to foreign jurisdictions. As with incoming

requests, IDIA also has guidelines in place for sending MLA requests. IDIA attorneys are assisted in practice by LAU officers and district prosecutors. LAU will assist investigative units preparing the background for MLA requests that are submitted to foreign authorities. LAU will usually transmit requests to DIA within the day of receipt from police units, and will maintain records of these requests.

502. Between 2013 and 2017, Israel made 469 MLA requests to 63 countries – 187 of the requests had a ML component. Around 80% of the outgoing requests were granted by foreign counterparts (see table below). Of the remaining 20%, most remained unanswered or withdrawn. Formally refused requests related to assistance being not granted for fiscal offences or for failure to meet the requested country's domestic legal requirements (either evidentiary or other). In these cases, the matter was referred to police-to-police channels for execution.

503. In relation to TF, Israel sent four MLA requests in relation to three cases between 2015-2016.

Table 33. **MLA requests submitted by Israel from 2013 to 2017**

	2013		2014		2015		2016		2017	
	ML	PO	ML	PO	ML	PO	ML	PO	ML	PO
Outgoing Requests	**61**		**95**		**78**		**145**		**90**	
	22	**39**	**37**	**58**	**36**	**42**	**58**	**87**	**34**	**56**
(incl. from ITA)	0	0	0	0	1	0	6	0	3	0
Granted	21	36	36	53	29	34	38	57	22	37
Refused	1	3	0	1	0	0	4	5	0	2
Pending	0	0	1	4	7	8	16	25	12	17

Box 25

***Siemens* case**

Example of successful international co-operation with ISA's foreign counterparts, leading to confiscation

Context – five former senior executives of the Israeli Electricity Company were convicted as part of a plea bargain after admitting to bribery, fraud, breach of trust and ML offences. Bribes – in amounts of USD 200 000 to 500 000 - were paid by Siemens. The proceeds were concealed using, inter alia, safes and accounts in foreign banks.

Relevance to IO.2 – This case included investigative actions in foreign countries and the exchange of information which contributed to confiscations (ranging from NIS 200 000 to 1.7 million (EUR 46 700 – 397 000). To obtain information on these foreign bank accounts, Israel (ISA) requested a number of MLA requests to be sent to these countries.

Outcomes – The District Court convicted defendants of bribery, fraud, breach of trust and ML (including imprisonment sentences ranging from 24 to 45 months). Information provided (e.g. evidence of bank accounts used to conceal illegal proceeds) also led to a number of confiscations (totalling NIS 5 million (EUR 1.2 million)).

***RLG* case**

Example of successful international co-operation with ITA's foreign counterparts, leading to confiscation.

Context: This was a case involving counterfeit pharmaceutical trafficking by an international smuggling ring. The case was investigated by ITA's "*Yahalom*" Unit, VAT investigators, INP, with the assistance of IMPA.

Relevance to IO.2: ITA sent MLA requests to five countries. The received information greatly contributed to the ML investigation in Israel and resulted in the freezing of assets in Israel (over NIS 10 million (EUR 2.3 million)).

Outcome: The case is still ongoing.

Extradition

504. Between 2013 and 2017, Israel made 65 extradition requests, with 19 executed by the foreign authorities and 10 still under litigation. Most of the remaining 36 cases did not progress to a full extradition request (past the provisional arrest stage) because the fugitive could not be located. The following table shows the number of outgoing extradition requests:

Table 34. **Outcomes of Extradition Requests submitted by Israel from 2013 to 2017**

Year	Requests	Extradited	With the Court	Refused	Pending	Fugitive not in Requested Country
2013	10	4	1	1	0	2
2014	15	7	1	0	5	1
2015	10	2	3	0	4	0
2016	11	6	3	0	2	0
2017	19	0	2	0	15	2
Total	**65**	**19**	**10**	**1**	**26**	**5**

Source: SAO

Seeking and providing other forms of international co-operation for AML/CFT purposes

505. Similarly to its domestic co-operation, Israel proactively and extensively uses agency-to-agency international co-operation for AML/CFT purposes and efficient information-sharing, including MOUs and various arrangements with foreign counterparts.

FIU

506. IMPA exchanges information and financial intelligence via the Egmont Secure Web effectively and on a daily basis. IMPA does not need an MOU to exchange of financial intelligence with foreign counterparts. That said, it has signed 66 MOUs and to date maintains ongoing exchanges of information with 110 jurisdictions. IMPA seeks financial intelligence for the purpose of its own

analysis, and also at the request of LEAs, including security agencies (80% of the outgoing requests between 2013-2017 originated from an INP request). Between 2013 and 2017, IMPA received 1 071 requests (from 96 jurisdictions), made 672 requests (to 84 jurisdictions), of which 86 spontaneous disclosures to foreign FIUs (see table below). Out of these received requests, IMPA only refused two. This was due to a conflict with domestic investigations.

507. There has been an increase in the number of incoming requests from foreign FIUs in recent years. As a result, IMPA established in 2017 a new department responsible for international co-operation matters, including the exchange of financial information with foreign counterparts. IMPA also increased the number of its staff attending to international requests from two to six, which significantly reduced the response time to incoming requests to less than 30 days towards the end of 2017. With the exception of 2017, the number of spontaneous disclosures by IMPA increased over the past years. Between January and March 2018, IMPA sent 19 spontaneous disclosures to foreign counterparts.

Table 35. **Incoming and outgoing FIU-to-FIU requests (2013-2017)**

Year	Incoming Requests	Outgoing Requests	Spontaneous Disclosures to IMPA	Spontaneous Disclosures by IMPA
2013	147	74	20	6
2014	129	121	44	20
2015	134	131	68	22
2016	165	159	92	33
2017	151	187	121	4
Total	726	672	345	85

Source: IMPA

Table 36. **Requests made by IMPA to foreign FIUs – by requesting agency (2013-2017)**

	2013	2014	2015	2016	2017
IMPA (including ITA)	6	20	22	27	4
INP (including ITA for joint investigations)	63	88	102	118	171
Intelligence Fusion Centre	1	0	5	6	0
Security Agencies	4	13	2	8	12
TOTAL	**74**	**121**	**131**	**159**	**187**

Source: IMPA

508. Feedback from FATF and FSRBs members on FIU-to-FIU co-operation largely complimented IMPA's responsiveness, as well as the quality and usefulness of the responses provided. Of the top ten countries that exchanged information with IMPA between 2013-2017, six countries provided positive feedback (the other four did not provide any feedback). Overall, countries noted that the average response time ranges between 4 to 8 weeks, and in a few occasions, it took 4 to 7 months. Urgent requests were satisfied promptly, i.e. less than a week. Feedback also noted that the timeliness of IMPA's responses has improved over time. Some countries noted the low level of spontaneous disclosures, as opposed to requests sent by IMPA on behalf of LEAs in support of domestic financial investigations. Several countries noted that the information provided by IMPA included

information on company registers, information collected from a number of government databases (including tax information), and was useful in the identification of ML offences, but also fraud and tax evasion.

Box 26. **The Checklist Case**

Context - This case relates to an underground bank operating in the Israeli Diamond Exchange.

*Relevance to IO.*2 - IMPA proactively disseminated 15 intelligence reports to five foreign FIUs. These countries provided comprehensive financial information on companies owned by the main suspects, their bank accounts, including transactions.

Outcome - 15 indictments and four convictions for ML as well as other offences. In addition, over NIS 12 million (EUR 2.8 million) were confiscated. Criminal proceedings are still ongoing and further convictions are expected.

8

Law enforcement

509. Overall, LEAs, namely INP, ITA and *Shin-Bet*, co-operate effectively with their foreign counterparts. The International Co-ordination and Operations (ICO) section of the INP, currently comprised of 31 police officers, includes the Interpol unit, the Foreign Attaché unit and LAU. ICO deals with foreign LEAs, especially through its 11 police attaches abroad.

510. In 2017, INP assessed its infrastructure to determine the efficiency of its international co-operation framework and with the view to increasing the number of joint operations with foreign LEAs. As a result, it was decided to increase ICO's staff and to create several new units over the next two years, starting January 2018 – as following:

- Special Foreign Intelligence Unit (3 officers) – is a newly created unit assigned to foreign intelligence.
- Foreign Attaché Unit is composed of 11 police officers stationed abroad and 4 located in INP headquarters. The number of staff is expected to be increased.
- Foreign Representatives Unit currently exists as part of the Interpol Unit and serves as the liaison between all foreign attaches. It is managed by one officer. It will become a separate unit by then end of the re-organisation period.
- Interpol unit, established in 1949 (8 officers), is responsible for the communication with other Interpol members. It also deals with extradition requests (see above). The information received from Interpol channels is used for intelligence only, and not for judicial purposes. The number of staff is also expected to be increased.

511. Co-operation with Interpol, while led by INP's Interpol unit, is in conjunction with other INP units, such as the financial enforcement unit and operational co-ordination unit (see IO.7). Between 2014 and 2015, an FBI agent was permanently stationed in INP's *Lahav 433*, working on US/Israeli organised crime and ML joint investigations. This joint work led to a number of successful cases (see for example Box 27 below).

512. As an observer to CARIN, Israel has two points of contacts, one from INP and one from the ITA. Authorities increasingly use the CARIN framework to seek financial information, with an average of 13 incoming and 8 outgoing requests between 2015 and 2017. Requests channelled through CARIN usually facilitate subsequent requests through the formal MLA process. It is unknown whether the CARIN channel in itself has proved to be successful for the purpose of ML/TF investigations.

513. Since INP's co-operation with foreign authorities is extensive, but often informal (e.g. involving daily phone calls and discussions) it was not possible to estimate the total number of requests made and received.

ITA

514. ITA receives and sends requests for assistance on the basis of the 32 customs MOUs and 55 tax treaties with other countries. Since January 2017, Israel can also exchange information with the 117 jurisdictions that currently participate in the *1988 Convention on Mutual Administrative Assistance in Tax Matters*.

Box 27. **Example of informal bilateral co-operation on customs matters**

Israel and the US maintain regular and ongoing communication and information exchange on customs matters – including in relation to cash smuggling and ML. Their respective customs authorities signed an MOU which allows them to share information, conuct joint projects and operations (e.g. exchange of information for violations of the reporting obligation by their citizens). ITA has been collaborating for a number of years with the US customs in operation "Flying Green" intended to detect money being smuggled between the US and Israel. As part of this operation, both countries respectively increase their monitoring of incoming travellers. Occasionally, a team of US customs would travel to Israel to jointly conduct passengers' checks.

ISA

515. ISA, acting as the LEA for securities-related offences, conducts criminal and administrative investigations and requests assistance from foreign counterparts. ISA is a signatory of the IOSCO MMoU since 2006. If assistance cannot be provided under the IOSCO MMoU, a formal request for legal assistance is then sent to the Ministry of Justice (SAO), as described above for MLA requests.

516. Between 2013 and 2017, ISA supplied information involving 13 jurisdictions, targeting numerous legal entities and entities with no legal personality. These requests mainly related to issues such as insider trading, securities frauds, and unauthorised financial intermediation/unregistered brokerage, but also involved ML matters. Some of the cases also included information regarding the transfer of funds between accounts. Regarding cases of suspected market abuse (including fraud and use of inside information) and potential unauthorised financial intermediation, ISA made 53 requests for international assistance.

Bank of Israel (BoI)

517. BoI shares supervisory information according to the framework of the international standards to which the BoI is committed. These include Financial Services Board (FSB) in the European Regional Consultative Group, the OECD, the International Monetary Fund, the World Bank, and the International Conference of Banking Supervisors.

518. BoI's International Relations Unit (comprising of three officers) is responsible for international co-operation and communication. The unit has internal guidelines on the processing of incoming and outgoing requests. BoI is not required to sign a MoU in order to exchange information with another state. Nevertheless, BoI has signed MoUs with supervisors in India and the US, and has informal co-operation via signed letters with the UK supervisors and via working visits with the Swiss supervisors in the framework of home-host supervision.

519. BoI receives requests from foreign regulators for assistance on fit-and-proper requirements and issues relating to the home-host relationship. BoI also receives requests from banks which have correspondent relations with BoI and the Israeli banking system on those issues. Between 2014 and 2017, BoI received 15 requests (with an average of 3-4 per year) regarding fit-and-proper, all of which were responded to within 14 business days.

520. Supervisory information is shared with other countries by virtue of the home-host relationship. BoI did not make or receive requests relating to AML/CFT. Usually, the information relates to the financial state of Israeli banks, and in exceptional circumstances information pertaining to negative developments or a stability concern regarding an Israeli bank. After the provision of information, BoI maintains ongoing communication with its foreign counterparts and receives feedback on the provided information's contribution.

CMISA

521. CMISA is signatory to the International Association of Insurance Supervisors (IAIS) Multilateral Memorandum of Understanding (MMoU) since November 2013, which enables Israel to co-operate and exchange information on insurance companies with other supervising authorities. Under the MMoU, the exchange of information includes information on ML, corporate governance as well as any area of relevance to supervisors and which pertains to insurance companies. CMISA also regularly participates in the IAIS meetings.

522. Since 2013, CMISA has successfully provided and sought information to and from foreign counterparts, including information on officials and subsidiaries. CMISA's financial department (comprising of two employees) is responsible for international relations. The licensing department deals with the exchange of information with foreign counterparts on issues relating to control permits for supervised entities. As part of this licensing requests process, the licensing department conducts a comprehensive examination of ML and TF issues (e.g. applicant's capital resources, fit-and-proper procedures).

International exchange of basic and beneficial ownership information of legal persons and arrangements

523. Israel does not maintain specific statistics on the number of requests it sends and receives for basic and BO information on legal persons and arrangements. Central authorities however indicated that such requests exist, as evidenced by a number of cases examples provided during the on-site. However, these BO-related requests are often part of broader requests.

524. When executing an MLA request regarding BO information, LAU will direct a request to the ICA for all relevant information. ICA maintains a range of information on companies and partnerships, including listings of all active registered companies and details on the shareholders, directors and partners of legal entities (see IO.5). LEAs, IMPA, and regulators can obtain this information from ICA either by request or by direct access. LAU also requests and receives information (through court orders) from ITA, INP, FIs and DNFBPs. LAU verifies the accuracy of the information received, and its consistency and reliability against different sources, before responding to the MLA request.

Overall conclusions on IO.2

525. **Israel has achieved a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluations in 2008 and 2013. These reports are available from here.

OBLIGATIONS AND DECISIONS FOR COUNTRIES

Recommendation 1 – Assessing risks & applying a risk-based approach

Criterion 1.1 – Israel conducted a number of risk assessments, relevant to money-laundering (ML), terrorist financing (FT) and the financial sector, over a period of two years (May 2015 - March 2017). These assessments were co-ordinated by the Money Laundering and Terror Financing Prohibition Authority (IMPA), with the participation of all relevant enforcement and supervisory authorities, and also financial and non-financial sectors (e.g. FIs, trust service providers (TSCs)). In addition to the information collected by means of a questionnaire sent to all participants and round-table discussions, self-risk assessments were also taken into account in the assessment of risks (e.g. Diamond Exchange, Israel Bar Association and Institute of Certified Public Accountants) (for more information on the NRA process, see Chapter 2).

In addition to these NRAs, Israel also conducted a number of sectoral and thematic assessments (e.g. gambling, alternative payment systems, MSBs and use of cash) and assessments of issues relevant to ML/TF (e.g. 2016 risk assessment of corruption, 2003 RA of tax offences and 2004 RA of serious and organised crime). These assessments were conducted within inter-governmental committees, similarly using a wide range of information The ML/TF risk level posed to the banking system by "digital currencies" was assessed as moderate high in the financial sector' NRA. In November 2015, the Committee for the Promotion of the Use of Advanced Payment Methods published a report,[39] the findings of which were taken into account in the ML NRA.

Criterion 1.2 – The Executive Steering Committee (ESC) and the inter-agency Implementation Committee (IC) are the designated authorities in charge of the NRA project (Decision no. 4618 of the

39. Interim Report of the Committee for Promoting Use of Advanced Means of Payment in Israel, November 2015. http://www.boi.org.il/en/NewsAndPublications/PressReleases/Documents/Interim%20Report-The%20Committee%20for%20Promoting%20Use%20of%20Advanced%20Means%20of%20Payment%20in%20Israel.pdf

Israeli Government of January 2006). IMPA co-ordinated both the ML and TF risk assessment processes itself, under the instructions of the Attorney General.

Criterion 1.3 – It is provided in the NRA process that risk assessments are to be updated each year, or on a need basis (i.e. legislative changes, revisions to international standards). Some of the sectorial/thematic risk assessments mentioned in c.1.1 dating back to 2003/2004 have been reviewed and updated since their publication within the NRA.

Criterion 1.4 – The development of both the ML and TF NRA involved relevant industry associations, FIs and key stakeholders. Preliminary and final findings were presented formally during meetings of the IC, ESC and various supervisory forums, including at events dedicated to compliance officers and representatives of FIs/covered DNFBPs. Both reports were published on IMPA's website. A number of agencies (IC, ESC, LEAs, supervisors and relevant public authorities) also received the classified versions of the NRAs. The non-classified version of the ML NRA was published in November 2017 and distributed, while the non-classified version of the TF NRA was published in March 2018.

Risk mitigation

Criterion 1.5 – Israel implements elements of a RBA approach to AML/CFT measures across judicial and law enforcement agencies (incl. Israeli National Police (INP), State Attorney's Office, Israeli Tax Authority (ITA), Israeli Securities Authority (ISA), and IMPA) and supervisory authorities (Bank of Israel (BoI), ISA, CMISA). This is embedded in the legislation regarding FIs (see R.10-19) and covered DNFBPs (see R.22-23) and their supervisors (see R.26 and R.28). This includes allocation of resources and measures taken to prevent or reduce ML/TF on the basis of the NRA findings (e.g. strengthening capacities of INP's Intelligence Division and establishment of a dedicated financial enforcement squad). In addition, a detailed action-plan and a high-priority action plan were developed to mitigate the risks identified during the NRA process (on ML and financial sector). A separate action plan (classified) was developed following the TF NRA. The detailed ML action plan includes priorities areas, a timeline for the implementation of the recommendations and the designation of authorities in charge of implementation. Areas identified as high risk (e.g. MSBs, legal arrangements) have a specific high priority action plan that was approved by the Attorney General. However, resources are allocated to MSBs are only able to handle registration responsibilities but not AML/CFT control at this stage.

Criterion 1.6 – The Israeli AML/CFT framework does not include all FIs and covered DNFBPs. Some sectors are entirely exempt from applying FATF Recommendations, but not based on a proven low risk of ML/TF. Though real estate sector has been considered in the NRA and is exposed to moderate high risks; the sector is not subject to the AML/CFT regulatory regime. Dealers in precious metals are not subject to AML/CFT regulation, but only briefly considered in the NRA, which covers mainly gold and precious stones only. Lawyers and accountants, referred to as business service providers (BSPs) in Israel, are exempt from certain AML/CFT requirements such as reporting obligation. Again, this exemption from AML/CFT obligation is not due to proven low risk of ML/TF.

Exemptions are carried out on an occasional and limited basis for money service providers (MSBs) (i.e. CDD thresholds approach for occasional customers: NIS 10 000 (EUR 2 340) for cash transaction; NIS 5 000 (EUR 1 168) if it relates to an identified high risk geographic area; and NIS 50 000 (EUR 11 680) for non-cash transactions). While these exemptions do occur on an occasional and limited basis, they are not based on a proven low risk of ML/TF. This might not be consistent with

the higher risk character of MSBs (i.e. currency exchangers, MVTS) because their activities are associated with the use of cash, which was identified as ML/TF high risk in the NRA.

Criterion 1.7 – Regarding identified higher risk situations, FIs (including banks, postal bank, stock exchange members, trading platforms, portfolio managers, insurers and MSBs) and covered DNFBPs are required to take enhanced measures to manage and mitigate the risks, or require them to ensure that the high risks information is incorporated into their risks assessments. Insurers are also required to conduct increased monitoring over transactions that involve high risks of ML/TF. (S. 30 of the Banking Directive 411; s.26 of Postal Bank Directive; s.2(b) of Stock Exchange Members, Portfolio Managers and Trading Platforms Orders, s.11(3) of Stock Exchange Members order and s.9(3) of s.3.3.1(a), 7.2 and 9.1 of Trading Platforms Circular; s.3.1 of the Licensed Portfolio Managers Circular; s.9(5) of the Insurers Order; s.2(B)(2),(5) and (6) Insurers Circular; s.7 of and Sch.3 to the MSB Order; s.3, 5 and 6 MSB Circular; s.2(c) of Sch.4 to BSP Order; s.10 of the Diamond Dealers Order) (See also c.10.17).

Criterion 1.8 – There are no specific legal provisions or written rules allowing the application of simplified measures by FIs and covered DNFBPs. Respective sectoral orders list specific categories exempt from some CDD requirements (e.g. declaration of beneficial owner), but not every order expressly specifies that such exemption is based on an identification of lower risks. Such exclusion is also not mentioned under the risk assessment conducted by the country. (Banking sector: s.5 and 5B of the Banking Order; securities sector: s.6(a) and 8 of the Stock Exchange Members, s.6A of the Portfolio Managers, and s.6(a) of the Trading Platforms Orders; postal bank: s.6(a) of the Postal Bank Order; insurance sector: s.7 and 8 of the Insurers Order; s.4(d) of the MSB Order, s.4 and 5 of the BSP Order, s.2(c) of the Diamond Dealers Order.) (See also c.10.18).

Criterion 1.9 – Financial and DNFBP supervisors have been appointed to ensure AML/CFT compliance (c.26.1) and supervised entities are generally required to determine risk management practices for AML/CFT purposes (s.18 of the Stock Exchange Members Order, s.16 of the Portfolio Managers Order, s.18 of the Trading Platforms Order, s.12 of the MSB Order, s.17 of the Postal Bank Order and s.10 of the Insurers Order, s.2(e) of and Schedule 5 to the BSP order; s.15 of and Schedule 4 to the Diamond Dealers Order). Israel also makes use of sectoral orders/regulations to impose AML/CFT obligations on FIs and covered DNFBPs. These include supervising for enhanced due diligence (see c.1.7). These supervised entities also cannot carry out the transaction or establish/continue customer relationships in certain risks situations. Supervisors rely on their general supervisory powers provided under respective sectoral ordinances for AML/CFT purposes (including obligations under R.1), however there are no specific provisions requiring risk-based supervision (deficiency mentioned under c.28.5). (s.11N(d) of the Prohibition of Money Laundering Law (P Criterion 24.6 MLL), s.5 of the Banking Ordinance, s.44T, 56A1 and 56F of the Securities Law, s.29 of the Investment Advice Law, s.49C to 50 of the Insurance Law, s.88M of the Postal Law, and s.67, 68 and 70 of the Supervision of Financial Services Law (Regulated Financial Services) 5776-2016). (See R.26, 27, c.28.5).

OBLIGATIONS AND DECISIONS FOR FINANCIAL INSTITUTIONS AND DNFBPS

Risk assessment

Criterion 1.10 – The requirements to document ML/TF risk assessments, keep those assessments up-to-date, and put in place mechanisms to provide the risk assessment information to their sectoral

supervisors are only relevant to banks, postal bank, stock exchange members, trading platforms, and insurers. (For banks: s.24-26 of Directive 411; for postal bank: s.10(h) and 22 of the Postal Bank Directive; for insurers: s.2, 3(a) and 2(b)(6) of the Insurance Commissioner Directive; for stock exchange members and trading platforms: s.3.3.1 and s.4.2 of the respective circulars).

Supervisor of portfolio managers relies on general broad obligations in sectoral order, specifically (a) requiring supervised entities to determine policy, instruments and management of risk for CDD, reporting and record keeping obligations; and (b) on-going monitoring of customers data for AML/CFT purposes. But these provisions do not specify the need to document risk assessments, consider relevant risks factors for determining risks and corresponding risk mitigation measures, keep risk assessments up-to-date, and put in place appropriate mechanisms to provide risk assessment information to competent authorities and self-regulatory bodies (SRBs). The case is similar for BSPs, and diamond dealers. (s.16 of the Portfolio Managers Order, s.2(c) and (e) of and fourth and fifth schedule to the BSP Order, and s.10 and 15 of and the fourth schedule to the Diamond Dealers Order).

Risk mitigation

Criterion 1.11 - There are no specific legal provisions or written rules requiring all FIs and DNFBPs to have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the FI or DNFBP), or monitor the implementation of these controls and to enhance them if necessary; and take enhanced measures to manage and mitigate the risks where higher risks are identified. That said, Israel has made use of directives and circulars to ask banks, stock exchange members, trading Platforms, insurers, MSBs and postal bank to carry out enhanced monitoring in certain high risk situations (for banks: s.30 of Banking Directive 411, s.6. 10, 15 and 26 of Postal Bank Directive, s.3.2, 3.3.1 and 4 of the Stock Exchange Members and Trading Platforms circular, for insurers: s.2(B)(2)-(3) of the Commissioner Circular, s.3-4 MSBs circular). (See also c.1.7)

Criterion 1.12 - Israel does not allow FIs and DNFBPs undertaking simplified measures, regardless of the ML/TF risks level identified. FIs and covered DNFBPs (e.g. banks, securities sector, MSBs, insurers, and BSPs), however are allowed to be exempt from CDD, in certain situations – but not when there is a suspicion of ML/TF, or specific higher risk scenarios apply. (Banking sector: s.5 to 7 of the Banking Order; securities sector: s.6(a) of the Stock Exchange Members Order, and Trading Platforms Orders; 6A of the Portfolio Managers Order, postal bank: s.6(a) of the Postal Bank Order; insurance sector: s.7 and 8 of the Insurers Order; s.4(d) of the MSB Order; s.4-5 of the BSP Order; s.2(c) of the Diamond Dealers Order.)

Weighting and Conclusion

Israel has identified and assessed ML/TF risks for the country. Israel has designated an overall authority to co-ordinate the NRA, which involve relevant public and private stakeholders, and will be updated annual and when necessary. The exclusion of a few sectors from AML/CFT without fully basing on the results of the NRA, however, has a bearing to the rating of this Recommendation. There are also certain sectors excluded from all or some AML/CFT requirements, and not based on proven low risk.

Recommendation 1 is rated largely compliant.

Recommendation 2 – National co-operation and co-ordination

In its last mutual evaluation, Israel was rated compliant for these requirements.

Criterion 2.1 – Israel has a national integrated policy "*Countering Serious and Organised Crime and their proceeds*" – referred to below as "Decision 4618". This national policy was approved on 1 January 2006 and sets up the targeting of illicit proceeds as a primary objective in the fight against serious and organised crime. It also sets the requirement on all relevant agencies to co-operate together and establishes the Executive Steering Committee (ESC) and the Inter-Agency Implementation Committee (IC) (see c1.2). *Decision 4618* pre-dates the NRA, and is thus not informed by risks identified in the subsequent ML and TF NRAs. However, as part of its function, the IC prepares annually a consolidated intelligence assessments, the last of which included the findings of the NRA. There is also the government decision (Decision B/86) issued by the Ministerial Committee on National Security Affairs relating to TF. It is classified as confidential and therefore not published.

Criterion 2.2 – The ESC is in charge of implementing *Decision 4618* and increasing the country's effectiveness to combat serious and organised crimes and their proceeds (incl. ML). To do so, the ESC approves multi-year and annual work plans and defines goals and priority actions in these areas. The ESC is composed of the highest officials of LEAs (i.e. Attorney General, State Attorney, Inspector General of INP, Head of the ITA and ISA Chairman). Representatives of the Israeli Security Service, the Institute for Intelligence and Special Assignments (*Mossad*) and representatives of other State authorities are invited on a case-by-case basis. The Decision 4618 also establishes the "Inter-Agency Implementation Committee" (IC), which co-ordinates activities taken by the ESC. To do so, the IC formulates multi-annual and annual action-plans for the implementation of the policy and priorities established on the basis of the ESC's decisions.

The National Bureau on Counter Terror Financing (NBCTF) was established on 11 March 2018 is the inter-ministerial co-operation structure under the Ministry of Defence dedicated to combating TF. NBCTF took over from the Interagency Co-ordination Committee established in 2003 by the Ministerial Committee on National Security Affairs (Security Cabinet). The Unit was mandated to outline the national enforcement policy and co-ordinate ministries and authorities in the fight against TF. With the NBCTF, the mandate was expanded to include inter alia the conducting of CFT risk assessments.

Criterion 2.3 – As described in c.2.2, the IC implements ESC's directives into operational mechanisms. The IC also determines the operational priorities for activities, and co-ordinates investigation, enforcement, intelligence and regulation authorities. The IC is composed of the Head of IID/INP, and heads of various relevant police units and district attorneys, senior officials from the ITA, Prison Service, ISA, ATA, as well as the Head of IMPA. The IC operates through a number of sub-committees (e.g. sub-committee for operational co-ordination, intelligence, legal issues, training and IT). The sub-committee for operational co-ordination sets the objectives and targets in accordance with risks identified in the NRA and annual intelligence assessments produced by the IC. Among the topics discussed are: mapping and analysis of current trends and risks, sharing knowledge and expertise, and increasing operational-investigative co-operation.

In addition, the State Attorney's Office also has its own co-operation mechanisms, such as the: 1) a *Financial Enforcement Headquarters*, which aims at increasing financial enforcement, including by

improving co-operation between all law enforcement authorities; 2) a *Financial Enforcement Forum* dedicated to ML, asset forfeiture and confiscation (composed of prosecutors, INP National Confiscation Officer, and representatives from the Administrator General, MOJ, IMPA and ITA); 3) *Financial-Enforcement Teams* of qualified prosecutors (criminal, fiscal, civil-financial) and 4) *ML/TF Task Forces* of Enforcement Agencies.

The *AML/CFT Regulators Forum* established in 2009 is in charge of ensuring the implementation of AML/CFT issues across the financial sector and DNFBPs. The Forum is led by IMPA and is composed of representatives from all supervisory agencies, including ITA, and when required INP, prosecution, and the Ministry of Justice (MoJ).

Criterion 2.4 – PF co-ordination issues fall within the competence of the MoF's Sanctions Bureau, which was established to implement the 2012 Law for Countering Iran's Nuclear Program. It also serves as a national information centre regarding all aspects of sanctions. It is comprised of representatives from the MoF, MFA, MoJ, Ministry of Defence (MoD), Ministry of Energy and Water, Ministry of Economics and Industry, National Security Council, and INP. With the new law Prevention of Distribution and Financing of Mass Destruction Weapons or Means of Carrying Thereof Law, which entered into force in March 2018, the Sanctions Bureau now also oversees sanctions relating to DPRK. There is also a Sanctions Headquarters operating within the MFA (implementation of UNSCRs), with the participation of the MoF, MoI, MoD and other agencies. The NBCTF within the MoD co-ordinates the operational activities of the security agencies on PF.

Weighting and Conclusion

Recommendation 2 is rated compliant.

Recommendation 3 – Money laundering offence

In its last MER, Israel was rated as largely compliant with R.1 and compliant with R.2. The main criticism was that s.4 of the Prohibition of Money Laundering Law (PMLL) contained a threshold approach and did not extend to all possible categories of property. The PMLL was since updated, with amendments coming into force on 7 December 2017.

Criterion 3.1 – ML is criminalised in s.3(a) and 4 of the PMLL. The scope of the ML offence in s.3(a) applies to anyone who engages in a property transaction involving prohibited property with the intent to conceal or disguise its origin, the identity of the rights' holders therein, its location, movements or transaction in it. "*Property*" and "*property transaction*" are broadly defined in section 1. This covers most elements of Article 3(1)(b)&(c) of the Vienna Convention and Article 6(1) of the Palermo Convention. However, s.3(a) is supplemented by the more general s.4, which covers any property transaction – thus including acquisition, possession, and use – regardless of purpose. Whilst there is no threshold which applies to activities captured by offences under s.3(a), there are thresholds for offences captured by section 4 (see analysis of 3.2/3.3 below). These s.4 thresholds narrow the scope of the offence under which the laundering of the proceeds of crime can be captured by this legislation so that it is not fully in line with the Vienna or Palermo Conventions. See c.3.2 and 3.3 below.

Criterion 3.2 and 3.3 – The predicate offences for ML are defined as transactions in prohibited property related to an "offence" as listed in Schedule 1 of the PMLL. These cover all predicate offences required by the FATF. While the list covers all major proceeds generating offences, a value threshold limits some of the offence types. Schedule 1 limits the applicability of the legislation on

Value Added Tax, Income Tax and Real Estate Tax when the offence does not exceed specified thresholds. The threshold is lower or abolished when the offence is linked to a criminal organisation, terrorist organisation, or committed by a third party, or if the offence was carried out in a 'sophisticated manner', which includes, but is not limited to, the use of legal entities, legal structures, manipulation of financial institutions and typologies issued by FATF (s.17(A), (B) and (C) of the PMLL).

The various thresholds are not insignificant of themselves with examples from VAT (with the exception of fictitious invoices offences that have no threshold) (s17(A)) being NIS 480 000 (EUR 112 200) in a 48-month period or NIS 170 000 (EUR 39 700) in a 12-month period, income tax (s.17(B)) being NIS 2 500 000 (EUR 584 200) in a 4-year period or NIS 1 000 000 (EUR 233 700) in a 1-year period, and real estate (s17(C)) being an omission of value on a transaction exceeding NIS 1 500 000 (EUR 350 500). However given the caveats concerning connections to criminal organisations etc., these are assessed as minor but relevant shortcomings.

Additionally, regarding the Convention elements of acquisition, possession, and use covered by s.4, the previously identified deficiency regarding the threshold approach is extended to specific types of property and is not wide enough to capture the intention of the Recommendation. Under Schedule 2, a threshold of NIS 150 000 (EUR 35 050) applies to all property transactions if such a sum is within a single transaction or a series of transactions within a two-month period. The application of a timeframe of two months further reduces the compliance with this criterion. Thus the property below the amount listed in Schedule 2 of PMLL, would not be caught as regularly as the Recommendation envisages, as the value of the property is too low regardless of the fact that it originates from any of the other offences listed in Schedule 1 of PMLL. This suggests that in practice there are no ML cases of less than NIS 150 000 (EUR 35 050).

Although s.411-413 to the CC supplement offences of: receiving property obtained by felony, receiving property obtained by misdemeanour, and possession of suspect property – all of which relate to any asset with no threshold – they do not meet the criteria required for ML offences within the FATF standards.

Criterion 3.4 – The ML offence laid out in s.3(a) of the PMLL covers any type of property provided it is derived from or otherwise connected to the specific offences listed in schedule 1 of PMLL.

Criterion 3.5 – The PMLL (s.3) does not set the requirement that a person be convicted of the predicate offence in order for the property to be considered proceeds of crime (s.3(a) defines '*prohibited property*'). This position was supported by case law within the criminal justice system of Israel (case *no. 7953/08 Ritblat v. The State of Israel*) which merely demands that it is a circumstance that must be proven, along with all the other elements of the crime, beyond a reasonable doubt. However there is still a requirement to associate the proceeds of crime to the offences set out in schedule 1 PMLL.

Criterion 3.6 – Predicate offences to ML under the PMLL extend to conduct committed in another jurisdiction subject to a dual criminality requirement (s.2(b)).

Criterion 3.7 – Section 3(a) of the PMLL offence is broad enough to cover 'self -laundering' as it makes reference to any 'person undertaking a property transaction'.

Criterion 3.8 – Israeli jurisprudence supports the concept of inferring the intent and knowledge requirements of the ML offence from the objective factual circumstances (criminal case no. 21432-04-14 the *State of Israel v. Eitan Hiya*). However, s.4 of the PMLL limits the use of the wilful blindness

doctrine to substitute the need to prove knowledge, thus depriving the prosecution of a tool to assist in proving the mental element of the ML offence. Knowledge can be inferred from factual circumstances as demonstrated by various cases (e.g. the cases of Hiya and Danker). The definition of wilful blindness is found at section 20(c)(1) CC: ' *if a person suspected the nature of his conduct or the possibility that the said circumstances would be caused, then he shall be deemed to have been aware of them, if he failed to clarify the matter*'. This matter was raised in Israel's previous MONEYVAL evaluations and accepted as unhelpful but not in contravention of the standards. A recommendation regarding this point is made in the IO7.[40]

Criterion 3.9 – Sanctions for natural persons convicted of a ML offence are provided under section 3(a) and (b) (ten years imprisonment and/or a fine of 20 times the statutory amount) and section 4 of the PMLL (seven years imprisonment and/or a fine of 10 times the statutory amount). As a result of judicial criticism changes to the PMLL have been made recognising that the sentences for offences contrary to section 3(b) PMLL which involve a defendant's legitimate property were too harsh; thus a second sentencing tier has been created, with a maximum period of five years imprisonment, when false information is given regarding legitimate property. The statutory amount is determined by reference to Criminal Code that sets the base monetary fine in relation to the maximum prison sentence (s.61(a)(4)). In this case, the fine is for offences that carry at least three years imprisonment as a penalty. It is the highest base level of fines which, as at December 2017, would led to a maximum fine for a section 3(a) PMLL offence of NIS 4 520 000 (EUR 1 056 200). By reference to the Criminal Code, it can be seen that other serious and non-violent offences carry greater sentences and/or fines e.g. production or manufacture of drugs carries a maximum of 20 years or 25 times the statutory sum (which is the same base level as that for ML), whilst possession of drugs is three years imprisonment unless it is in a school (which the person possessing the drugs does not attend), in which case the sentence is five years. The offence of robbery carries a sentence of up to 14 years, and aggravated robbery up to 20 years.

Criterion 3.10 – There is no definition of 'person' in section 1 of the PMLL – Israel indicated such definition is provided in the *Interpretation Order.*[41] Jurisprudence demonstrated however that imposition of sanctions on the company does not preclude the imposition of criminal liability on a natural person (Case no. 35790-01-14 *Jerusalem District Attorney's Office v. Hamed*).

S.23 of the Criminal Code addresses the conditions applicable to a legal person being made criminally liable for the actions of an employee or office of a corporate body. This appears to be capable of being applied to all legal person irrespective of them being subject to the obligations imposed by s.7 to s.9 of the PMLL or not.

Criterion 3.11 – Schedule 1 (para. 20) specifically references the act of conspiracy to commit any of the other offences listed in the schedule as being a trigger to commit the ML offence. The Criminal Code also provides, and details the penalties for, the circumstances when the range of ancillary offences would be available (s. attempt; s. 29 – definition of perpetrator; s.30 – enticement; s.31 – accessory; s.32 - penalties).

40. See paragraphs 127 and 128 of the MONEYVAL Report on Israel dated 12 December 2013.
41. "Interpretation Order" – Person including a company or organisation or a body of persons, whether incorporated or not.

Weighting and Conclusion

There are a significant number of criteria in this Recommendation that can be shown to be met by Israel. However there are minor shortcomings that relate to thresholds (see 3.1 to 3.3 inclusive above).
Recommendation 3 is rated largely compliant.

Recommendation 4 – Confiscation and Provisional Measures

Current FATF Recommendation 4 was, at the time of the last evaluation, Recommendation 3.

In its last MER, Israel was rated as largely compliant with R.3 with the main criticism being that there was a failure to provide a comprehensive system for value confiscation.

Criterion 4.1 – There is no single piece primary legislation that captures this criterion 4.1 Israel adopted an approach that covers the confiscation of: (a) property laundered; (b) proceeds and instrumentalities used and intended for use in ML (s.21 PMLL) and predicate offences (s.32 Criminal Procedure Ordinance; s.5 Combatting Criminal Organisations Law; s.36A(a) Dangerous Drugs Ordinance; ss. 297, 377D, 469, and 483 Criminal Code); and (c) property that is the proceeds of, or used in or intended for use in TF (s.53 and 66(a) of the CTL). However none of these (save for s.21(a) of PMLL and s.5(2) CCOL) allow for the confiscation of property of corresponding value (criterion c4.1d) in stand-alone predicate cases such as fraud. It is noted that the courts have taken the view that, in relation to the balance of bank accounts at least, there is a partial equivalent value approach as any balance can be subject to confiscation even if the funds do not meet standard asset tracing definitions or criminal proceeds definitions.

Criterion 4.2 –

(a) There are a number of measures, both procedural and legislative, that enable competent authorities to identify, trace and evaluate property that is subject to confiscation. Sections 24 and 25 of the Criminal Procedure Ordnance addresses general searches with or without a warrant respectively, which is often extended to various types of criminal offence, as by way of example, the Dangerous Drugs Ordnance does by way of s.28(a). Additionally various bespoke powers are extended to other laws e.g. the power to search cargo and merchandise on entry or exit from Israel in accordance with s.28(b)(4) is extended to the PMLL by virtue of s.26 of that Act. The power to trace property for the purposes of confiscation is not limited to police officers as ISA investigators also have powers under s.56A and 56C of the Securities Law. The identification and tracing of property can be assisted by the dissemination, by the IMPA, of information it has received in accordance with s7, 8A and 31(c) of the PMLL.

However tracing may be artificially hampered by the restriction placed on the use of information provided to the INP and Shin-Bet by the IMPA as a result of the Regulations.[42] As such, the information that IMPA provides spontaneously cannot be used, or passed on, if the competent authority (namely the INP or Shin-Bet) has held it for more than two years (see PML Regulations (Rules of Use), section 3(c) read in conjunction with Part 1 of the Third Schedule to the Regulations which lists a number of investigating authorities). This restriction does not apply for information provided by IMPA upon request. To overcome this issue the competent authority merely makes a request for the information. It is unclear why the Regulation exists or what purpose it serves.

42. Prohibition on Money Laundering Regulations (Rules for Use of Information Transferred to the Israel Police Force and Shin-Bet for Investigation of Other Offences and for Transferring it to Another Authority) 5766-2006.

(b) There are legislative processes in place to take provisional measures to freeze or seize property to prevent its disposal pending confiscation. Many of the powers available to seize or freeze assets exist in parallel in the Criminal Procedure Ordinance and PMLL. The Combatting Criminal Organisations Law, at s.21 to s.27, provides for restraint orders to be made before or after an indictment has been issued. The Dangerous Drugs Ordnance, at s.36(F)(a), allows for a court to grant a temporary non-renewable order, for 90 days, effectively freezing assets that will be subject to confiscation; these provisions are extended to the PMLL by virtue of s.23 of PMLL. The Criminal Procedure Ordnance allows for the seizure of assets (or items) which are connected to the crime being investigated to be seized. The assets can be subject to seizure for an indefinite period but are subject to a judicial review after 180 days. For TF, administrative seizure orders are provided for in the CTL (s. 56 and 67).

In instances in which both statutory regimes may apply, the courts have ruled that, while the investigation is on-going, the assets should be seized under the Criminal Procedure Ordnance. Once an indictment has been issued the assets must be made subject to the freezing provisions under the Dangerous Drugs Ordnance. This appears to work well for matters involving money laundering and/or drugs and is capable of covering all assets that could be subject to confiscation. The provisional seizure or freezing orders can be obtained on an initial ex-parte basis.

The provisional measures in place for freezing assets focus on those assets which would be capable of being confiscated under the current legal framework in Israel. However it should be highlighted that some predicate offences do not include a value-based confiscation capability, and thus the current provisional measures framework is not capable of meeting the scope of the assets and actions envisaged within the Standards.

(c) Israel relies on early judicially authorised actions. However, s.6(1)(a) of the PMLL underlines that a person does not commit an offence if they have reported, to the competent authority, the property transaction prior to undertaking the transaction and have complied with the instructions pertaining thereto. This would indicate that there is a mechanism to prevent actions that would prejudice freezing or seizure. Furthermore section 21(c) PMLL underlines that confiscation can be enforced against the property of a third party if that property was paid for by the defendant or gifted to the third party. This approach is mirrored in other limited but high profile legislation. This demonstrates that there are steps that have been taken to void actions that would undermine the country's ability to recover property subject to confiscation.

(d) Wide investigative measures are available to the Israel National Police in connection with investigations to support forfeiture or confiscation. Investigative measures are available to 'Customs Investigators' under the PMLL only insofar as the predicate offence that leads to the money laundering must be derived from one of a number of tax type offences.

Criterion 4.3 – The rights of bona fide third parties are protected. This extends to circumstances where a party obtains property in good faith and for appropriate value consideration as well as offer protection to such a third party when they would be left without reasonable means of support or accommodation if confiscation was to be enforced.

Criterion 4.4 – The Asset Recovery and Forfeiture Office, established in 2014, has the function of managing, and, when necessary, disposing of property frozen, seized or confiscated.

Weighting and Conclusion

Israel meets or mostly meets all the technical criteria for Recommendation 4. The main deficiency is that Israel's legislative framework does not have a generic value-based confiscation system. In

addition there are restrictions on the extent of such provisional measures in relation to certain stand-alone predicate cases.

Recommendation 4 is rated largely compliant.

Recommendation 5 – Criminalisation of TF

In its last MER, Israel was rated compliant for these requirements. Since then Israel has updated its TF offences under the new Counter-Terrorism Law (CTL) which entered into force in November 2016.

Criterion 5.1 – Israel's TF offences cover the conduct criminalised in Art.2 of the UN Convention for the Suppression of the Financing of Terrorism (TF Convention). There are two key TF offences: prohibition on a property transaction for the purposes of terrorism, and prohibition on a transaction in terrorist property.

Prohibition on a property transaction for the purposes of terrorism: It is an offence to perform a property transaction with the intention of assisting, advancing or financing the commission of a grave terrorist offence or rewarding its commission, or with the intention of assisting, advancing or financing the activity of a terrorist organisation (CTL s.31(a)). Proof that the transaction was performed for one of the intentions set forth is sufficient, even if it is not proven for which of those intentions specifically.

Property transaction is broadly defined (see c.3.1). *Grave terrorist offence* is defined as a *terrorist act* that meets certain conditions, namely that it carries a penalty of five years or more (after increasing the penalty of the offence as specified in s.37). A *terrorist act* is an offence or threat to carry out an offence which: (a) is carried out with a political, religious, nationalistic, or ideological motive; (b) is aimed to provoke fear or panic or to compel a government or international organisation to do or abstain from doing any act; and (c) includes a risk of serious harm to personal safety, property, religious objects including places of worship, infrastructure, or the State's economy or environment. All activities covered by the Conventions and Protocols in the Annex to the TF Convention have been criminalised and meet the definition of *grave terrorist offence* in Israel.

Prohibition on a transaction in terrorist property: It is also an offence to carry out a *property transaction* that is capable of assisting, advancing or financing the commission of a grave terrorist offence or rewarding its commission, even if the recipient of the reward is not the person who committed the terrorist offence or the person who intended to commit it. It is sufficient to prove that the person who carried out the transaction was aware that one of the aforementioned possibilities existed even if it is not proven which one of them (CTL s.32(a)(1)).

Criterion 5.2 – The TF offences described above extend to any person who provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part, to carry out a terrorist act. The offence in s.31(a) also applies to financing a terrorist organisation. In addition, it is an offence to provide a service or resources to a terrorist organisation, where doing so may assist or promote the organisation's activity (CTL s.23).

With regard to the individual terrorist, it is an offence for anyone to perform a property transaction with a person whom he knows to be a terrorist operative, or he knows that the person or the organisation in which he takes an active part is a designated terrorist organisation. *Terrorist operative* is defined as a person who takes part in the commission of a terrorist act or who aids or solicits the commission of a terrorist act, or who takes an active part in a designated terrorist organisation (CTL s.32(b)). In addition, it is an offence for any person to provide a service such as a

transportation service, shelter, refuge, money, food, vehicles, or any other resource to any person in which doing so may facilitate, directly or indirectly, the commission of a terrorist act, ease its commission, or facilitate escape from justice (CTL s.25).

Prior to the CTL entering into force in November 2016, the main TF offences, similar to those above, were contained in the Prohibition on Terrorism Financing Law 2005 (PTFL) and previous legislation. These include:

- PTFL, s.8(a), relates to prohibition on a property transaction for the purposes of terrorism. It penalises "One who performs a transaction in property for the purpose of enabling, furthering or financing the perpetration of an act of terrorism, or to reward the perpetration of an act of terrorism, or for the purpose of enabling, furthering or financing the activity of a declared terrorist organisation or of a terrorist organisation".
- PTFL, s.9, relates to the prohibition on a transaction in terrorist property.
- The Defence Regulations (State of Emergency) (1945), established various relevant offences including fund raising and provision of services to an unlawful (terrorist) association (s.85(1)(c) and (h)).
- Prevention of Terrorism Ordinance (1948), s.4, provides that a person who gives money or money's worth for the benefit of a terrorist organisation is guilty of a criminal offence. The provision of a location or an article to a terrorist organisation for its use is similarly treated.
- Penal Law (1977), s.148, criminalises the payment of membership dues to an unlawful (terrorist) organisation.

Criterion 5.2bis – As mentioned above it is an offence to provide any service or resource to a terrorist organisation, where doing so may assist or promote the organisation's activity (CTL s.23), and providing any service, including a transportation service, money, vehicles, or gasoline, where doing say may facilitate, directly or indirectly the commission of a terrorist act, ease its commission or facilitate escape from justice (CTL s.25). These offences seem broad enough to cover the financing the travel of individuals for the purpose of perpetration, planning, preparation of, or participation in terrorist acts or providing or receiving terrorist training. In addition, providing or receiving terrorist training is an offence (CTL s.29), and anyone who finances this can also be prosecuted as an accessory.

Criterion 5.3 – The TF offences relate to "property" which is broadly defined to include land, moveable property, money and rights, including property that is consideration for the aforementioned property, and any property that grew or derived from the property or its profits. This definition would appear to cover any funds or other assets whether from a legitimate or illegitimate source.

Criterion 5.4 – The TF offences do not require that the property was actually used to carry out or for the attempt to carry out a terrorist act, nor be linked to a specific terrorist act. It is sufficient that one of the possibilities in the sections 31 and 32 exists even if it is not proven which one of them.

Criterion 5.5 – The intentional element of offences (including TF) can be inferred from the objective factual circumstances. For example, there is a presumption in the Israeli jurisprudence that a person intends to the natural consequences of his deeds. In addition, this is covered specifically in law such as in s.32(a), which provides that when a person who carries out a transaction in property of a person whom he knows is a terrorist activist or he knows that is designated as a terrorist activist or terrorist organisation, there is a presumption that he did so with the knowledge that the transaction might enable, further or finance the perpetration of an act of terrorism, or serves as a reward for the

perpetration of an act of terrorism, as relevant, unless he proves that he did not know so. This is reinforced by s.2(b) CTL, which indicates that wherever the word "intention" appears in the law, foreseeing as near-certain possibility that an act will result in certain outcomes in tantamount to an intention to cause them.

Criterion 5.6 – Proportionate and dissuasive criminal sanctions apply to natural persons convicted of TF. These are as follows:

s.31(a)	Prohibition on a property transaction for the purposes of terrorism – offences related to the financing of terrorist acts and terrorist organisations	10 years imprisonment or a fine twenty-times the fine prescribed in Section 61(a)(4) of the CC
s.32(a)	Prohibition on a transaction in terrorist property – offences related to the financing of terrorist acts	7 years imprisonment or a fine ten-times the fine prescribed in Section 61(a)(4) of the CC
s.32(b)	Prohibition on a transaction in terrorist property – offences related to the financing of an individual terrorist	7 years imprisonment or a fine ten-times the fine prescribed in Section 61(a)(4) of the CC
s.23	Prohibition on providing a service or resources to a terrorist organisation – offences related to the financing of a terrorist organisation.	5 years imprisonment
s.25	Providing resources for committing a terrorist act - offences related to the financing of an individual terrorist and financing the travel for terrorist training	5 years imprisonment

Criterion 5.7 is According to Israeli law the offences of terrorist financing extend to legal entities as well. Section 1 of Interpretation order defines *"person"* – including corporation or association or association of individuals, whether they are incorporated or not. According to section 23 of the CC, a legal person may be prosecuted when the offences are committed by a person who according to his position, authority and responsibility in the management of the legal person, the act by which he committed the offence, his criminal intent or his negligence, under the circumstances of the case, are attributed to the legal person. This does not preclude the possibility of parallel civil or administrative proceedings.

Criterion 5.8 – The Criminal Code provides, and details the penalties for, the circumstances when the range of ancillary offences to TF would be available. For example attempt (s.25); participating as an accomplice (ss.29 and 31); organising or directing others (s.29 and 30); and contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose (s.29(b)).

Criterion 5.9 – TF offences are predicate offences for ML, pursuant to Schedule 1 of the PMLL – these include for example, the offences in ss.23, 25, 31, and 32 of the CTL.

Criterion 5.10 – TF offences do not require the offender to be in the same country in which the terrorist organisation is located or the terrorist act occurred. According to section 7(a)(1) of the CC, a Domestic Offence is an offence, which all or part of it was committed within Israel territory. Therefore, any part of the TF offence can occur within Israel and this would be covered. According to section 41 of the CTL, an offence pursuant to sections 20, 21, 22, 29, 30 or 31 that is a foreign offence as defined in section 7(b) of the CC (e.g. preparation, attempt, conspiracy) and that is committed by a member of a designated terrorist organisation where the organisation has a link to Israel, or [is committed] in connection with such a designated terrorist organisation, shall be deemed an offence against national security, and therefore can be tried in Israel.

Weighting and Conclusion

Recommendation 5 is rated compliant.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

In its last mutual evaluation, Israel was rated largely compliant for these requirements. The technical deficiencies were that the declaration process did not apply to Israeli citizens who are Israeli residents, and that the timeframe for given effect to declarations following listings made pursuant to UNSCR 1267/1989 and 1988 was insufficiently prompt. Since then, Israel has adopted the CTL in 2016. The CTL sets out counter-terrorism and CTF measures, including targeted financial sanctions (TFS). Amendments to the CTL entered into force on 14 February 2018. These amendments streamline the designation process.

Criterion 6.1 –

(a) The Ministry of Foreign Affairs (MFA) is the competent authority for proposing designations to the 1267/1989 UN Committee and the 1988 UN Committee.

(b) Israel has not yet proposed any designation to the UN. A request to the UN would be based on information from security agencies, co-ordinated between all relevant authorities and forwarded to the UN Sanctions Committee by the MFA.. Israel has the necessary mechanisms for identifying targets.

(c) The legislation does not specify the evidentiary standard of proof that would apply to proposed designations. Israel indicates that this would be "reasonable grounds", since this is already contained in the CTL as the basis for adopting foreign designations (e.g. non-UN and foreign countries).

(d) and (e) Although it is not specified in the legislation or written procedure, Israel indicated it would follow the procedures adopted by the relevant UN Committees and provide as much as information to the Committees in making a designation proposal.

Criterion 6.2 –

(a) The CTL sets out the procedures for designation in accordance with the criteria listed in the s.2(a) of the law – compatible to those of UNSCR 1373. The Minister of Defence (MoD) shall designate persons/entities on Israeli's own motion. This is based on a reasoned request from the Israeli Defence Authority and subject to approval by the Attorney General, with information and facts for a basis of their designation requests. (CTL ss.3, 4, and 6)).

The MoD shall also designate terrorists and terrorist organisations following requests by parties outside of Israel (CTL s.11(a)(1)-(2)). The Advisory Committee may advise to the MoD upon their designation (s.14).

Previous to the CTL coming into force in 2016, Israel used the Defence Regulations (State of Emergency) (1945) to designate "unlawful associations" under section 84 of the regulations. A number of (terrorist) organisations are still designated pursuant to those regulations.

(b) Israel has mechanisms to identify targets for designation based on the designation criteria set out in UNSCR 1373. Domestic designations are based on a reasoned written request from the head of the Israel Security Agency, or from the head of another Defence Authority, and subject to the approval of the AG. In the request, the Head of the Defence Authority shall specify the information and facts on which he is basing his position.

(c) With regard to designations based on requests from other countries, the MoD will make its designation based on reasonable grounds to assume that the person or entity is a terrorist operative or terrorist organisation (s.11(a)(1)-(2)). The legislation does not indicate that this process must

occur "promptly", but the Israel authorities indicated that this would be the case in practice similar to the adoption of UN designations.

(d) The evidentiary standard of proof for making a designation is "reasonable grounds" and not conditional upon the existence of a criminal proceeding (s.11(a)(1)-(2)).

(e) When requesting another country to give effect to its freezing mechanisms/designations, Israel provides as much identifying and specific supporting information as possible.

Criterion 6.3 –

(a) In submitting their designation requests, Israeli Defence Authorities, including Israel Security Agency (ISA), should identify information and facts, which form a basis of their requests (s.3(b) of CTL). The Israeli authorities responsible for designation should have reasonable grounds to assume persons/entities, either in designation process initiated by Israeli own motion or foreign initiatives, are terrorist organisation (See also the Criterion 6.1(c)).

(b) The CTL designations operate *ex parte*. The MoD does not notify persons/entities to be considered prior to their designation. MoD first issues orders of temporary designation (*ex parte*), which are then notified to persons/entities with the aim at giving an opportunity to submit claims prior to permanent designation (ss.4 and 5 of CTL). However, s.4(e) of CTL ensures effects of temporary designation orders, and such orders enter into force upon MoD's decision of temporary designation (s.17(a) of CTL).

Criterion 6.4 – Under s.11(a)(3) of CTL, a designation by the UN Security Council of a foreign terrorist organisation is, upon publication on the UN website, automatically designated in Israel and enters into force at that time. This is a temporary designation for three months, which can be extended three more months. The time period is used for the MoD to complete the examination of the organisation and make a decision on the possibility to formally designate it as a foreign terrorist organisation under s.11(a)(3)(c) or "internally" under Article A. If the internal route is chosen, the MoD will use reasonable grounds to assume that the organisation meets the definition of a terrorist organisation (s.3(a)). Nevertheless, the process allows discretion for the MoD not to formally designate it, in which case the temporary designation will expire. Israel indicates that in formal legislative language in Israel, it is customary to grant discretionary powers to a minister, and in this case the discretion of the MoD is only the choice between the two routs of designations.

The UN designation of a terrorist operative is similarly applied automatically as a temporary designation upon publication on the UN website. The temporary designation is for 30 days, with a process to formally designate it as a foreign terrorist operative under s.11(a)(3)(c). The timeframe of 30 days is less since there is no mechanism to designate it "internally" under Article A, and therefore does not require the same level of examination. Israel indicates that for individual terrorist operatives, the MoD's discretion about formal designation is limited to checking whether the individual is an Israel citizen or resident – the designations made pursuant to s.11(a) (requests from third countries) and s.11(b)(3) (pursuant to UNSCR designations) cannot cover individuals who are Israeli citizens or Israeli residents.

Formal orders of designation enter into force upon their publication (s.17(a) of CTL); according to s.18(a), the designations are published on the MoD's website. This take place on the same day the designation was made.

In practice, all UN designations have been formally designated domestically.

Criterion 6.5 –

(a) To implement relevant UNSCRs 1267/1989, 1988 and 1373, s.34(c) of CTL prohibits any person from performing any property transaction of any terrorist organisation designated in accordance with CTL. S.32(b) prohibits property transactions with, *inter alia*, designated terrorist operatives. These prohibitions apply to all natural and legal persons. As indicated above in Recommendation 5, the definition of "property transaction" is broad. The comprehensive prohibitions on any transaction involving such property effectively meet the definition of "freeze" accounting to the FATF Methodology, as they prohibit the transfer, conversion, disposition, or movement of any funds or other assets that are owned or controlled by designated persons or entities. Since it also requires the entity to immediately refrain from performing any action, the "freeze" applies without delay and without prior notice.

Sectoral orders, directives, and circulars, require the entities to check their customers – including account holders, authorised signatories, beneficial owners, controlling shareholders, and the persons performing the transaction or parties to the transaction – against the designation lists (s.10(k) of Directive 411, s.11.1 and 11.7 of the Stock Exchange Members Circular, s.101 of the Trading Platforms Circular, s.15 of the Portfolio Managers Order and Insurers Orders, s.16 of the Postal Bank Order, s.11 of the MSBs Order, s.9 of the BSPs Order, and the s.14 of the Dealers in Precious Stones Order).

In the event of a possible match, supervised entities must immediately suspend any activity in the customer's account or transaction, and submit a report to the INP and IMPA regarding suspicious or unusual transactions and to wait for the INP instructions concerning the continuation of the activity. In the event of positive matches against the designation lists, , the MoD issues administrative seizure orders in relation to their property (s.56 and 67 of the CTL). Administrative forfeiture orders can then be issued be issued for these cases (s.66(a) of the CTL).

To facilitate the potential identification of potential accounts and funds, there are additional obligations in the AML/CFT Orders issued to supervised institutions. According to the definitions section of the various Orders, the "List" is a centralised list of designated terrorist organisations and of people designated to be terrorist activists, published pursuant to section 18 of the CTL. The entities are required to review the consolidated list of designated terrorist operatives and terrorist organisations published pursuant to section 18 of the CTL, the names of various entities in the account, as well as the names of the parties to the action they are requested to carry out. (s.11 of the MSB Order, s.13A of the Banking Corporations Order; s.9 BSP of the Order, s.16 of the Postal Bank Order, s.15 of the Insurers and the Portfolio Managers Orders, s.17 of the Stock Exchange Members and Trading Platforms Orders).

(b) The scope of "property" defined in CTL covers land, moveable property, money and rights, including property that is consideration for the aforementioned property, and any property that grew or derived from that property or its profits. It also includes property owned by, or in the possession, control or custody of a terrorist organisation, by itself or together with another (and by extension terrorist operative), as well as property used or designated for use by a terrorist organisation or for a terrorist organisation's activity, including property whose purchase was financed by the organisation or that the organisation transferred to another for no consideration. Under Israeli jurisprudence, "control" covers indirect control.

(c) The prohibitions in s.25, 32 and 34(c) of CTL broadly cover the prohibition of making any other funds or assets, or financial or related services, available to designated persons or entities. However, they do not specifically cover providing funds or assets "wholly or jointly".

(d) A notice of designation or revocation orders issued by MoD, the Ministerial Committee or the Government are published on the website of MoD (s.18(a) of the CTL). Those orders should include

identity of designated persons/entities (s.2 of the Regulation for the Combating Terrorism (CTR)). Furthermore, MoD, in consultation with MoJ, may take additional ways to communicate with the public on those orders (s.18(b) of CTL). In addition, IMPA and Israeli supervisory authorities disseminate the list of the designated persons/entities (via email, and other means if necessary) and provided guidance to obliged entities on their TFS obligations.

(e) The CTL requires any person, including FIs and DNFBPs, to report to the Israeli Police when she/he could have been engaged in transactions of or hold properties of designated persons/entities in his control (ss.33 and 34 of CTL respectively). In case of breaching the said reporting duties, penalty of imprisonment or fine set out in the Penal Code will be imposed (s.36 of CTL).

(f) The rights of bona fide third patties acting in good faith are protected when implementing their TFS obligations (s.35(a) CTL).

Criterion 6.6 –

(a) Israel did not provide information on its procedures for submitting de-listing requests to the UN Sanctions Committee, in line with this criterion.

(b) Israel has legal authorities and procedures to de-list and unfreeze funds or other assets of persons and entities designated pursuant to UNSCR 1373, that no longer meeting the criteria for designation. The MoD may revoke its designation orders when there are no longer grounds for the designation or designated persons/entities or are no longer engaged in terrorist activities (s.7(a) and 13(b) of CTL). Designation by foreign parties, which forms a basis for designation in accordance with s.11(a) of CTL, should be examined annually (s.6(2) of CTR). The Advisory Committee conducts a periodic review on the list of designation and makes recommendations to the Ministerial Committee, considering any additional information provided Defence Authorities (s.12 CTL and s.12 of CTR).

(c) Persons and entities designated pursuant to UNSCR 1373 may apply to having their designation reviewed and revoked. They may submit written de-listing requests, with any supporting documents, to the Minister of Defence (ss.5(a), 7, and 13 of CTL respectively). These requests are channelled through the Advisory Committee, who discusses the matter and may summon the parties to appear before it, then provides a reasoned opinion to the Minster of Defence (ss.5(e) and 13(a)). Sections 7 and 8 of the CTR set out detailed procedures for requesting revocation of designations.

(d) and (e) Israel did not provide information on procedures to facilitate review by the 1988 Committee, or procedures for informing designated person and entities of the availability of the UN Office of the Ombudsperson.

(f) Israel has procedures for unfreezing funds or other assets of persons who are inadvertently affected by a freezing mechanism (s.32(c)(1)-(2) of the CTL). This procedure allows – following verification with the Police that the person or entity involved is not a designated person or entity – to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities.

(g) See the analysis on the Criterion 6.5(d).

Criterion 6.7 – The CTL does not have comprehensive measures to cover access to frozen funds for basic and extraordinary expenses. Section 60 indicates that for the seizure and forfeiture of property, section 36C of the Drugs Ordinance applies. This indicates that the court shall not order the forfeiture of property unless the owner of the confiscated property and his family members living with him will have reasonable means of subsistence and a reasonable place of residence. Firstly, this only applies following a seizure (at confiscation stage) rather than after the freeze. Secondly, the article does not cover all the situations in UNSCR 1452.

Weighting and Conclusion

The provisions in the CTL meet or mostly meet most of the technical criteria for Recommendation 6, in particular, the most important criteria regarding the freezing without delay and without prior notice of funds and other assets of individuals and entities designated pursuant to UNSCRs 1267 and 1373. This obligation applies to all natural and legal persons. Nevertheless, the process allows discretion for the MoD not to make permanent the automatic designations from the UN, in which case the designation will expire. The designations made pursuant to requests from 3rd countries and pursuant to UNSCR designations cannot cover individuals who are Israeli citizens or Israeli residents. There are not procedures for submitting de-listing requests to the 1267/1989 or the 1988 Sanctions Committees, to facilitate review by the 1988 Committee, or for informing designated persons and entities of the availability of the UN Office of the Ombudsperson. Finally, the CTL does not have comprehensive measures to cover access to frozen funds for basic and extraordinary expenses.
Recommendation 6 is rated largely compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation financing

Israel has several pieces of legislation dealing with proliferation and proliferation financing from Iran. New legislation – the Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law – entered into force on 11 March 2018 (during the on-site visit). This legislation transposes immediately all proliferation financing UN listings on Iran and DPRK, while processing them for permanent domestic designation similar to the process described in R.6. The legislation also expands the role of the Sanctions Bureau within the Ministry of Finance. Previously, the applicable legislation was the Trading with the Enemy Ordinance, 1939, as clarified in the Trading with the Enemy Order, 2011. Israel also used the Combat of the Iranian Nuclear Program Law, 5772-2012 (CINPL). The Sanctions Bureau co-ordinates the designation and sanctioning process.

The previous legislation and measures did not include targeted financial sanctions related to DPRK. Israel had relied on the Import and Export Order (Control of the Export of Goods to the Democratic People's Republic of Korea), 5776 – 2105.

Criterion 7.1 – Targeted financial sanctions on PF are implemented without delay. The PF-TFS measures were updated and enhanced with the Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law, which entered into force on 11 March 2018. The law incorporates all proliferation and PF-related UNSCRs automatically on a temporary basis, with a process to make them permanent designations, as described below.

Criterion 7.2 –

(a) Section 3(a) of the new law states that any foreign entity designated as assisting a country in distributing and financing of weapons of mass destruction shall be automatically designated by Israel on a temporary basis, for up to four months. The measure is in force upon publication on the Sanctions Bureau's website, which must be within 24 hours of the UN designation. Then, the Minister (of Finance) upon consultation with the MoF's Sanctions Bureau and its recommendation, is entitled to make the declaration permanent. All persons must refrain from conducting any financial activity with a declared entity or a "related entity" (s.5(a)). "Related entity" refers to a controlling shareholder or stakeholder in a corporation that is a declared entity, or a corporation where the declared entity is a controlling shareholder or stakeholder.

Financial activity is broadly defined to include any activity of financial value, including trade, extending or obtaining a loan, providing or obtaining a service, including a financial service, grant or

receipt of ownership or other right to property or granting a financial right under law. While the measures do not specifically call for "freezing" action as defined by the FATF, the broad prohibitions on any financial activities with the designated entities satisfy this criterion. Since it also requires the entity to immediately refrain from performing any action, the "freeze" applies without delay and without prior notice.

However, there is discretion for the Minister not to permanently declare the entity, or to revoke a declaration even if the UNSC does not de-list it. Declarations cannot be applied to Israeli citizens or residents. Israel relies on its domestic legislation and criminal proceedings in cases where Israeli citizens or residents on the lists (e.g. s.3 of Trading with the Enemy Ordinance, s.4-5 of the 2012 Law for Countering Iran's Nuclear Programme, s.5 of the Prevention of Distribution and Financing of Weapons of Mass Destruction Law, and the PMLL). However, since UNSCR resolutions pertain to Iranian and DPRK persons and entities, this is only a minor deficiency.

(b) The prohibition on economic and financial activity in the new law largely applies to all funds or other assets that are owned or controlled by the designated person or entity. The prohibition on financial activity with a "related entity" extends the scope to controlling shareholders or stakeholders or a corporation controlled by a designated entity. It does not specifically cover funds that are wholly or jointly owned or controlled, directly or indirectly, by the designated person or entity; or the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly.

(c) The new law effectively covers preventing any funds or other assets from being made available to or for the benefit of designated persons or entities (s.5(a)). The Minister may allow certain financial transactions with designated entities, pursuant to UNSCR guidelines or upon authorisation (s.5(b)).

(d) Israel has mechanisms to communicate the Iran and DPRK designations. All Israeli supervisors (BoI, CMISA, ISA, and the Postal Bank) issued guidelines and circulars alerting entities under their supervision of the Order directing them to adapt their internal policies and procedures to be aware of the PF risks and evaluate their exposure, and to monitor transactions and conduct due diligence and identify matches with international lists. The guidelines and circulars did not refer specifically to measures on DPRK. However, they do refer to the need to refer to the UN lists on PF (and for banks, non-bank stock exchange members, and trading platforms screen against these lists), and take these into account for their AML/CFT programmes. The entities are required to check their customers – including account holders, authorised signatories, beneficial owners, controlling shareholders, and the persons performing the transaction or parties to the transaction – against the designation lists (Directive 411, s.10(k), Stock Exchange Members Circular, s.11.1 and 11.7, and Trading Platforms Circular s.10.1).

In July 2017 IMPA published guidelines to the supervised entities regarding the requirements for the prevention of TF and proliferation, including: checking against the list of designated entities, delaying action, obtaining instructions from the police and reporting to IMPA - by virtue of the provisions of the orders and the law. The guidelines do not refer specifically to DPRK. However, IMPA distributes the list of entities designated in accordance with the UN Security Council resolutions, including Iran and DPRK, shortly after their announcement by the UN. In this way, the supervised bodies can take immediate action after the designation if there is a match with the list. Israel also recently updates the guidelines in March 2018 (during on-site).

(e) The Trading with the Enemy Ordinance requires persons who suspect that they have been asked to trade with the enemy, to report the matter to the INP and IMPA (ss.5A and 5C). The Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law also

requires reporting of any suspected transaction (including an attempted transaction) with a designated entity to the INP (s.6(a)).

(f) The Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law protect the rights of *bona fide* third parties when acting in good faith to comply with the law (s.7(a)).

Criterion 7.3 – There are measures for monitoring and ensuring compliance with the obligations against Iran pursuant to the Trading with the Enemy Order. Each supervisor designated under the PMLL also monitors for compliance with the Order, with the same enforcement powers (s.5(C)(a) and (c)-(d)). Enforcement measures include criminal sanctions (s.3) and administrative sanctions (s.5C 5C(e)). There are parallel provisions in the Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law ss. 8(c)-(e)). However, some DNFBPs are not covered under the AML/CFT framework. There are also criminal sanctions applying to all persons: three years imprisonment and a fine up to four times the sum contained in s.61(a)(4) of the Criminal Code. For a legal person, the fine is doubled.

Criterion 7.4 – The Sanctions Bureau has published the UN procedure – including submitting de-listing requests – on its website. However, there are no official domestic procedures for submitting de-listing requests to the UN Security Council in the case of designated persons and entities that, in view of the country, do not or no longer meeting the criteria for designation. The Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law contains measures to consider not continuing with a temporary designation (s.10) or revoking a permanent designation (s.11), but these measures do not involve the UN.

Criterion 7.5 – With regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to TFS pursuant to the Order or the Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law, the person must immediately cease any financial activity and report this to the Sanctions Bureau (s.5(d)). The law does not cover permitting the addition to the accounts frozen pursuant to UNSCRs 1718 or 2231 of interest or other earnings, or not preventing a designated person or entity from making a payment due under a contract entered into prior to their listing.

Weighting and Conclusion

Israel meets or mostly meets the most important criteria of Recommendation 7. The Prevention of Distribution and Financing of Weapons of Mass Destruction or Means of Carrying Thereof Law, cover the most important requirements of PF-related TFS in terms of requiring all natural and legal persons to freeze funds and other assets without delay and without prior notice, and to prohibit making funds available to designated persons. There are measures to ensure compliance, including criminal and administrative sanctions. However, there are some minor deficiencies: there is discretion for the Minister to not make a UN designation permanent; it is not clear that the prohibitions apply to all funds that are wholly or jointly owned or controlled, directly or indirectly, by the designated person or entity or the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly; there are no official domestic procedures for submitting de-listing requests to the UN Security Council in the case of designated persons and entities that, in view of the country, do not or no longer meeting the criteria for designation; and there are no provisions with regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to TFS.

Recommendation 7 is rated largely compliant.

Recommendation 8 – Non-profit organisations

Israel has not been assessed against the detailed requirements of R.8 following the 2016 adoption of changes to Recommendation 8 and its Interpretative Note.

The ICA which includes, inter alia, the Registrar of Amutot, the Registrar of Charities and the Registrar of Companies, is responsible for the registration of NPOs and enforcement of the legislation pertaining to NPOs.

The vast majority of NPOs are established as Amutot; which are legal persons incorporated and registered with the ICA under the Amutot Law. NPOs are also incorporated and registered as charitable companies under the Companies Law. There is one further type of incorporated NPO (but not registered with the ICA), namely the ottoman association. The Ottoman Associations Law was cancelled by the Amutot Law except that it continues to apply to existing ottoman associations that are not registered as Amutot or have not been struck off or otherwise dissolved. Government Decision 3662 of 11 March 2018 transfers responsibility for registering ottoman associations from the Ministry of the Interior to the Minister of Justice and the ICA.

Public trusts are legal arrangements governed by the Trust Law and registered by the ICA (except with regard to religious trusts).

There are no general legal provisions prohibiting or explicitly recognising unincorporated non-profit activity; nevertheless, such activity is undertaken. The main type of unincorporated organisation is the Gemach ("act of kindness"). These are not required to be registered with the ICA although the Israeli authorities have advised that Gemach are registered with the ITA by virtue of the FATCA framework. A statutory regulatory framework for Gemach is under discussion in the Knesset.

Criterion 8.1 –

(a), (b) & (c): Israel has identified NPOs that fall within the FATF definition of NPO, and identified those features and types of NPOs that are more likely to be at risk of TF abuse. The non-classified TF NRA report includes some analysis of donations and charities and specifies that the financial system is not used for TF (also see IO.1 and IO.10). The classified TF NRA report includes much more detail and assessment. Israel has used wide ranging sources of information, and identified that NPOs with international transfers and foreign donors as having higher risks, including the nature of their threats. In addition, Israel has reviewed its measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for TF purposes.

(d): The action plans developed after the NRA specify that the NPO risk assessment will be updated periodically. The State Attorney is specifically charged with instructing the IC to examine and update, where necessary, Israel's national risk assessment (which includes NPOs).

Criterion 8.2 –

(a) – While clear polices have not been articulated in writing, measures have been taken to promote accountability, integrity, and public confidence in the administration and management of NPOs through governmental decisions, regulations and published guidelines for the conduct of amutot and charitable companies (see below) and operational measures undertaken in practice. Measures differ as between different types of NPO but not due to counter ML/TF purposes. In practice, the measures outlined in this criterion below cover the NPOs most at risk of TF abuse (and NPOs not covered by the text below are not material in terms of TF).

i) There are requirements for registration with the Registrars within the ICA (including requirements to provide information to support the registration) for:
- Amutot at sections 1 - 8 of the Amutot Law;
- charitable companies at sections 5, 8, 10, 23 and 345B of the Companies Law as well as the Companies Regulations (Reporting Registration Details and Forms), 5759-1999; and
- public trusts which are not religious trusts (see section 41 of the Trust Law for this exemption) under section 26 of the Trust Law within three months of the appointment of a trustee.
- The ICA has established a publicly accessible, free of charge, database on NPOs on its website or in more detail - the "GuideStar" website. This includes, inter alia, information on individual NPOs such as annual financial statements and reports. It also includes a document by IMPA on ML and TF red flags. Information is published on the website under section 39(a) of the Amutot Law, which applies to charitable companies under section 345X(e) of Companies Law, and section 26(c) of the Trust Law. These statutory provisions also enable public access to more extensive information held by the ICA.
- Amendments to the Amutot and Companies Laws (section 39A of the Amutot law and section 345C1 of the Companies Law) in 2015 require the Registrar to publish guidelines to facilitate the conduct of amutot and charitable companies in accordance with the relevant law. Guidelines on amutot were published in December 2015 and have been updated several times, most recently in March 2017. As expressly specified in the preface of the guidelines, they also apply to charitable companies. The guidelines stem from the law and are considered an interpretation of the law by the Registrar. Therefore, not complying with the guidelines is considered by the ICA to be non-compliance with the law and enforceable as such. In the absence of court judgments on this matter the assessment team is not wholly persuaded that the guidelines are enforceable.
- Under section 39A of the Amutot Law and section 345C1 of the Companies Law, the ICA and its staff participate in seminars and conferences with NPOs (including their accountants and lawyers) to promote awareness of policy and interpretation of the law and to give guidance so as to ensure compliance with the legislation.

ii) NPOs registered at the ICA are under a statutory obligation to submit information on an annual basis. Sections 36, 37A, 38(3), (6), (6A) and annex 2 of the Amutot Law include a requirement to provide an annual report and financial statements. Section 141 of the Companies Law requires provision of an annual report, the form and content of which is prescribed under the Companies Regulations (Reporting Registration Details and Forms), 5759-1999. Section 345x of the Companies Law provides that, in addition to the general reporting requirements for companies which must be submitted to the Registrar of Charities, a charitable company is also subject to all the reporting requirements of amutot under sections 36, 36A, 38, 38A and annex 2 of the Amutot Law of Charities, including the provision of annual financial statements and other reports to the Registrar of Charities. Regulations 11 and 12 of the Charities Regulation (Charity), 5743-1974 and form 2 in the annex of those regulations mandate the submission of an annual financial report by a charity and the form of that report.

iii) There is a requirement for amutot and charitable companies to report donors' names in an annex to the financial statements submitted annually, in donations exceeding the amount set in the Amutot (Non-Profit Associations) Regulations (Determination of the Maximum Amount and Procedures for the Recording of Donations in the Financial Statements as Anonymous), 5763-2002. The financial statements and the annex, including donors' names, are available for public perusal. The ICA can provide exemptions in individual cases from public perusal of a

particular donor's information although the information must still be submitted to the ICA; this stems from section 36(a) and article c of the annex 2 of the Amutot Law and the aforementioned regulations. The provisions of the Amutot Law mandating disclosure of donors' names are applied to charitable companies under sections 345X(b) and (f) of the Companies Law.

iv) The ICA, using its own staff or inspectors can require information to be provided by officers, staff of NPOs and any other person related to the matter (sections 38-39E of the Amutot Law; sections 345x1 and 345x4 of the Companies Law; section 29 of the Trust Law) The ICA also uses these provisions to deal with complaints by the public and governmental bodies regarding amutot and charitable companies.

v) The ICA can also conduct inspections by using its own staff or third parties under sections 39B-39E of the Amutot Law, sections 345x1 and 345x4 of the Companies Law and section 29(b) of the Trust Law. In addition, section 30 of the Trust Law provides for investigations to be undertaken by the Registrar in relation to trusts.

vi) Amutot, charitable companies and public trusts which seek governmental support must obtain an annual certificate of proper conduct from the Registrar. Government Decisions 4418 from 1998 and 562 from 2001 refer. Although not mandated by legislation, practice has developed in which NPOs may also request such a certificate for the purpose of collecting private donations. The issue of a certificate depends on the NPO meeting reporting requirements and compliance with the law. NPOs receiving a certificate are subject to assessment by the ICA; if the NPO does not remediate issues found or if the misconduct is significant, the certificate can be cancelled or not renewed until such time that the Registrar is satisfied that the misconduct has been resolved. The Israeli authorities have advised that, although there is no explicit statutory language with regard to a refusal by the ICA to issue a certificate nor an explicit ability not to renew or to cancel a certificate, it can do so under generally accepted powers on the exercise of public administrative powers and the conduct of government authorities under sections 14 to 18 of the Interpretation Law 5741-1981. The ICA has exercised all of these powers.

vii) The powers of NPO audit committees for amutot and charitable companies were expanded in 2015 (sections 345H(6A)-(6D) of the Companies Law and sections 30(6A)-(6C) of the Amutot Law). In addition, NPOs with a yearly income of more than 10 million NIS are required to appoint an internal auditor (sections 30 and 30A of the Amutot Law; sections 345H and 345I of the Companies Law).

viii) Under Charities Regulation 5734 of 1974 there are requirements for the contents of a deed of endowment for a public trust to be provided to the Registrar of Charities, the management of endowment assets, furnishing the Registrar with an annual report and the publication by the Registrar of a list of endowments.

ix) Under section 50 of the Amutot Law and section 345S of the Companies Law, the relevant Registrar can apply to court for the dissolution of an amuta or charitable company including, inter alia, if the NPO is not complying with the law, its purposes or its articles of association.

x) Under section 131(a)(5) of the Income Tax Ordinance, NPOs with an income must file annual reports, which specify income and expenditure, with the ITA, together with a letter by the NPO informing the ITA of a change in its goals or the expenditure of the funds when there has been

such a change. NPOs can also apply for a donation certificate (see section 46(a) of the Income Tax Ordinance). Donors to NPOs in possession of such a certificate can receive a tax deduction against their donation.

(b) – There is a written procedure in connection with outreach, but also a mechanism which demonstrates that outreach is taking place in practice. The ICA has distributed IMPA's red flags document at outreach events for NPOs and lawyers and accountants which act in an advisory capacity to NPOs. Some outreach has been undertaken to the donor community and the ICA has published "golden rules" for donors on its website. Round tables and advisory fora for issues in the NPO sector have also included representatives of the donor community, in particular the business sector. See sub-criterion 8.2(a) above and IO.10 on relevant legal provisions and activities directed at NPOs.

(c) – No written policies or procedures have been provided demonstrating that best practices to address TF risk and vulnerabilities were developed and refined in collaboration with NPOs, although the Israeli authorities indicate that the policy is drawn from a combination of guidance and practice. The ICA has developed guidelines for amutot and charitable companies and published the red flags document by IMPA on its website.

(d) – The ICA has produced guidelines for the conduct of amutot. While they do not explicitly encourage NPOs to conduct transactions via regulated financial channels (e.g. through banks) the effect of the provisions in the guidelines is that transactions should take place through regulated financial channels. The guidelines also apply to charitable companies in accordance with section 345C1 of the Companies Law and as expressly addressed in the preface to the published guidelines. They do not apply to public trusts (although there are administrative guidelines which do not stem from any legal provision). The supervisory mechanisms of the ICA also directs the NPOs to use regulated financial channels.

Criterion 8.3 – The Amutot and Companies Laws provide powers for the Registrar to ensure compliance with the relevant law by NPOs. See c.8.2(a) above for the Registrar's powers to obtain information, conduct onsite inspections and issue guidelines.

Amutot and charitable companies are subject to two types of inspections. First, in depth inspections are conducted by external auditors using some of between 6 and 12 standard focal points to guide the inspection. The nature of the NPO informs the inspection approach and which of the focal points will be reviewed. Input from a third-party such as a request by the INP or the *Shin-Bet* leads to a specific focal point beings selected for the NPO in question. The second type of inspection is conducted by ICA staff, undertaken without notice to the NPO, usually as a result of complaints received from the public against a specific NPO. The overall approach is guided by way of procedure, with the focal points being published on the ICA's website.

While not all NPOs are subject to registration and supervision by the ICA, the types of NPO identified as more vulnerable to abuse are subject to registration and supervision. Supervision also addresses the risks of international transfers and donors (see IO.10). However, ICA's overall approach is not risk based.

In addition, the ITA has an oversight role for NPOs which have an income and declare that income to it. The ITA does not have written policies, procedures or checklists on oversight mechanisms. With the assistance of a computerised risk management system, the ITA checks NPOs' annual reports to verify if expenditure is in line with public activity, and seeks to ascertain the destination of funds and whether expenditure is consistent with the definition of public institution. While, mainly for the purposes of dealing with tax exemption applications, the ITA's activities are relevant to addressing TF risk even if the activities themselves do not comprise a TF-focussed approach. See IO.10. (S.9(2) of the Income Tax Ordinance and circular 9/2015.)

Criterion 8.4 –

(a) – See c.8.3.

(b) – See c.8.3 and, for charitable companies, the "violating company" analysis in c.24.13. If deficiencies are found in the conduct of an amuta or charitable company, the NPO is potentially exposed to liquidation proceedings and the certificate of proper conduct, if applied for or received, can be denied or withdrawn (see above). In addition, the ICA has striking off powers under section 59 of the Amutot Law; criminal sanctions are available against Amutot under sections 64 and 64A of the Amutot Law; administrative fines are available against charitable companies under section 354 of the Companies Law (also see c.24.13).

The power of liquidation is interpreted and implemented by the ICA (supported by the courts) in a way that includes interim powers so that the NPO may be allowed (when circumstances warrant this), to remedy the deficiencies to the ICA's satisfaction as an alternative to undertaking liquidation proceedings, and since the certificate of proper conduct can also be used to require a NPO to remedy the deficiencies found in the NPO's conduct.

However, the ICA lacks a wider range of sanctions, such as directly issuing directions and imposing fines. Powers available to ICA are also not consistent across registered NPOs.

Separately, ITA has additional powers of civil sanctions (sections 188, 191-191B of the Income Tax Ordinance) and criminal sanctions (sections 215 to 228A of the Income Tax Ordinance).

Criterion 8.5 –

(a) – Co-operation and co-ordination of operational matters on NPOs between authorities is strong but the overall jurisdictional response is not co-ordinated. There is also no policy, procedure, or written process for effective co-operation and information sharing to the extent possible separate to the Decision. Government Decision 1933 requires government authorities to put in place policies so that information received by one government authority should be disclosed as appropriate to other authorities rather than the public having to provide the same information more than once to different parts of government. The Government Information and Communication Technology Authority is responsible for co-ordinating the implementation of this Decision. However, this Decision is more relevant to enhancing government efficiency rather than CFT.

Legislation does not expressly enable the ICA to obtain information for other investigative bodies such as the INP, the ITA or IMPA but it has been able to obtain information on behalf of third parties. There are no express provisions for the ICA to disclose information voluntarily but the Israeli authorities have advised that non-public information held by the ICA can be disclosed to another governmental authority under chapter 4 of the privacy protection law and principles of generally accepted conduct for a public authority unless disclosure is expressly prohibited by law; such information has been disclosed. Information on suspicion of criminality is disseminated by the relevant Registrar to IMPA, the Shin Bet and the INP under these principles and it shares files with LEAs conducting investigations.

There is co-operation between the ICA and the Shin Bet. The ICA has received information from the Shin Beit and requests from the Shin Beit to provide information about a NPO or to conduct an inquiry in connection with a NPO.

During the course of an investigation by the INP information is disclosed to the ITA within the limitations that apply to the INP (for example, prohibition on sharing information, disclosure of sources and disruption of the investigation). In some cases, when more information is needed, the INP issues a request to IMPA for information it holds or to facilitate the obtaining of information from the enforcement agencies in other countries (for example, countries where the NPOs are registered).

In cases where the controlling shareholder/beneficiaries of these NPOs are known, these persons are also examined by the LEAs. Where there are grounds for a criminal investigation, the possibility of conducting a joint investigation with several relevant LEAs will be considered by the INP; joint investigation teams have been established in practice.

(b) – As mentioned above, the ICA has powers to obtain information from NPOs and conduct inspections on compliance with the legislation it administers. In addition, the Registrar can open a statutory investigation in relation to a NPO (section 40 of the Amutot Law, section 345r of the Companies Law and section 30 of the Trust Law). When the ICA receives information which raises suspicion of criminality, it provides the information to the INP and IMPA for further investigation. The INP, as the authority responsible for TF investigations, and IMPA have relevant expertise and capabilities to examine and investigate those NPOs suspected of being exploited by, or actively supporting, terrorist activity or terrorist organisations.

The ITA has powers of investigation and can obtain information in relation to civil and criminal tax matters under section 227 of the Income Tax Ordinance. It has the relevant expertise and capabilities to examine and investigate NPOs.

(c) – The INP is responsible for the investigation of terrorism and terrorist financing offences under the Police Ordinance (s.3). With reference to s.ss.23-25 of the Criminal Procedure Ordinance (Arrest and search), it is entitled to obtain information from any person on the administration and management of particular NPOs, as well as any financial and programmatic information which exists, and also provides for provisional measures such as search and seizure to be available to the INP, including when investigating suspicion of TF committed by an NPO or in relation to an NPO.

In addition, the transfer to the INP of information on the ICA's central database for legal persons (which includes information on ownership or control of NPOs) was permitted in accordance with the procedure under chapter 4 of the Privacy Protection Law.

(d) – See R.20 and R.23 for the requirements on FIs and DNFBPs to report suspicion of TF. Following receipt of an STR, IMPA provides information to the INP and the security agencies for investigation and seizure of property. The INP has measures that allow it to take provisional measures (freezing or seizure) in order to prevent transactions taking place. No procedure on the prompt sharing of information between authorities and preventive and investigative action has been provided to the evaluation team.

Criterion 8.6 – The Israeli authorities advise that the point of contact for international requests is the INP's legal assistance section. The dissemination of information within Israel to the INP is separate to the main route for MLA. Where a request for information is received from abroad by the INP, it will be passed through the Interpol squad to the EEU, which has a ML/TF squad (one of its employees is regularly located in IMPA). While the INP is responsible for TF investigations and the Israeli authorities have identified an appropriate point of contact, there is no written policy or procedure on this or public information that articulates that the legal assistance section of the INP is the designated point of contact. Notwithstanding this, the close operational co-ordination between the authorities suggests to the assessment team that any international contact with an authority other than the INP or to part of the INP other than its legal assistance section would be directed to the right respondents.

Weighting and Conclusion

There are mechanisms on promoting accountability, integrity and public confidence but clear policies are not in place. The ICA is proactive, but its overall approach is not risk-based. Sanctions are in place

but not wholly proportionate. Operational co-operation is strong but there is a gap with regard to whole of government co-ordination.

Recommendation 8 is rated largely compliant.

Recommendation 9 – Financial institution secrecy laws

In its last MER, Israel was rated compliant for these requirements.

Criterion 9.1 – There are no statutory laws or other measures (including data protection and privacy law) which inhibit implementation of the AML/CFT obligations. Financial institutions are provided with safeguards from liability (including data protection and privacy law) when carrying out AML/CFT obligations: s.24(a) and 30 of the PMLL and s.35(a) of the CTL.

a) *Access to information by competent authorities*: There is a general provision allowing investigators appointed by financial supervisors to require any person to provide all documents (including computer materials and print-outs) and seize a document if the investigator reasonably believes that AML/CFT requirements have been breached. Supervised entities also have a general duty to provide documents upon request to financial supervisors under sectoral-specific orders : s.7, 8A, 8B, 11N(b) of the PMLL, and s.95(a) of the CTL, s.5(a) of the Banking Ordinance, s.18 of Portfolio Managers and Insurers Order, s.20 of Trading Platforms and Stock Exchange Members Orders, s.14 of the MSB Order, s.19 of the Postal Bank Order, and s.17 of the Credit Services Providers Order.

b) *Sharing of information between competent authorities*: Sharing of ML/TF information among the IMPA, law enforcement and intelligence agencies, and financial supervisors is provided for under Israeli law: s.30 and 31(a) of the PMLL. As for information exchange internationally, the legal basis is provided under the PMLL (see s.30(f) of the PMLL and additional analysis under R.40).

c) *Sharing of information between financial institutions*: There are no restrictions in legislation preventing FIs to fulfil their obligations according to R.13 and 16 (R.17 is not applicable).

Weighting and Conclusion

Recommendation 9 is rated compliant.

Recommendation 10 – Customer due diligence

In its last MER, Israel was rated partially compliant for these requirements. There were technical deficiencies in the respective sector orders in relation to CDD obligations and imposition of thresholds, etc.

Criterion 10.1 – Opening of anonymous accounts or accounts in fictitious names is broadly prohibited across the financial sectors.

For the banking sector, this is specifically prohibited (s.51 and 52 of the Banking Directive 411).

For the securities sector, accounts cannot be opened without proper CDD being conducted (s.2(a) of the Stock Exchange Members[43], the Portfolio Managers[44], and the Trading Platforms Orders). There are also specific prohibitions on opening of accounts under aliases or fictitious names (s.2(d) of Stock Exchange Members and Portfolio Managers Orders and s.3.3.11 of the Trading Platform Circular).

Similarly, for insurers and credit service providers, while there are no specific provisions, keeping of such accounts is prohibited through CDD requirements and verification requirements of customers' names and identities (s.3(a) and 4(a)(3) of the Insurers Order[45] and s.3 and 4 of the Credit Service Providers Order).[46]

For the Postal Bank, the opening of numbered accounts is allowed, if approved in writing and in advance by the Supervisor: s.27 of the Postal Bank Directive.[47] However, the Directive does prohibit accounts to be opened in assumed names, and accounts cannot be opened without proper CDD being conducted (s.2(a) of the Postal Bank Order).

Criterion 10.2 – FIs are required to undertake the CDD measures as required under this criterion as follows:

a) when establishing business relations: s.2 and 2A of the Banking Order, s.2-3 of the Stock Exchange Members, Portfolio Managers, Trading Platform, Credit Service Providers and Insurers Orders, s.2 of the Postal Bank Order, s.2 and s.3(a) of the MSB Order;

b) carrying out occasional transactions above the threshold of (USD/EUR 15 000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked: s.2A(a) of the Banking Order, s.3(f) and (g) of the Stock Exchange Members Order, s.3(g) of the Insurers Order, s.3(d) of the Credit Service Providers Order, and s.3(f) to (g) of the Postal Bank Order –subject to a threshold of NIS 10 000 (EUR 2 340) for cash transactions and a lower threshold of NIS 5 000 (EUR 1 168) for non-cash transactions, s.3(a) of the MSB Order;

c) carrying out occasional transactions that are wire transfers in the circumstances covered by R.16 and its Interpretive Note (i.e. a threshold of EUR/USD 1 000): s.2(k) and 2A(a) of the Banking Order, s.3(h)-(k) of the Stock Exchange Members Order, s.3(j) and (k) of the Postal Bank Order, s.3(g) of the Insurers order, s.3(d) of the Credit Service Providers Order, and s.3(b) of the MSB Order. Transactions handled by stock exchange members, the Postal Bank, insurers and MSBs are subject to threshold (NIS 5 000[48] or EUR 1 168). This is slightly higher than the threshold of EUR 1 000 as required by the standards due to the change in the exchange rate since the Orders went into effect (when the threshold was equivalent);

43. Prohibition of Money Laundering (Obligations of Stock Exchange Members to identify, report and retain lists for the purpose of preventing money laundering and financing terrorism), 5770-2010.
44. Prohibition of Money Laundering (Obligations of Portfolio Managers to identify, report and retain lists for the purpose of preventing money laundering and financing terrorism), 5770-2010.
45. Prohibition of Money Laundering (Obligations of Identification, Reporting and Keeping Records of Insurers, Insurance Agents and management Companies to Prevent Money Laundering and Financing Terrorism), 5776-2016.
46. Prohibition of Money Laundering (Obligations of Identification, Reporting and Keeping Records of Credit Service Providers to Prevent Money Laundering and Financing Terrorism), 5777-2017.
47. Prevention of Money Laundering and Terror Financing, and Customer Identification
48. Israel indicates that this amount was equivalent to USD/EUR at the time of enactment.

d) there is suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations: s.12 of the Banking Directive 411; s.5.2 and 5.4 of the Stock Exchange Members Circular; s.2.2 of the Portfolio Managers Circular. Portfolio managers are required to undertake CDD should there be unusual activities (s.5.4 of Stock Exchange Members and Trading Platforms Circulars and s.2.2 of Portfolio Managers Circular). MSBs are only required to take reasonable measures for knowing the customer (rather than full measures to identify, and reasonable measures to verify) where there is a concern of ML/TF (s.6(b)(3) of MSB Circular). There are no requirements for insurers, a small subset of credit service providers, and the Postal Bank;

e) FIs have doubts about the veracity or adequacy of previously obtained customer identification data: s.2(a)(b) of the Banking Order, s.2(c) of the Stock Exchange Members, Portfolio Managers and Trading Platforms Orders, s.9(1) of the Insurers Order, s.2(c) of the Postal Bank Order, s.2(d) of the MSB Order, and s.10(a)(1) of the Credit Service Providers Order.

Required CDD measures for all customers

Criterion 10.3 – FIs are required to identify the customer (whether permanent or occasional, a natural or a legal person) and verify its identity using reliable, independent source documents, data or information, although there is a threshold for triggering the verification requirements regarding the MSB sector (i.e. cash transaction exceeding NIS 10 000 (EUR 2 340), non-cash transactions exceeding NIS 50 000 (EUR 11 680), or transactions exceeding NIS 5 000 (EUR 1 168) involving certain jurisdictions of higher risk, s.3(a) of MSB Order): s.2, 2a and 3 of the Banking Order, s.2(a) and 4 of the Stock Exchange, Portfolio Managers, Trading Platform, Insurers, Postal Bank, Credit Service Providers and MSB Orders : s.3 of the Banking Order, s.2(a) of the Stock Exchange Members, Portfolio Managers, Trading Platform, Insurers, Postal Bank, Credit Service Providers and MSB Orders.

Criterion 10.4 – FIs are required to verify that any person purporting to act on behalf of the customer is so authorised and are also required to verify the identity of that person. s.2(a) and 3 of the Banking Order, s.3(a) and 4 of the Stock Exchange, Portfolio Managers, Trading Platform, Postal Bank and MSB Orders, s.3(a)(1) and 4 of the Insurers Order, and s.3(a) and 4 of the Credit Service Providers Order. These cover for example authorised signatories to accounts, proxies and service applicants, which are defined as a person requesting a financial service, whether for himself or for another.

Criterion 10.5 – FIs (with the exception of MSBs) are required to record information on the beneficial owner before opening an account, and take reasonable steps to verify the identity of the beneficial owner (in a risk-based manner), using the relevant information or data obtained from a reliable source, such that the covered FI is satisfied that it knows who the beneficial owner is. "Beneficial owner" is defined in the PMLL (s.7(a)(1)) as "a person for whom or for whose benefit the property is being held, the transaction is being undertaken, or who has the ability to direct the disposition, and all whether directly or indirectly. "Person" can be a natural or legal person. For legal persons, FIs must then also identify and verify the controlling person. (See criterion 10.10 below). In the event that there is no legal person involved, case law demonstrates that the FI must identify the ultimate natural person who is the beneficial owner as defined above. There are no similar requirements for the MSB sector, although the service recipient must declare if he or she is acting on behalf of someone else. See s.2(b) and 4 of the Banking Order, s.3(b) and 5 of the Stock Exchange Members, Portfolio Managers, Trading Platform, Insurers, Credit Service Providers, Postal Bank Order, and s.5 and the fourth addendum to the MSBs Order.

Criterion 10.6 – CDD obligations in the respective sectoral orders duly encompass the obligation to understand and obtain information on the purpose and intended nature of the business relationship:

s.2a.(a) of the Banking Order, s.2(a) of the Stock Exchange Members, Portfolio Managers, Trading Platform, Insurers, Postal Bank, Credit Service Providers, and MSB Orders.

Criterion 10.7 –

FIs are required to scrutinise transactions regularly to ensure that the transactions being conducted are consistent with the FI's knowledge of the customer, their business and risk profile, and consistency of transactions with the source of funds.

FIs are also required to conduct ongoing due diligence on the business relationship to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records. Such reviews are required based on the individual customer's ML/TF risks. (S.2a.(b) of the Banking Order and s.31-34 and 82 of the Banking Directive 411, s.2(c) and s.11 of the Stock Exchange Members Order, s.2(c) and s.9 of the Portfolio Managers Order, s.2(c) and s.9 and 11 of the Trading Platforms Order, s.6(c) of the MSB Circular, s.2(c) of s.10 of the Postal Bank Order and s.24 of the Postal Bank Directive, and s.9 of the Insurers Order and s.2(b)(6)(c) of the Insurers Circular.)

Specific CDD measures required for legal persons and legal arrangements

Criterion 10.8 – All FIs are required to understand the nature of all customers' business and their ownership and control structure, although the provisions do not specifically distinguish between legal persons and arrangements: s.2(c), (d) and (e) of the Banking Order and s.29(f) of the Banking Directive 411, s.3(c) and (d) of the Stock Exchange Members, Portfolio Managers, Trading Platform and Postal Bank Orders, s.3(c) of the Credit Service Providers Order, s.3(c)(2) of the Insurers Order and s.2(h) of appendix 1 of the Insurers Circular, s.2(a) and s.4(a)(4) of the MSB Order, and s.3 of Appendix 1 to the MSB Circular. Trust and endowment are separately required under the PMLL to understand the identification details (s.7(1)).

Criterion 10.9 –

a) All FIs are required to identify and verify the customer's identity through name, legal form, proof of existence and address of the registered office and, if different, a principal place of business. Similar to c.10.8, the provisions do not specifically distinguish between legal persons and arrangements; trusts and endowment are separately required under the PMLL to understand the identification details. Sectoral orders of insurers, stock exchange members, trading platforms and portfolio managers provide additional specific requirements for public institutions and of a corporation established by legislation overseas. (S.7 of the PMLL, s.2(a), 3.(a)(3), (4), (5), (6) of the Banking Order; s.3(a) and s.4(a)(3), (4) and (6) of the Stock Exchange Members, Portfolio Managers, and Trading Platforms Orders; s.3(a), s.4(a)(3), (4) and (6) of the Postal Bank Order; s.3(a), s.4(a)(3) and (4) of the Insurers Order; s.3(a), s.4(a)(3), (4),(5) and (6) of the Credit Service Providers Order; s.3(a) and s.4(a)(3) of the MSB Order).

b) Banks, stock exchange members, portfolio managers, MSBs, credit service providers and insurers are required to identify the names of the relevant persons having a senior management position in the legal person or arrangement, but there are no requirements for trading platforms and the Postal Bank: s.29(f) of Banking Directive 411, s.3(c) of the Stock Exchange and Portfolio Managers Orders (s.2(h) of Appendix1 of the Insurers Circular), s.3 of Appendix 1 of the MSB Circular, and s.3(c) of the Credit Service Providers Order. In addition, banks and the Postal Bank must be provided with the powers that regulate and bind the legal person or arrangement: s.3(a)(3)(b) of the Banking Order and s.4(a)(3)(b) of the Postal Bank Order. But a similar requirement is not in place for the other sectors (i.e. insurance, securities, credit service providers, MSBs).

c) As far as legal persons are concerned, FIs are required to identify and verify the address of the registered office and, if different, a principal place of business. Banks and the Postal Bank are specifically required to seek for this information in relation to corporations: s.2(a) and s.3(a)(3), s.3(a)(4) of the Banking Order, s.3(a), s.4(a)(3), s.4(a)(4) of the Stock Exchange Members, Portfolio Managers, Trading Platforms, Credit Service Providers, MSB, Insurers, and Postal Bank Orders. There are not similar specific requirements for legal arrangements.

Criterion 10.10 – For customers that are legal persons, as mentioned under c.10.5, FIs are required to identify and take reasonable measures to verify the identity of the beneficiary and the "controlling person". This is defined as an individual who has the power to direct the activities of the legal person, alone or with others or through others, directly or indirectly. It also includes an individual who holds 25% of any controlling measures. If such an individual cannot be identified, the controlling person to be identified would be the chairman of the board of director or other equivalent senior officer and managing director: s.2, 4(b), 4(e) of the Banking Order; s.5 of the Stock Exchange Members, Portfolio Managers and Trading Platforms Orders; s.5 of the Postal Bank Order; s.4(c) and 5 of the Insurers Order; s.5 of the MSB Order; s.4(c) and 5 of the Credit Service Providers Order.

Criterion 10.11 – For customers that are trusts or other types of legal arrangements, banks, the Postal Bank, insurers, MSBs are required to take reasonable measures to identify the identity of beneficial owners. The identification information required includes the identity of the settlor, the trustee, the protector, the beneficiaries, but not any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership). However, only banks are required to verify the protector's identity (s.54 of the Banking Directive 411) and there are no similar requirements for other FIs. (Stock exchange members, portfolio managers, trading platforms, and MSBs: s.53-56 of the Banking Directive 411; s.2(M) of the First Appendix of Insurance Circular; s.28 of Postal Bank Directive, s.4 of Appendix A of the MSB Risk Management Circular).

CDD for Beneficiaries of Life Insurance Policies

Israeli laws only allow licensed insurers not engaging in any other financial sectors to issue life insurance and other investment related insurance policies (s.14 and 15 of the Control of Financial Services (Insurance) Law, 5741-1981).

Criterion 10.12 – Insurers are required to conduct CDD and verification measures for every transaction (including at time of payout) on the beneficiary of life insurance that is identified as specifically named natural persons or corporations, and for a beneficiary that is designated by characteristics. (S.2, 3(a), 3(c)-(f), and 4 of Insurers Order.)

Criterion 10.13 – Insurers are required to take ML/TF risks into account when conducting CDD measures and the beneficiary of a life insurance policy has been specified as a relevant risk factor in determining whether enhanced CDD measures are applicable. If an insurer determines that a beneficiary is a corporation, relevant EDD measures at the time of pay-out is also required (s.2(B)(6)(b)(1)(d) and s.3 of Appendix A of the Insurers Circular).

Timing of Verification

Criterion 10.14 – All FIs apart from MSBs and insurers are required to verify the identity of the customer and beneficial owner before establishing a business relationship or conducting transactions for occasional customers: s.3 of the Banking and the Postal Bank Order, and s.4 of the Stock Exchange Members, Portfolio Managers, Trading Platform and Credit Service Providers Orders. For MSBs, verification requirements are in relation to customers and not to beneficial owners: s.3 and s.4 of the MSB Order. Delayed verification is allowed for insurers in certain situations, including

entering into a contract or opening the account (verifications within 30 days), but not at the time of payout: s.4 of Insurers Order.

Criterion 10.15 – Israeli laws do not allow opening of accounts or commencing business relations prior to verification of identification documents, and do not provide for risk-based delay identity verification situations. This criterion is therefore not applicable.

Existing Customers

Criterion 10.16 – FIs are required to apply CDD requirements to existing customers on an on-going basis, and subject to ML/TF risks. The sectoral orders require CDD be conducted on all customers that were customers of the financial institution before the relevant orders came into effect, and provide a transitional period for doing so (e.g. 18 months or 2 years). (s.17 of the Banking Order; s.24 of the Stock Exchange Members Order, s.21 of Portfolio Managers and Trading Platforms Orders; s.22 of Postal Bank Order; s.23 of Insurers Order and s.19 of the Credit Service Providers Order).

Risk-based Approach

Criterion 10.17 – FIs have requirements to apply EDD with regard to higher-risk situations (s.30 of the Banking Directive 411; s.26(c) of the Postal Bank Directive; s.9.1 Stock Exchange Members Risk Management and Trading Platforms Circulars, and s.3.1 of the Licensed Portfolio Managers Circular). The Directives and Circulars provide examples of EDD measures that should be taken, including acquiring additional information on the customer, verifying the source of wealth and source of funds, and obtaining senior management approval. They also set out a list of risk factors to take into account when establishing CDD measures and enhanced due diligence measures to be undertaken for identified high risk activities. Stock exchange members, portfolio managers and insurers must perform enhanced CDD in relation to a list of specific high classes of customers (e.g. trusts and NPOs) (s.4 and 7 of Stock Exchange Members Risk Management Circular, paragraphs 1 and 3 of the Portfolio Managers Circular, and s.2(b)(5), 2(b)(6)(a), s.2(b)(6)(b) of the Insurers Circular), and s.5, 6(a) and 6(b) of the MSB Circular.

Criterion 10.18 – Most sectoral orders provide for exemptions from certain CDD requirements (e.g. declaration of the beneficial owner) for certain categories. These categories include an account of a public institution, an account of a banking corporation, insurer or a stock exchange member, an account on behalf of a registered public charity, an account managed for communal purposes, or an attorney account on behalf of clients below a certain threshold. This list of categories, although it can be generally interpreted as having lower risks, is not backed by an adequate analysis by the country or the FI. There are also no specific provisions stating that the simplified measures are not acceptable whenever there is a suspicion of ML/TF, or when specific higher risk scenarios apply – with the exception of credit service provider and MSBs in case of ML/TF suspicion. (s.5 to 7 of the Banking Order; s.6(a) of the Stock Exchange Members, Portfolio Managers, and Trading Platforms Orders; s.6(a) of the Postal Bank Order; s.7 and 8 of the Insurers Order; s.4(d) of the MSB Order; s.7-8 of the Credit Service Providers Order.)

Failure to satisfactorily complete CDD

Criterion 10.19 – FIs are not allowed to open an account, commence business relations or perform a transaction if CDD measures cannot be completed: banking sector: s.2, 2a and 3 of the Banking Order; securities, postal bank, insurance, credit service provider and MSB sectors: s.2-4 of the Stock Exchange Members, Portfolio Managers, Trading Platform, Credit Service Providers, Postal Bank, Insurers and MSB Orders. Similar CDD deficiencies identified under c.10.3 to 10.7 exist for MSB sector. The respective orders do not contain a specific provision requiring FIs to consider filing a UAR

if CDD measures cannot be satisfactorily completed, but do list out certain CDD-related indicators which an FI must consider filing a UAR.

Criterion 10.20 – Save for banks and the Postal Bank, all FIs are allowed not to pursue the CDD process if they form a suspicion of ML/TF and reasonably believe that performing the CDD process will tip-off the customer. They must also report to IMPA (s.6(a)(3) of the MSBs Circular, s.2(b)(6)(a)(5) of the Insurers Circular, s.5.8 of the Trading Platforms Circular, s.8(b) of the Portfolio Managers Order, s.10(b) of the Stock Exchange Members Order).

Weighting and Conclusion

Israel meets or mostly meets the most important criteria for Recommendation 10, including when CDD is required, required CDD measures, beneficial ownership, ongoing due diligence and enhanced due diligence. However, there are some minor deficiencies: there is no general beneficial ownership requirement for MSBs, FIs other than banks are not required to verify beneficial ownership information for trusts; no specific provisions permitting banks and the Postal Bank not to pursue the CDD process; and simplified due diligence are not based on adequate risk analysis. **Recommendation 10 is rated largely compliant.**

Recommendation 11 – Record-keeping

Israel was rated partially compliant for these requirements in the last MER. The deficiencies were: presence of thresholds for retaining of documents; absence of requirement to keep all documents recording the details of all transactions carried out by the client in the course of an established business relationship; absence of general requirement in Law or Regulation to retain documents for more than five years if requested by a competent authority; decree on post bank not in law or regulation.

Criterion 11.1 – FIs are required to keep all necessary records on transactions, although MSBs are subject to thresholds (e.g. for transactions exceeding NIS 10 000 (EUR 2 340). For the banking, postal bank, and insurance sectors, this applies for seven years from the date the transaction was recorded: s.14(a1) and (b) of the Banking Order, s.11 of the Postal Bank Directive and s.17 (b) to (e) of the Insurers Order. For the securities sector, the requirement applies for five years from the date of transaction: s.19(b) and (c) of the Stock Exchange Members Order, s.17(b) and (c) of the Portfolio Managers Order, and s.19(b) and (c) of the Trading Platforms Order. For the MSB sector, the requirement applies for seven years from the day of transaction subject to a threshold: s.13(c) of the MSB Order. For non-bank credit service providers, this applies from the date the transaction was recorded to five years after the conclusion of the transaction: s.16(b) and (c) of Credit Service Providers Order.

Criterion 11.2 – FIs are required to keep all records obtained through CDD measures and other information required in the orders for the same period specified under c.11.1 for the various sectors, as well as account files and business correspondence for most FIs: banking sector: s.14(a) of the Banking Order and s.35(c) of the Banking Directive 411; insurance sector: s.17(b) of the Insurers Order; securities sector: s.10 (a) and (b) of the Stock Exchange Members Order, s.17(a) and (b) of the Portfolio Managers Order, and s.9 and 19(a) of the Trading Platforms Order; non-bank lending sector: s.16(b) of the Credit Service Providers Order; the postal bank: s.9 and 18(a) of the Postal Bank Order and s.19(a) of the Postal Bank Directive; MSB sector: s.13 (a) and (b) of the MSB Order. However, the Trading Platforms Order does not cover business correspondence.

Criterion 11.3 – The obligation for FIs to keep transaction records that should be sufficient to permit reconstruction of individual transactions is provided for some FIs, namely banks (s.35 of the Banking

Directive 411), stock exchange members and portfolio managers (s.19(b) of the Stock Exchange Members Order and s.17(b) of the Portfolio Managers Order), insurers (s.2(b)(6)(d)(1)(b) of the Insurers Circular), and MSBs (s.6(d)(1)(b) of the MSB Circular). However, this requirement does not apply to trading platforms, a small part of the credit service providers sector, and the Postal Bank. Israel also relies on general requirements under the Evidence Regulation (Photocopies) (s.3A) and provisions mentioned under c.11.1 for this purpose.

Criterion 11.4 – FIs are required to keep all CDD information on a computer database that can be easily accessed, though the need to retain such information electronically is not required for smaller MSBs (i.e. annual turnover below NIS 3 million (EUR 701 000). FIs are also required to provide all documents (including CDD and transaction records) to domestic competent authorities upon appropriate authority. (S.11N(b)(1) of the PMLL, also s.13 and 14 of the MSB Order and s.4(b) of the third schedule, s.17 and 18 of the Insurers Order, s.16 of Credit Services Providers Order, s.2(b)(7)d(1)(a)), s.20 of the Stock Exchange Members and Trading Platforms Orders, s.18 of the Portfolio Managers Order, s.19 of the Postal Bank Order, and s.6(d)(1) of MSB Circular.)

Weighting and Conclusion

Israel mostly meets all the criteria for Recommendation 11. However, there are a few minor deficiencies: there is a threshold for record-keeping requirements for the MSB sector, trading platforms are not required to maintain business correspondence, and there is a lack of a specific requirement for trading platforms, part of the credit service providers sector, and the Postal Bank to ensure that records are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Recommendation 11 is rated largely compliant.

Recommendation 12 – Politically exposed persons

In its last MER, Israel was rated partially compliant for these requirements. The main technical deficiencies were: definition of PEPs only applicable to banks; the definition of PEPs did not cover family members and close associates of PEPs; absence of the requirement to seek senior management approval where a customer is subsequently found out to be a PEP or becomes a PEP; establishing business relationships with PEPs by banks not fully covered (limited to account opening), no senior management approval for establishing business relationships with PEPs only partly covered in respect of banks.

Criterion 12.1 –

(a) & (b) Most FIs are required to determine whether a customer or the beneficial owner is a foreign PEP. The need to put in place a risk management system for such decision, obtain senior management approval before establishing business relationships, and conduct enhanced ongoing monitoring on that relationship However credit service providers are only required to obtain such approval from any officer in the compliance department (i.e. not necessarily of senior management level), and the definition of PEP under the Postal Bank Order does not cover senior executives of state-owned corporations.

(c) Banks and the Postal Bank are required to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs. The Securities and insurance sectors, as well as MSBs and credit service providers, are required to do so as part of the CDD process for all customers. For the MSB sector, CDD deficiencies identified under R.10 (e.g.

CDD verification is triggered only either by a threshold or when the transactions are repeated ones) are also relevant (s.2(b) of the MSB Order).

(Legal references for c.12 (a) to (c) - Banks: s.2a.(a) of the Banking Order and s.58, 60 and 61 of the Banking Directive 411; Securities sector: s.1, 2(a), 2(b), 11 and 18 of the Stock Exchange Members and Trading Platforms Orders, and s.2(b), 9 and 16 of the Portfolio Managers Order; MSBs: s.2(a) of the MSB Order; Credit Service Providers: s.2(b), 10(a)(2)(b) and 15 of the Credit Service Providers Order; Insurers: s.2(b), 9(4) and 16 of the Insurers Order; Postal Bank: s.2(b), 10 and 17 of the Postal Bank Order and s.6(a)(6)(g) of the Postal Bank Directive).

(d) FIs are required to conduct enhanced on-going monitoring of PEP relationships (s.10 and 30 of Banking Directive 411; s.10 of the Postal Bank Order; s.11 of the Stock Exchange Members and Trading Platforms Orders; s.9 of the Portfolio Managers Order; s.9(4) of the Insurers Order; s.10(a)(2)(b); s.4(c)(1) of Third Schedule to MSB Order and s.6(b)(1)(2) and 6(c)(3) of the MSB Risk Circular).

Criterion 12.2 –

(a) Most FIs (banks, the Postal Bank, stock exchange members, MSBs, part of the credit service providers sector) are required to take reasonable measures to determine whether a customer or the beneficial owner is a domestic PEPs or person who has been entrusted with a prominent function by an international organisation.; There are not similar domestic PEP obligations for portfolio managers, trading platforms, and part of the credit service providers sector as the PEP definition does not cover domestic PEPs as defined by the FATF.

(b) In cases where there is higher-risk business relationship with such a person, most FIs (banks, stock exchange members, the Postal Bank and insurers) are required to obtain senior management approval, take reasonable measures to establish source of wealth/funds, and conduct enhanced on-going due diligence. As mentioned, there are not domestic PEP obligations for certain FIs. However, credit service providers are required to clarify the source of financial services in respect of PEP classified by the entity as high risk.

(S.1 and 2a.(a) of the Banking Order and s.61(b) of the Banking Directive 411; s.1, 2(b), 11(2) and 11(3) of the Stock Exchange Members Order and s.8.3.2.9 of the Stock Exchange Members Circular, s.1, 2(b), 9(2) of the Portfolio Managers Order, s.1, 2(b) and 11(3) of the Trading Platforms Order and s.8.3.2.9 of the Trading Platform Circular; s.1, 2(b) and 9(4) of the Insurers Order and s.2(b)(76)(b) and 2(b)(6)(a)(4).7(b) of the Insurers Circular; s.2(b) and 10(a)(2)(b) of Credit Service Providers Order; s.1 and 2(b) of the Postal Bank Order and s.29 of the Postal Bank Directive; s.2(b) of MSB Order and s.6(b) and s.6(a)(2) of the MSB Circular).

Criterion 12.3 – The requirements for family members and close associates are met for the FIs: s.58-63 of the Banking Directive 411, s.29(f) of Postal Bank Directive, s.1 of the Stock Exchange Members, Portfolio Managers, Trading Platform, Credit Service Providers, Insurers and MSB Orders. Again for MSBs, CDD deficiencies identified under R.10 (e.g. CDD verification is triggered only either by a threshold or when the transactions are repeated ones) are relevant.

Criterion 12.4 – For life insurance policies, insurers are required to take reasonable measures to determine whether the beneficiaries are PEPs at the time of establishing business relationship, but not at the time of the payout: s.(b) of Insurers Order.

Weighting and Conclusion

Israel mostly meets three of the four criteria for Recommendation 12. There are however some deficiencies: the definition of PEP for the Postal Bank does not cover senior executives of state-owned

corporations. Portfolio managers, trading platforms, and part of the credit service providers sector do not have domestic PEP requirements. And CDD deficiencies identified under R.10 (e.g. CDD verification is triggered only either by a threshold or when the transactions are repeated ones) also have implications on the CDD measures in relation to PEPs.

Recommendation 12 is rated largely compliant.

Recommendation 13 – Correspondent banking

Israel was rated largely compliant for these requirements in the last MER, mainly due to an absence of requirement for obtaining approval from senior management for new correspondent relationships.

Criterion 13.1 – Cross-border correspondent banking and other similar relationships are allowed for banks, stock exchange members, and the Postal Bank, but not other FIs.

a) Banks, stock exchange members, and the Postal Bank are required to gather information about a respondent institution including name of the corporation, parent company, country of incorporation and AML/CFT supervisory authority, a copy of latest annual statement or summary published in a public database, as well as a letter of reference from an OECD-country bank if the respondent institution is incorporated outside of the OECD. Stock exchange members and the postal bank are additionally required to obtain a declaration of conducting CDD measures for AML/CFT purposes from the respondent institution, but there are no such similar requirements for banks. Requirements for FIs to determine from publicly available information on the reputation of the institution and quality of supervision, including whether the respondent institution is subject to ML/TF investigation or regulatory action, are provided for under respective sectoral directives/circulars. S.5(a) of the Banking Order and s.64-66 of the Banking Directive 411, s.7 of the Stock Exchange Members Order and s.12.5 of the Stock Exchange Members Circular, and s.7 of the Postal Bank Order and s.25 of the Postal Bank Directive.

b) The obligations regarding the assessment of the respondent institution's AML/CFT controls are provided for banks, stock exchange members, and the Postal Bank. (S.65(c) of Banking Directive 411, s.12.5.3 of the Risk Management Circular for Stock Exchange Members, s.25(a) of Postal Bank Directive and s.7(3)(c)(2) of Postal Bank Order).

c) Banks, stock exchange members, and the postal bank are required to obtain approval from senior management before establishing new correspondent relationships: s.67(c) of the Banking Directive 411, s.7(4) of the Stock Exchange Members and Postal Bank Orders.

d) Banks, stock exchange members, and the Postal Bank are required to clearly understand the respective AML/CFT responsibilities of each institution: s.67(a) and 68 of the Banking Directive 411, s.12.3 and s.12.5.3 of the AML/CFT Risk Management Circular for Stock Exchange Members, and s.25(a) and (c) of the Postal Bank Directive.

Criterion 13.2 – With respect to "payable-through accounts", banks and stock exchange members are required to satisfy themselves that the respondent bank has performed CDD obligations on its customers that have direct access to the accounts of the correspondent banks; and is able to provide relevant CDD information upon request to the correspondent bank. There are no relevant enforceable requirements for the Postal Bank, as local branches do not perform such activity. S.65(f) and 70 of the Banking Directive 411 and s.12.6.5 of the Risk Management Circular for Stock Exchange Members.

Criterion 13.3 – Banks, stock exchange members, and the Postal Bank are prohibited from entering into, or continuing correspondent banking relationships with shell banks. S.67(b) of the Banking Directive 411, and s.7(5) of Stock Exchange Members and Postal Bank Order.

Weighting and Conclusion

Recommendation 13 is rated compliant.

Recommendation 14 – Money or value transfer services

In its last MER, Israel was rated partially compliant for these requirements because of deficiencies linked to CDD measures also impact on the money or value transfer sector.

Criterion 14.1 – Natural and legal persons providing non-bank money or value transfer services in Israel are required to be registered with the Registrar of Money Service Business appointed by the Minister of Finance. Licensed financial institutions (e.g. banks, stock exchange members) providing MVTS are not required to be separately registered with the Registrar, and Israel relies on sectoral AML/CFT orders to regulate their activities: s.11C of the PMLL, see also R.26. Considerations which the Registrar should take into account prior to the issue of the registration certificate are provided in the legislation (e.g. absence of criminal record): s.11E(4) of the PMLL. Mechanism for renewing the registration certificate is also provided in the law (i.e. valid until the end of the calendar year in which it was given): s.11G(a) of the PMLL. Written notification of any updated information regarding the registration should be made to the Registrar within seven days from the date of change: s.11F of the PMLL and s.5A(a)(3) and 88J of the Postal Law.

Criterion 14.2 – Israel has taken action, with a view to identifying natural or legal persons that carry out MVTS without a registration. Indictments have been filed against MSBs operating without a registration, and this is also one of the responsibilities of the new MSBs task force in the INP. The Registrar is provided with powers to investigate, request information, and seize documents: Chapter 4B of the PMLL. Operating money or value transfer services without registration, providing false registration information, and failure to provide updated information regarding a registration are subject to a criminal offence of up to one year imprisonment and/or a fine (both criminal and administrative): s.3(b), s.11L, and s.14(a) of the PMLL.

Criterion 14.3 – The Registrar of Money Service Business has the responsibility for monitoring AML/CFT compliance: s.11M of the PMLL and s.95(d) of the CTL.

Criterion 14.4 and Criterion 14.5 –The AML/CFT regulatory system regarding MVTS do not distinguish between the providers and agents. Israel relies on legal provisions stated in c.14.1-c.14.3 above in relation to registration and supervision for monitoring for compliance. These criteria are therefore not applicable.

Weighting and Conclusion

Recommendation 14 is rated compliant.

Recommendation 15 – New technologies

Israel was rated largely compliant for these requirements in its previous MER, mainly due to limited measures in the non-bank sectors. The new R.15 focuses on assessing risks related to the use of new technologies, in general, and no longer specifically targets distance contracts.

Criterion 15.1 – At the country level, Israel has assessed the risks posed by internet activities and digital currencies to the banking system, and in relation to the development of new products and new business practices such as debit cards, revovling credit cards, pre-paid cards, electronic wallets, online payments and cellular checks.: P.9 of ML NRA (Financial System) and Final Report: The Committee for the Promotion of the Use of Advanced Means of Payment in Israel June 2017.

At the institution level, banks are required to conduct ML/TF risk assessments for the use of new technologies, products or services, though the relevant provision does not specify the assessments are required for both new and pre-existing products or new delivery mechanisms: s.10(h) of the Banking Directive 411. Stock exchange members are required to define policy to monitor ML/TF threats, and assess risks before introducing any new or emerging product, practice or technology into use: s.3.3.7 of Stock Exchange Member Circular. Insurers, MSBs, portfolio managers, trading platforms, credit service providers, and the Postal Bank are required generally to identify ML/TF threats for the use of new technologies (e.g. non face-to-face and electronic transactions). Israel relies on general requirements in sectoral orders to require supervised entities to conduct risk assessments in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing prodcuts: s.12(2) of the MSB Order, s.18 of the Stock Exchange Members Order, s.18 of the Trading Platforms Order, s.15 of the Portfolio Managers Order, s.15(2) of the Credit Service Providers Order, and s.17(2) of the Postal Bank Order (see also s.6(a.3) of the Postal Bank Directive, s.5(d) of MSB Circular, s.2(b)(65)(d) of Insurers Circular). Nevertheless, BoI, CMISA, ITA, ISA, and IMPA have issued a non-enforceable joint press release / notice stating that FIs must take the use of virtual currencies into account within the framework of their AML/CFT risk management policy. (Para. 2, Notice to the public regarding possible risks in decentralised virtual currencies (such as Bitcoin)).

Criterion 15.2 – There is a general requirement for banks, stock exchange members, portfolio managers, trading platforms, insurers, and the postal bank to conduct risk assessments prior to the launch of new products and new delivery channels, and to review the risk policy document at least once a year. (See directives: s.15 and 16 of the Proper Conduct of Banking Business Directive 310, s.5(d) of MSB Circular, and s.16 of Postal Bank Directive.

Weighting and Conclusion

Recommendation 15 is rated compliant.

Recommendation 16 – Wire transfers

Israel was rated partially compliant for these requirements in its last MER as it did not require full originator information for cross-border wire transfers for the postal bank and other non-bank FIs.

Ordering financial institutions

Criterion 16.1 – For cross-border transfers, banks are required to include, in all SWIFT transfers (regardless of threshold), originator information including, the name, account number (or identification number, if no account), and address, and to the extent possible the name of the initiator of the transfer. As for cross-border wire transfers handled by all other FIs the, a threshold of NIS 5 000 or more (EUR 1 168), as of the time of the on-site visit, instead of EUR 1 000 or more as specified under this criterion) is applied. In these cases, they must include originator information (including name, account number (or identification number), and address) in the transfer documents. MSBs are not required to record the account number (or a unique transaction reference number) (c.16.1(a)(ii)) and therefore include it in cross-border transfers. There are also no specific provisions requiring the verification of originator information, though stock exchange members need

to do so when transactions are considered having high ML/TF risks. Portfolio managers are not allowed to conduct electronic transfers of money or assets under the law (s.20D(B) of the Advice Law and s.44P of the Securities Law).

As for beneficiary information, save for MSBs, all FIs are required to record the name and account number of the beneficiary and include it in the transfer document. MSBs are only required to record the name, address and identification number of the beneficiary if known. (S.2(k) of the Banking Order, s.3(h), (i) and (i1) of the Stock Exchange Members Order, s.3(f) and (g) of the Trading Platforms Order, s.3(j) and (k) of the Postal Bank Order, s.3(d) of Credit Service Providers Order, s.3(b) and (c) of the MSB Order, and s.3(g)(2) of the Insurers Order.)

Criterion 16.2 – There are no specific provisions covering the scenario where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries. However, with the exception of the insurers, all other FIs (i.e. banks, stock exchange members, trading platforms, credit service providers, the Postal Bank, and MSBs are required to record the originator and beneficiary information mentioned under c.16.1 above in "each transfer document" (which could be batch transfer). (S.2(k) of the Banking Order, s.3(h), (i) and (i1) of the Stock Exchange Members Order, s.3(f) and (g) of the Trading Platforms Order, s.3(d) of the Credit Service Providers Order, s.3(j) and (k) of the Postal Bank Order, and s.3(b) and (c) of the MSB Order).

Criterion 16.3 – As noted in c.16.1, financial institutions other than banks apply a *de minimis* threshold. For cross-border transfers below this amount, they are not required to include any originator or beneficiary information.

Criterion 16.4 – There are no separate provisions requiring all FIs to verify the information pertaining to the customer where there is a suspicion of ML/TF in relation to cross-border wire transfers below any applicable *de minimis* threshold. (see also c.10.2 and c.10.3). Israel relies on general CDD-related provisions for the purposes of c.16.4.

Criterion 16.5 – On domestic wire transfers, Israel requires banks to apply the same requirements as for cross-border transfers. Stock exchange members, credit service providers and insurers are required to record originator information including name, identification number and address (and for stock exchange members, account number or transaction reference number). But only credit service providers are required to include this in the transfer document. The Postal Bank is required to record the particulars of the originator, but the Directive does not specify in detail the specific identification information. There are so similar requirements for MSBs and trading platforms. (S.48(a) of Banking Directive 411, s.3(k) of the Stock Exchange Members Order, s.31(c) of the Postal Bank Directive, s.3(d), 12(2)(d) of the Credit Service Providers Order, and s.3(g)(1) and s.3(g)(2) of the Insurers Order.)

Criterion 16.6 – Again, there are no separate provisions requiring all FIs to make information available within three business days for receiving request from appropriate competent authorities, or empowering law enforcement authorities to compel immediate production of such information. Israel relies on the general powers regarding record keeping and providing information to LEAs for the purposes of c.16.6. (see also R.11).

Criterion 16.7 – FIs are required to maintain identification and transaction information (including originator and beneficiary information collected) in accordance with R.11. (S.14(a), (a1) and (b) of the Banking Order, s.19(a) and (b) of the Stock Exchange Members and Trading Platforms Orders, s.16(a) and (b) of Credit Service Providers Order, s.17(a) and (b) of Insurers Order, and s.88G1 of the Postal Law.) There are no similar specific requirements for MSBs, and Israel relies on general CDD-related provisions for the purpose of this criterion: s.2 and 13(b) of the MSB Order.

Criterion 16.8 – The ordering FIs are not allowed to execute the wire transfer if the transfer does not comply with the requirements set out in c.16.1-16.7. (S.2(k) of the Banking Order and s.48(a) of Banking Directive 411, s.3(h), (i), (i1) and (k), and 19(a) and (b) of the Stock Exchange Members Order, s.3(f) and (g) of the Trading Platforms Order, s.3(d) of the Credit Service Providers Order, s.3(j) and (k) of the Postal Bank Order, s.31(c) of the Postal Bank Directive and s.88G1 of the Postal Law, s.3(b) and (c) of the MSB Order, and s.3(g)(1) and (2) of the Insurers Order.)

Intermediary financial institutions

Criterion 16.9 – As far as banks, the Postal Bank and stock exchange members are concerned, intermediary FIs are required to ensure all originator and beneficiary information received and accompanying a wire transfer is kept with the transfer. Deficiencies identified under c.16.1 are also relevant. There are no specific provisions for MSBs, credit service providers, insurers, and trading platforms. (S.2(l) of the Banking Order, s.3(l) of the Postal Bank Order and s.3(j) of the Stock Exchange Members Order.)

Criterion 16.10 – While relevant sectoral orders have not covered the specific situations where intermediary FIs use a payment system with technical limitations, ISA does require stock exchange members to retain records of all transactions (including originator and beneficiary information) for five years: s.19(b) of the Stock Exchange Members Order. As explained above, there are no specific provisions specifying these requirements in all other FIs (i.e. banks, the Postal Bank, trading platforms, credit service providers, MSBs and insurers), and Israel relies on general record keeping provisions for the purpose of c.16.10 (see also R.11).

Criterion 16.11 – Banks acting as intermediary FIs are required to take reasonable measures to identify cross-border wire transfers that lack required originator or beneficiary information: s.2(l) of the Banking Order. As for stock exchange members, there is a general provision requiring them (without specifying their roles as intermediary FIs or not) to determine policy and tools to address wire transfers that are not accompanied by complete originator information, but not beneficiary information: s.18(3) of the Stock Exchange Members Order. Similar requirements for the Postal Bank are set out in s.31(b) of the Postal Bank Directive. There are no similar requirements for trading platforms, credit service providers, MSBs and insurers.

Criterion 16.12 – For banks and the Postal Bank, there is a general obligation for them (without specifying their role as intermediary FIs) to adopt risk-based procedures when handling transfers: s.47 of the Banking Directive 411 and s.31 of the Postal Bank Directive. As for securities sector, Israel requires stock exchange members (without specifying their role as intermediary FIs) to take ML/TF risks into account when conducting wire transfers not accompanying with complete originator information: s.18(3) of the Stock Exchange Members Order. There are no similar requirements for all other FIs (i.e. trading platforms, credit service providers, MSBs and insurers).

Beneficiary financial institutions

Criterion 16.13 – For banks, BoI relies on the broad general obligation under s.47 of the Banking Directive 411 mentioned under c.16.12 for this criterion. For securities sector, there is a general provision requiring stock exchange members (without specifying their role as beneficiary FIs) to determine policy and tools to address wire transfer that are not accompanied by complete originator information, but not on beneficiary information: s.18(3) of the Stock Exchange Members Order. As for other sectors, as explained above, Israel relies on general CDD provisions for the purpose of c.16.13 and there are no separate specific requirements for these FIs (i.e. the Postal Bank, trading platforms, credit service providers, insurers, and MSBs).

Criterion 16.14 – MSBs are required to verify the identity of beneficiary and maintain the information only when the cross-border wire transfer amounts exceeds NIS 50 000 (around EUR 11 680), or when the transfer exceeds NIS 5 000 (EUR 1 168) involving a high risk jurisdiction. There is no specific provision for all other FIs (i.e. banks, the Postal Bank, stock exchange members, trading platforms, credit service providers and insurers) requiring and verifying the identity of beneficiary information for cross-border wire transfers exceeding EUR/USD 1 000 or more. Israel relies on general CDD and record keeping provisions for the purposes of c.16.14.

Criterion 16.15 – For banks, there is a general obligation for FIs (without specifying the role as beneficiary FIs) to adopt risk-based procedures when handling transfers: s.47 of the Banking Directive 411. For the Postal Bank, there is also a general requirement to adopt risk-based procedures for handling transfers in which not all of the identification details of the originator: s.31(b) of the Postal Bank Directive. As for securities sector, stock exchange members (without specifying the role as beneficiary FIs) are required to take ML/TF risks into account when conducting wire transfers not accompanying with complete originator information: s.18(3) of the Stock Exchange Members Order. For insurers and MSBs, regulators rely on the broad provision to require FIs (without specifying the role as beneficiary FIs) to develop AML/CFT policies, tools and risk management for the purposes of fulfilling the obligations with respect to identification, reporting and keeping of records. There are no similar requirements for credit service providers and insurers.

Money or value transfer service operators

Criterion 16.16 – Israel requires MVTS operators to be registered as MSBs and deficiencies identified in the MSB sector under this Recommendation are relevant (s.11C(a)(3) of the PMLL).

Criterion 16.17 – There are no specific requirements in the MSB Order on this criterion and deficiencies identified above in MSB sector are also relevant.

Implementation of targeted financial sanctions

Criterion 16.18 – When processing wire transfers, FIs are required to check identification information of the originator and beneficiary against the designated list of persons and entities under UNSCRs 1267 and 1373 and their successor resolutions, and are prohibited from continuing with the transactions (see Recommendation 6). (S.32 and 34(c) of CTL, s.13a.(3)(a) of the Banking Order, s.17 of the Stock Exchange Members and Trading Platforms Orders, s.16(3) of the Postal Bank Order, s.15(3) of the Insurers Order, s.14 of the Credit Service Providers Order, s.11(1) and (2) of the MSB Order; see also R.6).

Weighting and Conclusion

There are moderate shortcomings in this Recommendation. While Israel applies the basic requirements for originator and beneficiary requirements for cross-border transfers, Israel otherwise relies on general CDD obligations instead of providing specific requirements for wire transfers. Particularly, MSBs whose business model often entails to a large extent the provision of wire transfers are not subject to specific obligations under c.16.3-c.16.7, c.16.9-c.16.14, and c.16.16. Save for stock exchange members, no FIs are required by law to verify originator information. **Recommendation 16 is rated partially compliant.**

Recommendation 17 – Reliance on third parties

Israel was rated compliant for these requirements in the last MER, because Israel laws do not permit reliance on third parties for undertaking CDD measures.

Criteria 17.1, 17.2, and 17.3 – Israeli laws do not allow FIs to rely on third parties to perform CDD measures. These criteria are therefore not applicable.

Weighting and Conclusion

Recommendation 17 is not rated as it is not applicable to the assessed country.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the last MER, Israel was rated partially compliant for these requirements. This is mainly due to a lack of general obligation for all financial institutions to establish internal AML/CFT controls to foreign branches and subsidiaries.

Criterion 18.1 – Most FIs including banks, stock exchange members, MSBs, trading platforms, insurers and the Postal Bank are required to implement AML/CFT programmes that have to take into account ML/TF risks and the size of the business. These internal controls include:

a) compliance management arrangements (including the appointment of a compliance officer at the management level): s.8 of the Banking Directive 411 and Postal Bank Directive, s.2(b)(4) of the Insurers Circular, s.3.3.11 of Risk Management Circular for Stock Exchange Members, s.3.3.9 of Risk Management Circular for Trading Platforms, and s.4 of the MSB Circular;

b) screening procedures to ensure high standards when hiring employees: s.38 of Banking Directive 411 and s.12(d) of Postal Bank Directive, s.3.3.10(c) of Risk Management Circular for Stock Exchange Members, s.3.3.8(c) of Risk Management Circular for Trading Platforms, s.2(b)(6)(g)(1) of the Insurers Circular and s.4(a) of the Commissioner Circular 2006-9-3, and s.6(g)(1) of the MSB Circular;

c) an ongoing employee training programme: s.7A of the PMLL, s.37 of Banking Directive 411 and s.12(a)-(c), (e)-(f) of Postal Bank Directive, s.3.3(10)(a) of Risk Management Circular for Stock Exchange Members, s.3.3.8(a) of Risk Management Circular for Trading Platforms, s.2(b)(4)(f)(7), 2(b)(6)(g)(2) and (3) of Insurers Circular, and s.4(e)(5) and 6(g)(2) of MSB Circular; and

d) an independent audit function to test the system: s.19-21 of Banking Directive 411 and s.7, 49 to 51 of Directive 307,[49] s.9 of Postal Bank Directive, s3.3.94 of Risk Management Circular for Stock Exchange Members, s.3.3.7 of Risk Management Circular for Trading Platforms, s.41(c) of Insurance Supervision Law, and s.4(a)(1) of Commissioner Circular 2007-9-14.

For portfolio managers, general obligation is only provided in relation to the aforementioned control item (c) above. Israel also relies on s.7A and 8(a) of the PMLL to require portfolio managers to appoint a compliance manager. There are no specific obligations for the two other requirements above.

Criterion 18.2 – Banks are required to implement group-wide AML/CFT programmes which are applicable to branches and subsidiaries of the financial group. The programmes require branches and subsidiaries to share information regarding enforcement of AML/CFT policies and procedures, including CDD and ML/TF risks information, to the parent FI. Safeguards on the confidentiality and use of information exchanged are also provided. (s.14(d), (f), 15, 16, 18 and 90 of the Banking Directive 411.)There are no similar requirements for other non-bank FIs including portfolio

49. Directive 411: Supervisor of Banks: Proper Conduct of Banking Business - Internal Audit Function

managers, MSBs, credit service providers, and insurers. As for the Postal Bank, this sub-criterion is not applicable as it does not operate in a group-wide manner.

Criterion 18.3 – Banks are required to ensure that branches and subsidiaries operating internationally apply AML/CFT measures consistent with the home country requirements, and that the stricter provisions should apply. Branches and subsidiaries of parent banks are also required to apply appropriate additional measures to manage ML/TF risks, and inform the home country supervisors, if the host country does not permit the implementation of stricter provisions of the home country. (S.88 (a) to (c) of the Banking Directive 411) Stock exchange members and trading platforms which conduct international operations through subsidiaries or local offices in foreign jurisdictions are required to develop a group-level AML/CFT policy which is consistent with the home country requirements and undertake additional control measures at both group and local levels. However, the provision does not specify the need to inform their home supervisors if the host country does not permit the proper implementation of AML/CFT measures are not consistent with the home requirements: s.3.3.13 of the Stock Exchange Members Circular and s.3.3.12 of the Trading Platform Circular. There are no similar requirements for other non-bank FIs including portfolio managers, MSBs, credit service providers, and insurers. As for the postal bank, this sub-criterion is not applicable as it does not operate through foreign branches or subsidiaries.

Weighting and Conclusion

There are a few shortcomings regarding FIs' internal controls, including lack of requirements for specific AML/CFT internal control programmes, particularly for portfolio managers. Obligations to implement group-wide AML/CFT controls and to ensure that branches and subsidiaries operating internationally apply AML/CFT measures consistent with home country requirements are required for banks and to a certain extent, stock exchange members and portfolio managers, but not for other FIs including portfolio managers, MSBs, credit service providers, and insurers.

Recommendation 18 is rated partially compliant.

Recommendation 19 – Higher-risk countries

In its last MER, Israel was rated partially compliant for these requirements because the requirements only covered banks. Other deficiencies included: absence of clear requirement to examine as far as possible the background and purpose of transactions with such countries with no economic or visible lawful purpose; no specific requirements for financial institutions to set forth their findings in writing and to keep the findings available to assist competent authorities.

Criterion 19.1 – Each of the sector-specific AML/CFT Orders contains a Schedule which: 1) authorises the IMPA to designate a list of countries and territories, based on the FATF lists, and 2) lists countries and territories determined by the state of Israel based on geographical measures and based on an internal risk evaluation regarding the risks these countries impose. The first list is updated following each FATF plenary, contains the countries and jurisdictions identified in the FATF's Public Statement and Compliance Document, and is published on IMPA's website. These lists operationalise other sections of each sectoral AML/CFT Order.

There are requirements for financial institutions to apply certain enhanced due diligence measures, proportionate to the risks, to business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF. Banks, the Postal Bank, MSBs, most credit service providers, and insurers are required to obtain the AML/CFT compliance officer's approval before finalising a funds transfers relating to listed jurisdictions (411 Directive on Management of AML and CFT Risks, s.82a-b; Insurers Circular, s.2(b)(4)(f)(6) and s.2(b)(6)(b), MSBs Circular,

s.4(e)(4) and 6(b); Postal Bank Directive, s.31; MSB Order, s.3 and Third Schedule). MSBs are also required to treat all transactions involving listed jurisdictions as high risk. Securities dealers, portfolio managers, and trading platforms must apply enhanced monitoring of accounts involving high risk countries (Stock Exchange Members Order, s.11(1); Portfolio Managers Order, s.9(1)), Trading Platforms Circular s.7.3). Nevertheless, the range of enhanced due diligence measures required is not fully comprehensive.

Criterion 19.2 – Financial institutions are able, and are required to, apply certain counter-measures when called upon to do so by the FATF. Most financial sector Orders, Directives, and circulars require the systematic reporting of certain transactions above certain thresholds involving high risk countries and territories as identified by the FATF and by Israel through the lists describe above. For banking corporations and the Postal Bank, these are cash transactions above certain thresholds (Banking Order s.8; Postal Order s.11(a)(3)). For MSBs, firms covered by the Trading Platforms Order, Stock Exchange Members Order, and insurers, these are all transactions above certain thresholds (MSB Order s.8(a)(3); Trading Platforms Order s.12(3); Insurers Order s.10(a)(2); Stock Exchange Members Order s.12). These measures now apply equally to the DPRK. However, this range of counter-measures is not fully comprehensive, and portfolio managers do not have similar obligations.

Separately, and independently of any call by the FATF, Israel applies broader counter-measures regarding Iran. This includes strictly limiting all business relationships or transactions with the country (see Recommendation 7).

Criterion 19.3 – Israel has measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. In addition to the countries and territories designated by Israel as high risk, IMPA also publishes the FATF's Compliance Document on its website. IMPA also disseminates the FATF's lists and its own list to IMPA's mailing list which includes financial institutions and the financial institution supervisors.

Weighting and Conclusion

Israel meets or mostly meets all the criteria of Recommendation 19. However, there is a minor deficiency in that the range of enhanced due diligence and counter-measures applied are not fully comprehensive with regard to DPRK.

Recommendation 19 is rated largely compliant.

Recommendation 20 – Reporting of suspicious transaction

Israel was largely compliant for these requirements in the last MER. Main technical deficiencies were that only transactions above certain thresholds require reporting, and attempted transactions are not explicity covered.

Criterion 20.1 – The PMLL contains a general obligation for financial institutions to report (s.7(a)(2) and 7(b)), and Schedule 3), with the specific requirements to be set out in sectoral Orders. These Orders require all FIs to report "unusual transactions" to IMPA (s.9(a) of the Banking Order, s.11(b) of and Fourth Schedule to the Credit Service Providers Order, s.13 of and Third Schedule to the Stock Exchange Members and Trading Platforms Order, s.10 and Third Addendum of Portfolio Managers Order, s.11 of and Fourth Schedule to the Insurers Order, s.12 of and Third Schedule to the Postal Bank Order, and s.8(b) of and Fifth Schedule to the MSB Order.

For banks, and the Postal Bank "unusual transaction" includes any transaction for which, in view of the information in the FI's possession, suspicion is raised that it is related to activity prohibited under

the PMLL or PTFL (and through transitory provisions, the CTL) (s.21(d) of the Postal Bank Directive). This therefore covers any suspicion of ML and predicate offences, and TF.

For the other financial institutions, the sector orders are issued under the authority of the PMLL and CTL in order to enforce these laws (s.7 of the PMLL and s.95 of the CTL – i.e. preventing ML (including predicate offences), terrorism, and TF. They define unusual transactions as any that appear to be unusual (in the context of ML/TF) and include a list of possible indicators (e.g. transactions with no apparent economic purpose, or not characteristic to the account, or those involving high risk countries and territories). The indicators also specifically list terrorism and TF offences. The Stock Exchange Members and the Trading Platforms Circulars (s.5.2) the Insurers and MSBs Circular (s.6(f)), and the Portfolio Managers Guidelines Circular (published in 2011) (s.5.2) further clarify that an unusual transaction includes any event that gives rise to suspicion of ML or TF.

Financial institutions are required to report these transactions "as soon as possible" (s.4(a)(2), Prohibition on Money Laundering Regulations (Methods and Times for Reporting to the Data Base by Banking Corporations and entities specified in the Third Schedule), 5762-2002).

Criterion 20.2 – The requirements above include all attempted transactions, regardless of the amount of the transaction.

Weighting and Conclusion

Recommendation 20 is rated compliant.

Recommendation 21 – Tipping-off and confidentiality

In the last MER, Israel was rated largely compliant for these requirements. The technical deficiencies are that tipping off provisions were not applicable to all other relevant information outisde of banking corporations.

Criterion 21.1 – FIs and their directors, officers and employees are protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. The provision in the PMLL does not distinguish between whether the FIs et al need to know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred: s.24(a) of the PMLL.

Criterion 21.2 – FIs and their directors, officers and employees are prohibited by law from disclosing the fact that an STR or related information is being filed with the FIU. S. 31A(a) of the PMLL; s.12 of the Banking Order; s.16 of the Stock Exchange Members and Trading Platforms Orders, s.14 of the Portfolio Managers Order; s.14 of Insurers Order; s.13 of the Credit Service Providers Order; s.15 of the Postal Bank Order; s.10 of the MSB Order.

Weighting and Conclusion

Recommendation 21 is rated compliant.

Recommendation 22 – DNFBPs: Customer due diligence

This Recommendation was rated non-compliant in the last MER because there was no CDD obligations for Designated Non-Financial Businesses and Professions (DNFBPs) including real estate agents, dealers in precious metals and stones, trust and company service providers, lawyers, notaries, other independent legal professionals and accountants. Some of these deficiencies have

since been resolved with the inclusion of sectors previously not covered for example dealers in precious stones.

At present, a number of DNFBP sectors continue to fall outside Israel's AML/CFT regulatory regime (see R.28), hence an absence of CDD requirements. According to the May 2015 to March 2017 NRA, the risk level of these DNFBP sectors range from low to medium high.

Criterion 22.1 – Casinos are deemed to be illegal in Israel.[50] However, other DNBFPs are required to comply with the CDD requirements for AML/CFT purposes in the following situations:

a) dealers in precious stones: s.2, 3, 4 of Dealers in Precious Stones Order and the Fourth Schedule; [51] and

b) lawyers[52] and accountants providing services under c.22.1(d) (e.g. buying and selling real estate, managing of client money, and organisation, operation and management of legal persons and arrangements): s.8B of the PMLL and s.2, 3 and 4 of Business Service Providers Order. [53] Deficiencies identified under the analysis of R.10 above are similar to those in the Dealers in Precious Stones Order and Business Service Providers Order.

For real estate agents,, dealers in precious metals, and TCSPs engaging in transactions that should be covered under R.22, Israel has not introduced any CDD requirements for AML/CFT purposes.

Criterion 22.2 – Among DNFBPs, only lawyers and accountants providing services in c.22.1(d), and dealers in precious stones are required to retain identification documents for a minimum period of five years after providing the business service. This can be extended at the written request of the supervisor. (S.8 of BSP Order and s.9 of Dealers in Precious Stones Order). For BSPs, the requirement also includes all the main records which a business service provider has used in performing the customer recognition procedure, in an efficient manner so as to facilitate identification of and availability of the information; there is no similar requirement for dealers in precious stones. There are no specific legal provisions stipulating the requirements of c.11.1 (transaction records), c.11.3 (that transaction records be sufficient to permit reconstruction of individual transactions), and c.11.4 (ensuring that CDD (for dealers in precious stones) and transaction records are available swiftly to competent authorities upon appropriate authority).

Criterion 22.3 – A 'foreign politically exposed person' is defined in the BSP Order and in the Dealers in Precious Stones Order and is considered as high risk. In addition to CDD measures required under c.22.1, lawyers and accountants as BSPs, as well as dealers in precious stones, are required to undertake some additional measures required under R.12 in relation to foreign PEPs. The additional measure includes a risk evaluation of ML/TF for determining the customer characteristics, type of

50. Most gambling, including casinos and casino activity, are prohibited in Israel (Article 12, s.225 and 226 of the Criminal Code). The exceptions are social gambling and two types of gambling under a special permit: the Israeli National Lottery (pursuant to the Notice on the granting of permit to the Mifal Hapais (National Lottery) pursuant to the Penal Law, 5737 – 1977 issued by the Ministry of Finance), and sports betting under the Israel Sports Betting Council (pursuant to the Regulation of the Sports Betting Law).
51. Prohibition of Money Laundering (Obligations of Dealers in Precious Stones regarding Identification, Reporting and Record-keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order 5775-2014
52. This includes other independent professionals and notaries, since these must also be lawyers in Israel.
53. Prohibition of Money Laundering (Obligations of Business Service Providers Regarding Identification and Record-Keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order 5775-2014

business service requested, and source of funds (but not source of wealth). The following requirements apply to dealers in precious stones but not for business service providers:

- obtaining senior management approval before establishing or continuing business relationship with foreign PEPs; and
- conducting on-going monitoring of business relationship including with foreign PEPs.

Neither sector is required to conduct CDD and additional measures for persons who have been entrusted with a prominent function by an international organisation. Analysis of c.22.1 is also relevant (For example, the Orders do not have any measures for domestic PEPs.) (S.1 and 3 of BSP Order; s.1 and 2(d) of Dealers in Precious Stones Order.)

Criterion 22.4 – Lawyers and accountants providing BSP services are required to monitor publications issued by the supervisor, relating to perceived threats deriving from new technologies and in particular those business services provided without the need to perform face-to-face identification (paragraph 3(a) of the Fifth Schedule to the BSP Order). However, they are not required to assess the ML/TF risks themselves, or to comply with any requirements under c.15.2. Dealers in precious stones, on the other hand, are required to monitor threats resulting from new technologies and in particular those which enable transactions to be conducted without face-to-face identification, and develop procedures. (S.15 of Dealers in Precious Stones Order).

Criterion 22.5 – (*Not applicable*) Similar to R.17, Israeli laws do not allow DNFBPs relying on third parties to perform CDD measures. This criterion is therefore not applicable (see also R.17).

Weighting and Conclusion

Israel meets some of the essential CDD criteria for DNFBPs, namely lawyers and accountants. Nevertheless, there are a number of deficiencies, and certain DNFBPs do not have AML/CFT obligations.

Recommendation 22 is rated partially compliant.

Recommendation 23 – DNFBPs: Other measures

Israel was rated non compliant for these requirements in the last MER, there were no reporting obligations upon real estate agents, dealers in precious metals, trust and company service providers, lawyers, notaries, other independent legal professionals and accountants.

Criterion 23.1 –

a) There is no legal provision requiring lawyers and accountants engaging in financial transactions in relation to the activities described in the FATF Recommendations to report suspicious transactions to any authorities.

b) Dealers in precious stones are required to report "unusual transactions", including attempted transactions, to the IMPA. S.11 of and Third Schedule to Dealers in Precious Stones Order.[54] However, unlike for FIs (see R.20), there is no further requirement specifying that reporting be based on suspicion of ML or proceeds of criminal activity; however, this is implied since the Orders are issued under the authority of the PMLL and CTL) and with the objective of enforcing these laws (s.7 of the PMLL and s.95 of the CTL – i.e. preventing ML (including predicate offences), terrorism, and TF.

54. Prohibition of Money Laundering Order (Identification, Reporting and Record-keeping Requirements of Dealers in Precious Stones to Prevent Money Laundering and the Financing of Terrorism), 5774-2014.

c) As mentioned in the analysis under R.22, Israel does not impose any AML/CFT obligations on real estate agents, dealers in precious metals and TCSPs; hence an absence of suspicious transactions reporting requirements.

Criterion 23.2 – Israel has only provided in its law the obligations for lawyers and accountants who are business service providers and dealers in precious stones to train their employees for the purposes of implementation of AML requirements, and for dealers in precious stones to appoint a compliance officer (s.8(B)(2)(e) and 8(A)(f) of the PMLL, s.3(d) of the Fourth Schedule to the Dealers in Precious Stones Order; s.3(b) of the Fifth Schedule to the BSP Order). There is no other legal provision specifying the requirement of R.18 – e.g. compliance management arrangements (for lawyers and accountants), screening procedures, or an independent audit function. As noted above, the three other DNFBPs do not have any AML/CFT requirements (including for R.18).

Criterion 23.3 – There are no specific provisions requiring enhanced due diligence requirements, proportionate to the risks, to business relationships and transactions with natural and legal persons from higher risk countries as required under c.19.1; the BSP order requires only that the BSPs (i.e. lawyers and accountants) monitor publications from the supervisor, including the risks stemming from higher-risk countries, and act accordingly (s.3(a) of the Fifth Schedule to the BSP Order). Country risk, including the list of high risk countries and territories distributed, is also factor that BSPs and dealers in precious stones *may* consider as higher-risk for CDD purposes. (Schedule 4 to the BSP Order). Dealers in precious stones must monitor transactions involving listed countries and territories (s.10(b)(2) DPS Order).

While there are no specific counter-measures in the BSP and DPS Orders, *all* DNFBPs must apply counter-measures with regard to Iran.

Finally, covered DNFBPs are advised of concerns about weaknesses in the AML/CFT systems of other countries, through the list distributed by IMPA and countries and territories specified in the BSP Order (Schedule 4) and DPS Order (Schedule 1).

Criterion 23.4 – Dealers in precious stones are prohibited by law from disclosing the fact that an unusual transaction report has been filed (s.24 of the PMLL and s.13 of Dealers in Precious Stones Order). Exemption from criminal and civil liability for reporting is provided for in the law (s.24(a) PMLL). As mentioned under c.23.1, Israel has not imposed any suspicious transactions reporting requirements for lawyers and accountants engaging in financial activities described in c.22.1(d), and therefore an absence of tipping-off and confidentiality provisions in the law.

Weighting and Conclusion

While dealers in precious stones have reporting obligations, the other DNFBPs in Israel do not. There are also only some requirements for applying the requirements of R.18, 19, and 22. Given these deficiencies, **Recommendation 23 is rated partially compliant.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

In its last MER, Israel was rated partially compliant for the requirements for legal persons. The deficiencies included: information on the Companies Register did not cover beneficial ownership; information on the Companies Register was not verified and considered not reliable.

There are two main types of legal persons in Israel, namely companies and partnerships. These legal persons are subject to registration with the Registrar of Companies and the Registrar of Partnerships

respectively. Companies are governed by the Companies Law, while partnerships are governed by the Partnerships Ordinance.

Criterion 24.1 –

(a) Israel has put in place mechanism to identify and describe the different types, forms, and basic features of legal persons in the country. Specifically, the Companies Law specifies the five types of company (all legal persons), namely private companies, bond companies, public companies, charitable companies and foreign companies (see Chapter 1). Separately, the Partnerships Ordinance identifies and describes four types of partnerships, namely general partnerships, limited partnerships, public limited partnerships and foreign partnerships (which may be either General Partnerships or Limited Partnerships). A partnership established for business purposes is required to be registered (section 4); a registered partnership is a legal person (section 66). A partnership established for non-business purposes may be registered and, in such cases, all of the relevant provisions of the law will apply to it equally; it may remain unregistered and, in such cases, it will not be a legal person.

(b) The process for the creation of each of the above types of legal persons is set out in the respective law and in regulations promulgated under the laws. The process includes submission of information such as ownership (shareholders, partners or members) on forms which are recorded in the ICA database. Scanned copies of the forms submitted and the information recorded in the ICA database are publicly available in the respective registry. See c.24.6 on the extent to which registered information comprises beneficial ownership information. Further, beneficial ownership information is obtained and recorded using other publicly available mechanisms as further detailed in c.24.6.

Criterion 24.2 – The Israeli authorities have assessed the risks of all types of legal persons under the NRA. The assessment process revealed that there is insufficient information on the scale of ML through legal persons (and arrangements, including NPOs), and that further analysis should be conducted; this contributed to the rating of the risks associated with legal persons created in Israel as moderate-high, and measures to remediate the gaps were included in the action-plan. See also IO.5. While an assessment has been carried out, it is not comprehensive and therefore is not regarded as complete, although understanding by the authorities has increased since the NRA was carried out.

Criterion 24.3 – Israel requires that all companies created in the country are registered in a company registry. The table below articulates where the various provisions on registration applicable to this criterion can be found in the Companies and Partnerships Law (and their respective regulations).

FATF requirement for what should be registered at a registry	Companies	Partnerships
Company name	Articles 18, 25 - 29; Regulation 1 and Form 1 in the Annex of the Reporting Regulations	Articles 7, 10-12; Regulation 4 and Form 1 in Annex 2 of the Partnerships Regulations
Proof of incorporation	Article 10, provided by the Registrar	Articles 8, 69, provided by the Registrar
Legal form and status	Articles 38, 140, 343	Articles 7, 58, 70; Regulation 4 and Form 1 in Annex 2 of the of the Partnerships Regulations
Address of registered office	Article 123; Regulation 1 and Form 1 in the Annex of the Reporting Regulations	Article 7; Regulation 4 and Form 1 in Annex 2 of the of the Partnerships Regulations

FATF requirement for what should be registered at a registry	Companies	Partnerships
Basic regulating powers	Article 8, 18-19, 23 regarding bylaws; Regulation 1 and Form 1 in the Annex of the Reporting Regulations; Default provisions throughout Company Law if provisions are not determined otherwise in the bylaws	Article 62 regarding limited partnerships; Default provisions throughout ordinance if provisions are not determined otherwise in the partnership agreement (Article 30 of the Partnerships Ordinance).
List of directors	Article 8; Regulation 1 and Form 2 in the Annex of the Reporting Regulations	Article 7 – all partners; Regulation 4 and Form 1 in Annex 2 of the of the Partnerships Regulations

By virtue of section 43 of the Companies Law all registered information at the Companies Registry is available to the public. Similar provision is made in section 70 of the Partnerships Ordinance. Information on the company/partnership name, registration date and number, legal form and status, and address of the registered office is publicly available free of charge. Information on current share capital and the identity of shareholders and directors and equivalent data for partnerships is publicly available subject to a small fee (currently NIS 10 (EUR 2.3), while a copy of the full docket of the company/partnership, including its constitutional documents, is also available for a small fee (currently NIS 33 (EUR 7.7) for a file sent by email or NIS 63 (EUR 14.7) for a CD-ROM).

Criterion 24.4 –Companies are required to have a registered office in Israel (and the provision of the address to the Registrar); keep certain documents, including the articles of association (setting out the company's name, legal form and status, and basic regulating powers); the register of shareholders (and, for a public company, the register of substantial shareholders) and the register of directors (sections 123, 124, 127, 128 of the Companies Law). Section 130 specifies that the information to be recorded in the register of shareholders (which must kept in the registered office, in Israel) includes the amount of shares and the class of shares held by each shareholder. Section 82 of the Companies Law permits a company to determine within its articles of association different voting rights attached to different classes of shares and that, if no such determination is made, specifies that each share will count as one vote.

Section 69(b) of the Partnerships Ordinance requires partnerships to keep and display in their main place of business a copy of all certificates received from the registrar that confirm the information reported by the partnership to the registry. Partnerships must provide information to the registrar at the time of formation and update the information within seven days of any change (c.24.3). See the legal provisions specified in c.24.5 below which address the element of c.24.5 on the maintaining of information. While partnerships do not have an obligation to maintain their main place of business within Israel, (i) as explained above, all information regarding the partners must be reported to the registrar, which maintains its registry within Israel; and (ii) an examination conducted by the ICA showed that 100% of the registered partnership provided an address in Israel as their main place of business.

Criterion 24.5 – Israel has specified in its law the obligation to maintain the information referred to in criteria 24.3 and 24.4 accurate. There are requirements for the timely updating of both companies- and partnerships-related information (see tables below). The table below summarises the provisions which require changes of information to be provided to the Registry.

FATF requirement for what information should be registered at a registry	Specify when registry information must be updated when company information changes and the legal provision(s)	Specify when registry information must be updated when partnership information changes and the legal provision(s)
Company/partnership name	Article 21 (within 14 days of the resolution), 31, 40, 140 (annual reporting obligation), 145; Regulation 7 and Form 8A in the Annex of the Reporting Regulations	Article 9 (within 7 days of the change), Article 13 (a change in the name is subject to the Registrar's approval); Regulation 4 and Form 2 in Annex 2 of the Partnerships Regulations
Proof of incorporation	N/A	N/A
Legal form and status	Articles 140 (annual reporting obligation), 343 (within 14 days of the change); Companies Ordinance provisions regarding dissolution	Articles 9 (within 7 days of the change), 59, 60; Regulation 4 and Form 4 in Annex 2 of the Partnership Regulations
Address of registered office	Article 123 (within 14 days of the change of address), 140 (annual reporting obligation), 141, 145; Regulation 9 and Form 9 in the Annex of the Reporting Regulations	Article 9 (within 7 days of the change); Regulation 4 and Form 2 in Annex 2 of the Partnership Regulations
Basic regulating powers	Articles 21 (within 14 days of the resolution), 40, 140 (annual reporting obligation); Regulation 7 and Form 8A in the Annex of the Reporting Regulations	Article 62 (limited partnership – a change to the by-laws of a limited partnership is subject to approval of the Minister of Justice, delegated to the registrar); Regulation 4 and Form 2 in Annex 2 of the Partnership Regulations
List of directors	Articles 140 (annual reporting obligation), 141, 223 (within 14 days of the change); Regulation 5 and Form 6 in the Annex of the reporting regulations	Articles 9 (within 7 days of the change), 59, 60; Regulation 4 and Form 4 in Annex 2 of the Partnership Regulations

The table below summarises the provisions which require information held by legal persons to be updated when there are changes to it.

FATF requirement for what information should be maintained by a legal person	Specify when registered office must be advised when company information changes and the legal provision(s)	Specify when registered office must be advised when partnership information changes and the legal provision(s)
Company/partnership name	Part of the articles of association – Articles 18, 124	Articles 7, 9, 13, 69
Proof of incorporation	N/A	N/A
Legal form and status	Part of the articles of association – Articles 18, 124	Articles 61, 69
Address of registered office	Articles 123, 124	Articles 7, 9, 69
Basic regulating powers	Part of the articles of association – Articles 18 - 19, 124	Article 34 and for limited partnerships also Articles 61, 69
List of directors	Articles 124, 224	Articles 9, 59,60, 69(b), 70
Number of shares by each shareholder or the level of partnership interest by each partner in a partnership	Articles 124, 127-134	Article 34
Category of shares held by each shareholder	Articles 124, 127-134	Articles 34, 69(b), 70
Nature of voting rights for each shareholder/holder of a partnership interest	Articles 19, 82 124 (if voting rights not equal between all classes, this needs to be specified in articles of association)	Article 34

In addition to the reporting of specific changes mentioned above, companies (but not partnerships) are required to submit an annual report to ensure the information in the registry is up-to-date. In addition to legislative provisions, Israel has other relevant mechanisms. Identification details provided to the ICA on shareholders, directors and partners who are Israeli citizens are checked for accuracy with the database of the population registry. The identification details provided for a legal person are also checked against the details held in the ICA's database for other registered legal persons of the same kind. Under sections 8 and 23 of the Companies Law, as well as the Companies Regulations (and Partnerships Regulations), all shareholders/directors/partners sign, in person, at least one of the documents submitted in the application for registration and each such signature and identity is verified by an Israeli lawyer. Shareholders/directors/ partners who are not Israeli citizens are also required to submit a certified copy of their passport (individuals) or a certified copy of the certificate of incorporation (legal persons). Under section 39 of the Companies Law and the respective Companies Regulations, changes in shareholders, directors or partners information as well as the annual report containing such information, submitted to the registrar, need to be signed by a natural person authorized to do so by the company, who declares that the information reported is true and complete. The signature and identity of such natural person are verified by a lawyer (or an accountant for the annual report). Submission of false information is a criminal offence (see criterion 24.13).

Also, in the past seven years, the ICA has undertaken measures to ensure compliance with the annual reporting requirements for private companies. These measures have included public campaigns to increase compliance and public awareness of the reporting requirements; declaring companies as "Violating Companies" under section 362A of the Companies Law, a status which is available to the public, allows the ICA to refuse to register and release charges (which significantly limits the ability of companies to obtain credit), change the company name or purpose, and register mergers; the ICA can also deny the controlling shareholder from registering new companies; and, from 2016, the imposition of fines against companies which have not submitted their annual reports. See IO.5.

Criterion 24.6 – Israel does not require legal entities or respective registrars to hold beneficial ownership information as such, but rather takes a holistic approach, relying on several mechanisms, which involve institutions actively obtaining and verifying beneficial ownership information (mainly through information obtained by the ITA (see IO.5), information obtained by FIs and DNFBPs through the obligatory CDD process (see c.10.5), information held by company as required under c.24.3 above, and information available on a stock exchange) to seek to meet this criterion.

First, beneficial ownership information is held by FIs and DNFBPs under the CDD process – see criterion 10.5 (mostly met). Lawyers subject to CDD obligations are always involved with the establishment of a company or partnership, and submission of the application to the registrar by a person who is not a lawyer (subject to CDD obligations) is very rare, particularly in recent years, as lawyers may submit all registration forms online, with designated digital certificates - under regulation 16A-16B of the Companies Regulations the online application to register a legal entity must be submitted by a lawyer with the rarely used exception that a natural person who is the sole shareholder and director in the company to be established may submit the application for himself after identifying himself with a personal electronic certificate. Even under this exception, a lawyer is still required in the process to verify the shareholder's signature on the articles of association. See below regarding the requirement that a lawyer (or an accountant, for annual reports), certifies the signatures on all forms submitted to the ICA regarding ownership. Furthermore, as the ITA requires any entity reporting to it to maintain an Israeli bank account, it would, in the view of the Israeli

authorities, be practically impossible for an Israeli legal entity to conduct any financial activity without opening an account with an Israeli bank (who is subject to CDD obligations).

Second, the ITA obtains significant information on all legal persons which are obliged to report to it (due to having income, owning property, having employees in Israel or buying/selling real estate in Israel), including a requirement for information to be provided to the ITA annually on the directors, shareholders and beneficial owners. The ITA requires the details of an Israeli bank account as part of the registration process of a legal person and is proactive in checking all relevant parties, including beneficial owners of legal persons and legal arrangements (See IO.5). The Israeli authorities consider that it is practically impossible for any Israeli entity to conduct any financial activity without providing beneficial ownership information to the ITA.

Third, in relation to public companies, under Regulation 33(c) of the Securities Regulations (Periodic and Immediate Reports) a company, the securities of which were offered to the public (and so long as such securities are held by the public) must file reports on its Interested Parties (including holders of 5% or more of the issued share capital or voting power and persons holding the power to nominate one or more of the directors or the general manager) with the ISA (and with the TASE if the company is a listed company). While not aimed at beneficial owners it is possible these provisions on legal owners and controllers might include beneficial owners. The information includes the fact of the securities being held by a trustee if that is the case, together with basic information on the trust and the beneficiary. Shareholdings in listed public companies or listed public limited partnerships where the shares/partnership interests are not held by "interested parties" are held through TASE members who are required to obtain beneficial ownership from their clients under the CDD obligations specified in R.10.

The above mechanisms are supported by certain verification applied with regard to the legal ownership aspect of beneficial ownership of shareholdings in companies and partnerships by the registrar of companies/partnerships respectively, where the legal owners of those companies (or partners in the partnerships) are individuals or where the ownership chain consists only of registered Israeli companies/partnerships or individuals; in such cases, identification details (name, ID number and address) of the beneficial owner can be traced by the registrar. With reference to section 23 of the Companies Law, the articles of association of a company must be signed by the first shareholders and specify the shares allotted to each shareholder, together with the name, ID number and address of each shareholder; a lawyer must verify the identity of the signing shareholders (Regulation 1 and Form 1 in the Annex of the Companies Regulations) and sign the articles to this effect. Furthermore, in accordance with section 8(2) of the Companies Law, the first directors of a company must provide a statement confirming their abilityto be directors. The statement must be verified by a lawyer (Regulation 1 and Form 2 in the Annex of the Companies Regulations) and provided to the Registrar. The initial registration form of a partnership must include the above mentioned identification details regarding all partners and their signatures on such form must be verified by a lawyer; any subsequent changes to the registration must include identification details of new/changed partners and signatures of a partner, verified by a lawyer (Articles 7, 9, 59 and 60 of the Partnerships Ordinance; Regulation 4 and forms 1 and 2 in Annex 2 of the Partnerships Regulations).

Where shares are held by trustees the fact of the trusteeship must be notified to the company under section 131 of the Companies Law and recorded in the register of shareholders maintained at the company's registered office under section 124, which is publicly available; such indication is also made to the registrar of companies, if an application or report has been submitted in the online

system, and subsequently reflected in the publicly available information. In turn – FIs, DFNBPs and the ITA are made aware of such holdings by a trustee and inquire regarding the beneficial ownership as part of the CDD procedures.

While it cannot be certain that the entirety of legal persons are covered by the above provisions (bearing in mind that a large number of legal persons are inactive), substantially all of the financial activity in Israel goes through reporting and accountable FIs & DNFBPs, and entails reporting obligations towards the ITA. Therefore, substantially all legal persons that have financial activity or assets are subject to the above mechanisms which complement each other and include procedures for active solicitation and verification of the beneficial ownership information.

Criterion 24.7 – This criterion follows the order of the approaches in c.24.6 to holding beneficial ownership information.

First, for FIs and DNFBPs, see c.10.10 (mostly met) and 10.7 (met) and the respective notes in c.24.6 above.

Second, reports regarding beneficial ownership to be made to the ITA are required to be updated annually. Legal persons established in Israel are always considered as Israeli residents for tax purposes, and always have to submit annual reports to the ITA (even if there is no income or tax liability in Israel).

Third, with regard to public and listed legal persons (both companies and limited partnerships whose units are offered to the public), an immediate report to the ISA (and the TASE, if listed) must be submitted in relation to any change in the registered or issued capital (Section 36 of the Securities Law and Regulation 31 of the Securities Regulations (Periodic and Immediate Reports)) and to the holdings of Interested Parties (Regulation 33(b) of the Securities Regulations (Periodic and Immediate Reports); annual reports in that regard must be submitted in accordance with Regulations 24 and 24A of the Securities Regulations (Periodic and Immediate Reports). See criterion 24.5 above in relation to verification by the ICA of information it holds.

Concerning information provided to the respective ICA registry, under section 292 of the Companies Law private companies must, within fourteen days of an allotment, provide the Registrar with a form specifying the details of the allotment; and any transfer of shares must be reported to the Registrar within 14 days (sections 140(6) and 299 of the Companies Law). In addition, section 141 of the Companies Law provides that private companies must provide the Registrar with an annual report, which includes updated information on shareholders and their holdings (Regulation 4 and Form 5 in the Annex of the Reporting Regulations). With regard to partnerships, under section 9 of the Partnerships Ordinance, partnerships are required to inform the registrar of any changes in the partners within seven days of the change. There are no annual reporting requirements for partnerships except for those partnerships whose units are offered to the public (see below in this criterion).

When an application to register a company is submitted online, or when the allotment of new shares or the transfer of shares is reported online, it is mandatory to report whether a shareholder holds the shares in trust or not. A change in trustee must be reported to the ICA as it will be a change in the identity of the shareholder (article 131 of the Companies Law).

As with c.24.6, while it cannot be certain that the entirety of legal persons are covered by the above provisions, Israel considers that any gaps in the beneficial ownership information obtained and held within Israel are immaterial, for the reasons detailed in c.24.6 above. It should be noted that inactive companies, who do not submit annual reports to the Companies Registrar, are subsequently declared "Violating Companies". Such a status is publicly available (free of charge), subjects the company and its controlling shareholders to certain sanctions (see c.24.5 above and c.24.13 below) and raises a red flag to FIs, who in turn inquire regarding the circumstances that caused such status and insist on its resolution.

Criterion 24.8 – Forms submitted to the Companies Registry or the Partnerships Registry pertaining to information regarding shareholders, directors or partners must be signed by natural persons who are authorised to sign them on behalf of the company/partnership (or by themselves as shareholders, directors or partners; all such wet-ink signatures must be verified by a lawyer (or, in relation to annual reports of companies, also by an accountant – see Regulation 4 of the Reporting Regulation and Form 5 in the Annex). If the form is submitted using the online system – the person submitting the report is identified personally by an electronic certificate. Such individuals who sign or submit the forms declare that the information submitted is true and complete and has been recorded in the company's registries and are accountable - see c.24.13 for the sanctions for providing false information. In addition, sections 360(a) and (e) of the Companies Law provide that an administrative fine not paid by the company may be demanded from the director or general manager that was appointed as accountable for the reporting obligations or, if one was not appointed, from any director of the company; a director must be a natural person or a legal person appointing a liable representative who is a natural person (sections 235-236 of the Companies Law).

The competent authorities can obtain information from FIs and DNFBPs required to obtain basic and beneficial ownership information through CDD measures. This includes lawyers and accountants providing professional services relating to the purchase or sale of a business; receiving, holding or transferring funds for the purpose of establishment or management of a corporation; and the establishment or management of a corporation, business or trust. Lawyers and accountants are therefore accountable. In this connection, the courts in Israel have issued rulings which clarify that basic and beneficial ownership information of clients of attorneys is not covered by attorney-client privilege (e.g. case 751/15 Abergil and case 2163/96 Fairzen).

LEAs can also obtain such basic and beneficial ownership information as is held by any person.

While there are no specific legal obligations requiring legal persons to authorise a natural person or DNFBP to be accountable to the competent authorities and give assistance to them, such information as is held can be obtained by the authorities. In addition, Israel has noted that all reports and declarations submitted to the FIs, DNFBPs and by any person to relevant authorities are signed by natural persons who are accountable in relation to the information reported/declared and future updates thereof. The same point on accountability will apply where reports/declarations are made by legal persons.

Criterion 24.9 – Under sections 127-130 of the Companies Law, a company is required to maintain a register of shareholders. Under sections 124-126 of the Companies Law, that register must be available in the company's registered office. Pursuant to section 130(b) of the Companies Law a company must keep all records recorded in the register and make any updates to the details as soon as it becomes aware of such updates. The obligations under the above sections apply to a company continuously until it is dissolved. Under section 366 of the Companies Ordinance, the records of a

company which ceases to exist must be maintained by a person appointed by the court for 5 years from the point of dissolution (although the provision is not clear and the new Bankruptcy Law (taking effect on September 2019) that replaces these provisions in the Companies Ordinance will clarify the provision and extend the record keeping obligation to a minimum of 7 years). Typically, the records are kept by the liquidator of the company. There are no similar requirements in relation to partnerships, although it is possible that the court might order records to be maintained. Partnerships are required to submit updates regarding the identity of partners to the Partnerships Registrar, and the registrar keeps such records. With regard to limited partnerships whose units are offered to the public, the partnership is obliged to keep a register of unit-holders pursuant to articles 65GG-65II of the Partnerships Ordinance, and (by virtue of section 65II(b) of the Ordinance) the provisions of section 130(b) of the Companies Law apply *mutatis mutandis*. According to section 12 of the Israeli Archives Law, the ICA is required to maintain all records in perpetuity, including those of legal persons after dissolution. The ITA is also subject to this law and keeps its computerised records in perpetuity. See also c.11.2 for the record keeping requirements for FIs (met in relation to CDD, including beneficial ownership) and c.22.2 for the record keeping requirements for DNFBPs (BSPs and dealers in precious stones are required to retain identification records for a minimum of five years after providing the business).

Criterion 24.10 – Information held by the company and partnership registries is publicly available and therefore also to competent authorities. In addition, the TASE holds information on basic and beneficial ownership of interested parties of public, listed legal persons. Also see R.31 for the powers of LEAs and R.s 27 and 28 for the powers of the relevant supervisory authorities.

Criterion 24.11 – Under section 289A of the Companies Law a company may not issue or allot any type of bearer security. In relation to any bearer securities which were issued or allotted prior to the section coming into force in September 2016, section 13 of Amendment 28 to the Companies Law provides that such securities will not grant their holder any rights until the holder surrenders the bearer certificate(s) to the company and the company registers the relevant securities under the holder's name (after obtaining the required identification details). The concept of bearer security would appear to embrace both shares and warrants.

Article 65ZW of the Partnership Ordinance applies the provisions in relation to bearer securities set out in the Companies Law in relation to public limited partnerships (but not other partnerships). Israel has advised that the other partnerships cannot issue bearer securities as there is no express provision that allows the issuance of such securities. This is different to the Companies Law, which contained an express provision.

Criterion 24.12 – Under section 131(a) of the Companies Law, where shares of a company are held by a trustee, the fact of the trusteeship must be declared to the company and a record made in the register that the trustee is a shareholder.

While Section 131(b) of the Companies Law provides an exemption to section 131(a) to shareholders of listed companies (the shares of which are registered in the name of a nominee company), holders of such shares must declare the fact of trusteeship and the identity of the beneficiary to the member of TASE concerned under the CDD requirements analysed in R.10 and also to the ISA and TASE if they are Interested Parties (see c.24.6 and 24.7 above).

While there are no specific provisions in the Companies Law governing nominee shareholders, the Israeli authorities were able to confirm that the applicable provisions of section 131(a) have a very

wide meaning, supported by section 1(a) of the Agency Law, interpretation by the State Attorney and precedent, and relate to a person "holding shares in trust/trusteeship", meaning any person holding shares on behalf of another person and that this includes nominee arrangements. It is possible that the person in question might not always be the nominator.

While there is no written requirement for companies to make the fact of a trusteeship known to the ICA. the voluntary online registration system includes a mandatory field requiring trustees to disclose their status. Some 85% of requests for incorporation of companies are made by way of the online system. It is not clear to what extent changes to shareholdings are made via the online system. If the establishment of a company/partnership or a change in ownership involves a lawyer (which is most usually the case), who is subject to CDD obligations, then the beneficial ownership information of the person holding the shares in trust must be obtained and kept by the lawyer. Where reports to the ICA after registration are made through the online system, the fact that the shares are held in trust are publicly available in the ICA database (and trigger beneficial ownership inquiry/verification by the banks (which are subject to CDD obligations), by the ITA and other authorities. For FIs and DNFBPs, see c.10.4 onwards and c.22.1 and the mechanisms governing the disclosure of beneficial ownership at c.24.6 and c.24.7 above). These mechanisms (relevant to c.24.12(c)) reduce the risk and materiality of the ICA not being provided with all of the information required by c.24.12(a) to the ICA but it cannot be certain that the criterion is fully met.

Provisions similar to section 131 of the Companies Law are not included in in the Partnerships Ordinance but the provisions above on registration with the ICA and the relevance of FIs and DNFBPs in mitigating risk are applicable.

Section 106(b) of the Companies Law provides that a person may only exercise the powers of a director if appointed to that position. The section also provides that directors must exercise independent discretion in a vote held by the board of directors and shall not be a party to a voting agreement. Failure to exercise independent discretion in these ways is a breach of fiduciary duty. Section 237 of the Companies Law specifies that alternate directors cannot be appointed unless this is permitted by the articles of association. Section 236 provides that, when a corporation is nominated as a director in a company, the corporation must nominate an individual to act on its behalf; the name of the individual will be registered in the company's register of directors, and the obligation applicable to a director apply to the corporation and individual jointly and severally. The Israeli authorities consider that these provisions mean that nominee directors are not allowed. Equivalent provisions apply to partnerships under the Partnership Ordinance (5735-1975), the Partnership Regulations (Registration and Fees) and Forms as the identity of a partner must be disclosed and the general partner is personally liable.

Criterion 24.13 – Sanction powers available to the ICA are applicable to failure to report information and to keep information up-to-date (including in the event that a report is rejected due to mismatches in its contents). Article 354 of the Companies Law permits the Registrar to impose a financial penalty of up to NIS 7 880 (EUR 1 841) if a company fails to comply with registration, recordkeeping and reporting obligations. The sanctions apply in respect of a failure to comply with the obligation to report changes to the information previously reported within 14 days of the change, a failure to comply with the submission of the annual report, and of a failure to comply with an order made by the registrar under section 37 of the Companies Law with regard to the shareholders registry maintained by the company if the company does not comply with its recordkeeping obligations and does not remedy any discrepancies found in its records within the timeframe set by the registrar (sections 37(b) and (c) of the Companies Law).

The same penalty can also be imposed on individual directors if the company cannot or will not pay a fine.

Under section 356(b1) of the law an additional fine can be payable for every day of non-compliance with payment of the initial fine up to a maximum of NIS 250 000 (EUR 58 431). Under s.356(c), repeated offenders could be subject to a heavier fine amount. Furthermore, the ICA can sanction companies by declaring them to be "violating companies" under section 362A of the Companies Law, a status which is publicly accessible, allows the ICA to refuse to register and release charges (which significantly limits the ability of companies to obtain credit), change the company name or purpose, and register mergers; the ICA can also deny the controlling shareholder from registering new companies. Pursuant to section 362 of the Companies Law, the ICA can seek the liquidation of a company which did not pay administrative fines. While the level of maximum financial penalties which the ICA can apply should be enhanced so as to achieve earlier compliance by companies and the power of strike-off should be added to its range of power, the ICA demonstrated that its use of sanctions has had a substantial degree of effectiveness. Also see IO.5.

The Partnerships Ordinance (ss. 9(b) and 59(b)) set out nominal fines for failure to register and file reports with the Registrar.

With reference to article 423 of the Penal Law, a founder, manager, member or officer of a corporation who registers, or causes the registration, of false information in the documents of a corporation (including in relation to the establishment of a company or partnership), with the intention of fraud, or who avoids registration of details which should have been registered, with the intention of fraud, is punishable with up to five years' imprisonment. In addition, the individuals signing the respective forms submitted to the ICA are required to declare that the details in the form are true and complete (such declaration is certified by a lawyer or CPA); according to article 239 of the Penal Law, a person who knowingly provides a false declaration is punishable with up to three years' imprisonment.

Section 53 of the Securities Law provides that a person who breaches its reporting obligation under section 37 of the law is punishable with up to two years' imprisonment or a fine of up to NIS 565 000 (EUR 132 055) where the person is an individual or a fine of up to NIS 2 825 000 (EUR 660 275) where the person is a corporation. The maximum penalty is increased to a maximum of five years' imprisonment or double the level of the fines if such breach occurred as a result of an intent to commit fraud.

Non-reporting or false reporting to the ITA in relation to beneficial ownership, where required, can be sanctioned under sections 188 (nominal civil fines), 191-191B (civil fines of 15-30% of the amount of tax avoided due to the non/false-reporting) and 215 to 218A (criminal sanctions of 1-2 years' imprisonment or a fine of up to NIS 71 300 (EUR 16 665)) of the Income Tax Ordinance. If done on purpose to evade tax, it can also be penalised under section 220 of the Income Tax Ordinance (criminal sanctions of up to 7 years' imprisonment and/or a fine of up to NIS 226 000 (EUR 52 822) or twice the amount of undeclared income), which is a predicate offence. False declarations can also be sanctioned under the Penal Law (same as declarations made to FIs and DFNBPs) or under section 3(b) of the PMLL if done on purpose to avoid AML/CTF reporting or cause false reporting (10 years imprisonment or a fine of up to NIS 4 520 000 (EUR 1 056 439)).

See also R.35.

Criterion 24.14 – All information maintained in the registries of the ICA (including basic and certain beneficial ownership information) is publicly available, including to foreign authorities. There have been no occasions where the ICA has had to facilitate access by a foreign authority.

As for the ISA, the Israeli Securities Law enables the ISA to co-operate and provide assistance to foreign securities authorities with which it has signed a MoU. Assistance is defined as including the provision of information and documents, conducting a search and/or seizure of documents, conducting investigations and the delivery of information and documents for the purposes of administering and implementing securities laws in a foreign country and for the purpose of supervising the execution of securities laws. Non-public information to a foreign securities authority, subject to certain conditions outlined in the law is also allowed under the law (sections 54K1 to 54K9). Separately, the IOSCO MMoU allows the ISA to provide company registration records on shareholders, and beneficial ownership information, to authorities in other countries.

See also R.37, R.40, and IO.2 concerning the ability of IMPA, the ITA and other LEAs and authorities to promptly provide information to foreign counterparts, including when such information should be obtained upon request.

There are no specific procedures in place which address this criterion but this is addressed by the public accessibility of the ICA's registers and mitigated in large part by the measures specified above.

Criterion 24.15 – There are no written policies or procedures specifying that Israel should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad. Though the ITA monitors the exchange of information under TIEAs, IMPA as part of its approach to meeting EGMONT procedures and best practices, as well as its own internal procedures, and the IP within the framework of joint working groups (as stated in bilateral treaties for legal assistance between countries, such monitoring of exchange does not extend to the quality of assistance received. In addition, the ICA does not monitor any of such exchange of information (including the quality of assistance received).

Weighting and Conclusion

The ML/TF risk assessments covered all types of legal persons but should be more comprehensive. The approach taken by Israel, utilising complementary mechanisms available to ensure beneficial information is available and updated in a timely manner is substantial but complete coverage cannot be certain. Coverage of nominee arrangements needs enhancement.

Recommendation 24 is rated largely compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its last MER, Israel was rated partially compliant for these requirements primarily because of the absence of any legal requirements on trust service providers to obtain, verify and retain records of the trusts they create (including beneficial ownership details).

Pursuant to the Trust Law, trusts may be created by operation of law (such trusts are not considered as express trusts), by means of a contract with a trustee or by an instrument of endowment. Trusts created by means of contract and endowment are considered to be express trusts by the Israeli

authorities. Trusts are either public trusts (i.e. a trust of which one or more of the purposes is a public purpose) or private trusts.

Criterion 25.1 –

(a) – Trustees which are bank subsidiaries, lawyers or accountants are obliged to obtain beneficial ownership information as part of their CDD obligations (s.53-57 of the Banking Directive 411, First Appendix to the BSP Order) (see c.10.5, 10.7 and R.22). Other trustees would be required to obtain details in order to make reports to the ITA (s.131(c1)) of the Income Tax Ordinance). Under the Income Tax Ordinance and the regulations made under the ordinance (which include reporting forms), information regarding the formation of any trusts by Israeli residents and the transfer of property to a trust must be reported to the ITA within 90 days. In addition, there is a transitional period of ten years in some circumstances for settlors who become Israeli resident for the first time and for veteran returning residents. This information includes the identity of the settlor, the trustee(s), the protector (if any) and the beneficiaries but not any other natural person who might exercise ultimate effective control of a trust (see also section 75p1 of the Income Tax Ordinance). There are no specific provisions dealing with trusts governed under Israeli law but having no connection with the country but in the circumstances mentioned above would be covered by transparency requirements in Israel. The Income Tax Ordinance covers settlors, trustees, protector and beneficiaries. It is not clear that the Ordinance would expressly cover other natual persons exercising ultimate effective control over a trust.

(b) – Under section 7 of the Trust Law, a trustee must maintain accounts in relation to all of the affairs of the trust, and must report to the beneficiaries annually and upon the termination of its appointment regarding the affairs of the trust. The trustee must also provide the beneficiaries with further information they may reasonably request. Under s.130 of the Income Tax Ordinance, the trustee must maintain accounting records for the trust (including any agents of and other service providers to the trust) for tax assessment purposes; registration with the ITA requires opening a bank account for the trust, which subject the trustee and the trust to CDD procedures. Although there are no specific provisions requiring that trustees must hold information on any agents of, and other service providers to, the trust, and to maintain accounting records for the trust, effectively fulfils such requirement.

(c) – Professional trustees, namely lawyers, accountants and those trust companies which are bank subsidiaries, must retain the information received as part of the CDD measures as described in R.11 and R.22. The records maintained for tax purposes must be retained by the tax payer for 7 years (section 25 of the Income Tax Regulations (Bookkeeping) although it cannot be certain that this provision covers all trusts.

Criterion 25.2 – In relation to trustees which are lawyers and accountants, the form of CDD affidavit prescribed under the respective AML/CFT Order contains a requirement for the client to update the trustee in relation to any change in the information provided. However, this is a slightly different requirement to requiring the lawyer and accountant to keep beneficial ownership information as accurate and up to date as possible. Trustees which are bank subsidiaries are required to conduct reviews in order to assure that the information is adequate and updated; however, these reviews are risk based rather than an absolute requirement to keep beneficial information as accurate and up to date as possible (s.36 of Banking Directive 411). Trustees must ensure that the information they submit to the ITA is accurate and up-to-date (section 217 of the Income Tax Ordinance).

With regard to public trusts, section 26(a) of the Trust Law requires the trustee to report any change to the name and address of the settlor and the name and address of each trustee (amongst other information) to the Registrar within three months of the change, which is not considered timely. Regulation 11 of the Endowment for Charity Purposes Regulation, 5743-1974 and Form 2 in the Annex of those regulations mandate the submission of an annual report by a charity, including financial statements. These provisions ensure that the information obtained by the Registrar of Charities, including the information regarding the trustees and public beneficiaries is accurate and up to date.

Criterion 25.3 – Israel relies on obligation under the PMLL and sectoral orders to require FIs and DNFBPs to obtain a declaration from customers (trustees) on whether they are acting for the benefit of another person before establishing a business relationship. S. 54-54 of the Banking Directive 411, s.28 of the Postal Bank Directive, s.9.3 of the ISA Circular, s.2(m) of Annex A to the CMISA Circular). The sanction for not providing this information or for providing false information is specified in s.3(b) of the PMLL.

Criterion 25.4 – There are no provisions in legislation or enforceable means preventing the disclosure of information to competent authorities or to FIs/DNFBPs relating to a trust.

Criterion 25.5 – Section 29(b) of the Trust Law expressly empowers the Registrar of Charities to instruct the trustee to provide information regarding a public trust/charity. (See R.8 for the ICA's powers as registrar of public trusts). The ICA does not have powers in relation to other express trusts. As for the ITA, it can obtain information on a person's income can be obtained by the ITA (for the purpose of the Ordinance the term "person" relates to the trustee making reports in relation to a trust); and require a professional trustee to deliver information and documents concerning its business relations even where such information and documents are not required to ascertain income. While these provisions under section 135a(a) do not apply to information or documents held by attorneys where they are bound by statute to keep such material confidential, the court rulings mentioned at c.24.8 apply in relation to lawyers acting in their capacity as trustees and the ITA is able to obtain information held by trustees and lawyers in a timely way. (S.135(1) and s.135a.(a) of the Income Tax Ordinance). See R.31 for the powers of LEAs and R.27 and 28 for the powers of supervisory authorities to obtain information and documents.

Criterion 25.6 – There are no written policies or procedures which cover sub-criteria (a) to (c) of this criterion. Nevertheless, section 214b of the Income Tax Ordinance enables the Director of Income Tax to transfer information to an authority of a foreign state in accordance with an international agreement (such as a TIEA) and upon fulfilment of conditions specified in the Ordinance (for example, that the information will be used for enforcement of tax legislation). The ITA has signed 55 TIEAs. In addition, under section 135g of the Ordinance the ITA has power to provide foreign tax authorities with information it has obtained (including information on trusts). (See also R.37 and R.40 regarding mutual legal assistance to foreign competent authorities and assistance by other authorities respectively).

Criterion 25.7– While the ICA has no administrative powers of sanction in relation to public trusts and their trustees, it may apply to the court in order to replace the trustee or request other measure be taken with regard to the public trust/charity (s.39 of the Trust Law). This allows Israel to ensure that trustee are held legally liable for failure to provide the duties relevant to meeting their obligations (see R.8).

In relation to the provision of false or misleading information by public trustees to the registrar, a person intentionally breaching an obligation under a law, by act or omission, and such matter is of public interest, is punishable with up to two years' imprisonment (s.61 and 286 of the Penal Law). (See c.8.4 for penalties in relation to public trustees and the ICA.) Section 61 of the Penal Law permits the court to impose the following penalties: if the offence is punishable with imprisonment of up to six months or only a fine, or a fine of an undetermined amount – a fine of up to NIS 14 400; if the offence is punishable with imprisonment of more than six months but not more than a year – a fine of up to NIS 29 200; if the offence is punishable with imprisonment of more than a year but not more than three years – a fine of up to NIS 75 300.

Trustees are in addition subject to fiduciary obligations, which are subject to civil liability (s.10-13 of the Trust Law).

Civil and criminal fines with respect to non-compliance with obligations (ranging from NIS 200 to (EUR 47) 30% of deficit sum, a fine or up to two years' imprisonment for providing false or misleading information to the ITA, a penalty of up to seven years' imprisonment or a where there is intent to avoid payment of tax are available to the ITA. (S.188-192a, 217, and 220 of the Income Tax Ordinance).

Trustees who are lawyers, accountants, and bank subsidiaries are subject to the criminal, administrative and disciplinary sanctions of the PMLL for failures in relation to maintenance of beneficial ownership information and record keeping. (See R.35.)

Trustees who submit false information to FIs or DNFBPs in the course of CDD procedures are subject to the criminal sanctions (s.3(b) of the PMLL).

A penalty of up to five years' imprisonment in relation to the false entry of information in the documents of a body corporate is also available (s. 423 of the CC).

Criterion 25.8 – Only administrative fines (of up to a high level of fine of NIS 2 260 000 (EUR 528 000)) are provided for under the PMLL in relation to failure to grant to competent authorities timely access to information regarding the trust referred to in c.25.1. The same applies to other FIs, including trustees which are bank subsidiaries. There are however no other dissuasive and proportionate sanctions such as civil or criminal provided under the PMLL.

Israel is also able to rely on sanctions available in other laws: failure to provide information to the ITA is subject to up to one year's imprisonment or a fine of NIS 29 200 (EUR 6 820) or both; and a trustee of a public trust is liable to a maximum of a year's imprisonment or a nominal fine if he does not submit the reports to the registrar. Fraud is an offence subject to a maximum term of imprisonment of two years. (S.215 of the Income Tax Ordinance and s.31 of the Trust Law).

Weighting and Conclusion

Israel meets or mostly meets nearly all the criteria for Recommendation 25. However, there are shortcomings in relation to holding accurate and current information, sanctions, and absence of written policies or procedures on international co-operation. **Recommendation 25 is rated largely compliant.**

Recommendation 26 – Regulation and supervision of financial institutions

In its last MER, Israel was rated partially compliant for these requirements. The main technical deficiencies related to an absence of mechanism for ensuring consistency for appropriate and sufficient level of supervision among the entire financial sector, as well as insufficient evidence of effective supervision in MSBs and the Postal Bank.

Criterion 26.1 – The following institutions are required to regulate and supervise the AML/CFT compliance of the financial entities covered by the AML/CFT legislation (s.11M(a) of and Schedule 3 to the PMLL, s.95(c) and (d) of the CTL)[55]

- Bank of Israel for banks, credit card, bank trust companies, foreign banks, mortgage banks, investment financing banks, business promotion banks or joint services companies, acquirers or auxiliary corporations engaging in the operations of acceptance of deposits and other repayable funds from the public; issuing and managing means of payment; trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities, and commodity futures trading; securities related financial services; individual and collective portfolio management; safekeeping and administration of cash of liquid securities on behalf of other persons; investing, administering or managing funds or money on behalf of other persons, underwriting and placement of life insurance and other investment related insurance; money and currency changing/MVTS services (s.11M(a)(1) of the PMLL and s.1, 10 and 361 of the Banking (Licensing) Law));
- Israel Security Authority (ISA) for securities-related services including exchange members, trading platforms and portfolio managers) (s.11M(a)(2) of the PMLL);
- Capital Markets, Insurance and Savings Authority (CMISA) for insurers and insurance agents engaging in underwriting and placement of life insurance and other investment related insurance, provident funds and non-bank lending services offered by credit service providers (s.11M(a)(3), s.11M(a)(4) and s.11M(a)(6a) of the PMLL, s.2(a) of the SFSL);
- Ministry of Communication for Postal Bank engaging in the operations of acceptance of deposits, transferring monies by monetary and postal checks, and MVTS services provided by the Postal Bank (s.11M(a)(5) of the PMLL and s.88A of the Postal Law);
- Registrar of Money Service Business Providers (and CMISA from 1 January 2018) for money services providers engaging in the operations of money and currency changing; managing travellers cheques; and non-bank credit service providers (s.11(c)(a) and 11M(a)(6) of the PMLL);

Criterion 26.2 – Core principles FIs in Israel include banks, stock exchange members, and insurance companies. All of them are subject to licensing obligations:

Core Principles FIs

- Banks, foreign banks, mortgage banks, investment financing banks, business promotion banks or joint services companies: s.3 and 4 of the Banking (Licensing) Law;
- Stock Exchange Members for trading in the Tel Aviv Stock Exchange: s.45, 45A, 45B, 46 and 48 of the Securities Law;
- Insurers: s.14 of the Control of Financial Services (Insurance) Law, 5741-1981;

55. The Counter-terrorism Law, 5766-2016

Other FIs

- Trading Platforms: s.44M of the Securities Law;
- Portfolio Managers: s.8 of Investment Advice Laws;
- Provident fund managing companies: s.4 of the Control of Financial Services (Provident Funds) Law, 5765-2005;
- Postal Bank: s.5A of the Postal Law.

All MSBs[56] stipulated under s.11C of the PMLL, including MVTS, are required to register in the MSB registry.

Implementation of the licensing regime by the BoI ensures that the country does not approve the establishment, or continued operation, of shell banks.

Criterion 26.3 – There are the necessary measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution. Fit-and-proper tests (including assessment elements such as integrity, eligibility, professional experience, liquidity position, and presence of any criminal records) apply to the management and supervisory boards, as well as people holding a qualified shareholding, including when changes occur after obtaining the licence to FIs as follows:

- Banking corporations: When issuing a licence, BoI must first review the 'suitability' of directors, managers and those who are holding 'means of control' (s.6(2) of the Banking (Licensing) Law). The Banking Ordinance provides for examples of applicant's integrity and eligibility (e.g. existence criminal convictions or history of being associated in the management of a banking corporation that was liquidated by court). Ultimate owners (including shareholders with an ownership interest of 5 percent or more) and those who hold interest indirectly are subject to a "fit-and-proper" procedure: s.6, 34(a), 34(b) and 34A(c) Banking Law, s.11, 11(a) Banking Ordinance, s.4 Proper Conduct of Banking Business 301. The Banking Supervision Department of BoI conducts the "fit-and-proper" process prior to the appointment of an officeholder[57]. This process involves the review of the applicant's business experience, integrity and honesty. Regarding significant or controlling interest, a person cannot own more than 5% of a certain type of controlling measures in a banking corporation or in a bank holding corporation, unless the Governor issued a permit (see s.34(a) of the Banking (Licensing) Law). The requirements of the Banking (Licensing) Law (s.6) also apply before such permit is issued.
- Securities sector:
    - Stock Exchange Members*:* Controlling[58] persons, stakeholders, or senior managers in a non-bank TASE member seeking TASE membership will undergo a review of their

56. All MSBs are expected to obtain a license according to the Supervision of Financial Services Businesses Law by October 2018.
57. S.11A(h) of the Banking Ordinance defines the term "officer" in a bank "as: a director, a general manager, an internal auditor and general counsel, and a person whom the Supervisor determines.
58. The Securities Law defines "control" as the power to direct the activity of a corporation, with the exception of a power that emanates solely from performing the function of a director or another position in the corporation. It is assumed that person controls a corporation if she/she holds half or more of the voting rights in the general assembly or has the power to appoint directors or the general manager.

reputation, including a screening for any criminal convictions involving moral turpitude (see s.5(a)(1) and 6(b)(1) of the TASE regulations). Membership can be revoked if such conviction occurs after granting of membership (s.78(h) ibid.). If the non-bank TASE member is a company that is not listed on the TASE, there is an obligation on the member to inform TASE of the true owners, of theirs shares and of any changes in its shareholdings (s.6(c) of the Stock Exchange regulations). Stock Exchange Members that belong to larger groups (i.e. an investment house -with shared management and control structure- engaged in trust fund or portfolio management) are also subject to a review of reliability of their controlling shareholders and senior officers (s.9, 9A, 10A, 13, 13A, 23B and 23D of the Joint Investment Law; s.10 and 27 of the Investment Advice Law).

- Trading platforms: Similarly, the Securities Law requires the review of the "reliability" of a trading platform, and of its officeholder or controlling shareholder, before the issuance of a licence (s.44M(c)). The ISA Chairman can suspend or revoke the licence if a deficiency in the reliability of the company (or its shareholders) is identified. ISA published a list[59] of circumstances for evaluating a possible deficiency in the reliability, such as: criminal conviction, indictment or conduct of a criminal investigation in connection with the commission of an offence under the Securities Law or another economic offence (incl. theft, bribery, counterfeiting, and fraud).
- Portfolio managers: a licence will not be issued in case of conviction for an offence under the PMLL, the Securities Law, the Companies Ordinance, the Companies Law, the Banking Law, etc. (s.8 of the Investment Advice Law). ISA can refuse to issue a license to a company if one of the officeholders or controlling shareholders fails the fit-and-proper test (s.8(c)(2) ibid). ISA can similarly revoke or suspend a license of someone that no longer complies with the terms of the license (s.10 ibid.).

- Insurance / provident funds: A person cannot acquire more than five percent of the controlling means in an insurance company or provident fund, without obtaining a permit from CMISA (s.31 of the Insurance Law (IL); s.9 of the Provident Funds Law (PFL)). Before issuing such a permit, CMISA will review the applicant's integrity and whether there is any criminal conviction, civil or disciplinary records (as per rules laid down in the CMISA Control Policy Document (2014)). An applicant company must attach documents regarding its officeholders and controlling persons, including their financial history and financial assets (s.16(a) of the IL; s.5(a) of the PFL). CMISA will conduct fit-and-proper tests of officeholders and controlling person (considerations to be taken into account are listed in s.17(a) of the IL; s.4(b) of the PFL). Prior appointment of an officer, director, general manager requires the approval by the CMISA, and the review of the applicant's background and integrity (s.41J of the IL; s.10 of the PFL).
- MSBs: S.11E of the PMLL sets up the conditions for the registration of an applicant MSB (e.g. criminal convictions or previously imposed financial sanctions under PMLL). The "applicant for registration" is defined to include the beneficiary (s.11E(4)(3)). Criminal records are also verified prior to the appointment of a senior office in a MSB providing non-bank lending services (s.31 of the SFSL). The SFSL also sets up strict fit-and-proper requirements for a non-bank financial instruments service providers and credit providers applying for a license (s.15 for a standard license and 16 for an extended license). Similar requirements are in place for deposit and credit services providers (s.25E and 25F for standard and extended licences

59. www.isa.gov.il/sites/ISAEng/1489/staff%20positions/Documents/26102015list.pdf

respectively). The fit-and-proper process covers officeholders, controlling persons and beneficial owners. Licences may be revoked in case of breach to the SFSL (s.23, 25I, 25M, 25O).

- Credit Service Providers: The SFSL establishes fit-and-proper requirements that must be met as a requisite for receiving a licence (s.15 and 16 for a standard and extended licence respectively) including that the applicant or any controlling person has not been convicted of an offence which deems him unsuitable to engage in the provision of such services. The section determines a list of specific offences in this regard. The sections also include the obligation to examine whether all applicant's officeholders, controlling persons and beneficial owners have met the conditions necessary in order to receive a permit or receive their appointment (chapters 4 and 5 of the Law for Controlling Persons and Beneficial Owners; and officeholders respectively). Under section 23 of the law the supervisor may revoke or suspend a licence for any of the circumstances specified, including if it has become apparent that the applicant submitted false information in order to obtain his licence or if he breeched any requirement under the SFSL.
- Postal Bank: The board of directors is appointed by the Postal Company (a governmental company), with the approval of the Minister of Finance and Minister of Communication (s.18(a) of the Government Companies Law). As supervisor, the Minister of Communication (MoC) is responsible for the licensing of ownership and the approval of senior officers. The MoC also determines the conditions for the holding, transferring or purchasing of control (s.1b(f) of the Postal Law). MoC's approval is needed for holding/transferring/purchasing of control means from 5% upwards. Managerial positions (incl. board of directors, senior officers), in addition to undertaking a fit-and-proper test, must be also granted a security clearance by *Shin-Bet*.

Criterion 26.4 –

Core principles institutions: The banking, securities, insurance sectors are regulated in line with the principles set by the BCBS, IOSCO and IAIS where relevant for AML/CFT.[60] In addition, banks are subject to consolidated group supervision for AML/CFT purposes under the Basel III framework.

All other FIs: All other FIs under the supervision of BoI, ISA, and CMISA (for provident funds and credit service providers) are under the same regime as core principles institutions. MSBs are subject to national AML/CFT requirements under the PMLL and the sectoral order: s.7, chapters 4A and 5 of the PMLL.

Criterion 26.5 –There are no specific provisions on the requirements under this criterion in Israeli laws and other enforceable insturments. In practice, the frequency and intensity of on-site and off-site AML/CFT supervision of FIs or groups is only partly done on the basis of:

a) the ML/TF risks and policies, internal controls and procedures associated with the instition or group, as identified by the supervisor's assessment of the instition's or group's risk profile;

60. Detailed Assessment of Observance of International Association of Insurance Supervisors Insurance Core Principles in Israel: https://www.imf.org/external/pubs/ft/scr/2012/cr1284.pdf; Financial System Stability Assessment: http://www.imf.org/en/Publications/CR/Issues/2016/12/31/Israel-Financial-System-Stability-Assessment-25815; Assessment of IOSCO Objectives and Principles of Securities Regulation : https://www.imf.org/external/pubs/ft/scr/2012/cr1287.pdf

b) the ML/TF risks present in the country; and

c) the characteristics of FIs or groups, in particular the diversity and number of FIs and degree of discretion allowed to them under the risk-based approach.

Criterion 26.6 – Banks and insurers are required to report their ML/TF risk profiles to BoI and CMISA on a semi-annual basis. There are no specific obligations requiring other supervisors to review the risk-based approach adopted by stock exchange members, trading platforms, portfolio managers, credit service providers and MSBs periodically, and when there are major events or developments in the maangement and operations of the covered FI/group. (Banking Directive 411 and Directive 825 and s.2(b)(6)(f) of the Insurers Circular).

Weighting and Conclusion

Israel fully meets the most important criteria in Recommendation 26 in relation to market entry and supervisory responsibility. However there are some gaps in relation to the regulation and supervision of FIs. In particular, the frequency and intensity of on-site and off-site AML/CFT supervision of FIs is only partly based on risks. There are also no requirements for supervisors to review the risk-based approach adopted by FIs regularly.

Recommendation 26 is rated largely compliant.

Recommendation 27 – Powers of supervisors

In the previous evaluation, Israel was rated compliant under the former requirements in this area.. The new R.27 extends the range of disciplinary and financial sanctions powers which supervisors should have, including the power to withdraw the licences of FIs.

Criteria 27.1 and 27.2 – Supervisors are provided with powers to supervise and ensure compliance by FIs with AML/CFT requirements, including powers to demand and seize information and conduct inspections, either with or without a warrant (s.11M, 11M1(a), 11N of the PMLL). Supervisors are also allowed to exercise the general supervisory powers under respective sectoral ordinances for AML/CFT purposes (s.11N(d) of the PMLL, s.5 of the Banking Ordinance, s.44T, 56A1 and 56F of the Securities Law, s.29 of the Investment Advice Law, s.49C to 50 of the Insurance Law, s.88M of the Postal Law, and s.67, 68 and 70 of the Supervision of Financial Services Law (Regulated Financial Services) 5776-2016).

Criterion 27.3 – Supervisors have broad powers to request documents and information for monitoring only FIs' AML/CFT compliance purposes without a court order, so long as the premises concerned are not used exclusively for residential purposes (s.11N(b) to (d) of the PMLL). In addition, the general supervisory powers under respective sectoral laws and regulations mentioned under c.27.1 and c.27.2 are also applicable.

Criterion 27.4 – Supervisors are provided with administrative sanction tools against AML/CFT non-compliance under the PMLL. For example, they are empowered to impose financial sanctions up to NIS 2 260 000 (approx. EUR 528 000) for non-compliance with AML/CFT-related requirements. The power to determine and impose such sanctions (including level of fines) is subject to the decision of a three-member committee with representatives from the supervisor (the chairperson), responsible policy ministry, and Ministry of Justice. (s.12 to 20 of the PMLL and s.95 of the CTL). Supervisors use their general sanction powers (e.g. revoking or suspending of licence) provided under respective sectoral laws and regulations for AML/CFT purposes, instead of through the PMLL. The sectoral laws and regulations separately provide for a range of administrative, criminal, and civil sanctions. (s.8A,

8C, 8E, 15(a)(2)(a) and 14H of the Banking Ordinance; s.44M(3) and 44Wof the Securities Law, s.8(A)(3), 8(B)(3), 10 and chapter G of the Investment Advice Law; s.18, 22 of the Insurance law; s.23, 25I and chapter 12 of the SFSL; s.12 and 109 of the Postal Law). See also c.35.1 for additional analysis on criminal sanctions powers against FIs.

Weighting and Conclusion

Recommendation 27 is rated compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its last MER, Israel was rated NC as there were no AML/CFT obligations on DNFBPs and therefore no compliance monitoring systems in relation to real estate agents, dealers in precious stones, trust and company services providers, lawyers, notaries, other independent legal professionals and accountants. To some extent, measures taken comprise the inclusion within the law of BSPs encompassing lawyers and accountants and dealers in precious stones for AML/CFT purposes along with provisions for supervision.

Criterion 28.1 – As mentioned under c.22.1, casinos are illegal in Israel. This criterion is therefore not applicable.

Criteria 28.2 and 28.3 – For DNFBPs that are subject to AML/CFT compliance, competent authorities have been designated as follows:

- *Lawyers and accountants providing the services covered in Recommendation 22* (or Business Service Providers (BSPs) as referred in Israeli laws): Ministry of Justice (s.11M(a)(9) and 11M1.(a) of the PMLL; and
- *Dealers in Precious Stones*: Ministry of Economy and Industry (MoE) (s.11M(a)(8) of the PMLL).

DNFBPs without AML/CFT regulation and supervision include real estate agents, dealers in precious metals and TCSP that are also not lawyers or accountants. There are no provisions specifying that these DNFBPs should be subject to AML/CFT regulation and supervision, or that a competent authority or self-regulatory body (SRB) should be designated for AML/CFT purposes.

Criterion 28.4 –

a) Supervisors for covered DNFBPs (i.e. MoJ & MoE) have specific powers to conduct supervisory/monitoring functions for AML/CFT purposes (e.g. on-site and off-site inspections): s.11M(a)(8), 11M(a)(9), 11N(b) of the PMLL and the relevant sectoral orders. In addition, supervisors for lawyers and accountants providing TCSP services are provided with power to request information (e.g. personal information, including the ID, addresses and other contact details of lawyers/accountants or any decisions regarding the suspension or revocation of their license or registration) from the SRBs (i.e. the Bar Association and the Accountants Council): s.11M1.(a) of the PMLL.

b) Measures to prevent criminals or their associates from being professionally accredited or holding a management function in a DNFBP apply to:

- *Lawyers and accountants providing TCSP services*: the Bar Association is empowered to refuse membership of an applicant, or suspend, temporarily suspend or cancel a licence of a member of the Bar under various conditions, e.g. conviction of a criminal offence, member has been sentenced in a disciplinary court or suspension, member has been declared bankrupt (s.44, 47, 48, 49 and 78 of the Bar Association Law). As for accountants, the law enables the Council

of Certified Public Accountants to refuse to grant a licence to an applicant if the Council considers the applicant is unfit to act as an auditor in regard to his character (s.4(b) of the Auditors Law); and

- *Dealers in precious stones:* the Diamond Industry Supervisor, who is the head of the diamond administration in the Ministry of Economy and Industry, is responsible for granting written business licences or one-time permit for dealing in diamonds, and may set licensing conditions (s.2 of the Control of Diamonds, their Import and Export Order, 5739-1979).

c) Supervisors (MoJ in respect of BSPs and MoE in respect of Dealers in Precious Stones) have the power to impose financial sanctions up to NIS 2 260 000 (approx. EUR 528 000) for non-compliance with AML/CFT-related requirements (s.12 to 20 of the PMLL; analysis under c.27.4 is also applicable). Furthermore, the Bar Association and the Accountants Council may issue disciplinary rules where the performance of a transaction constitutes a high-risk activity for ML/TF (s.44A and 44B of the Lawyers Disciplinary Rule and s.15 of the Accountants Disciplinary Rule). A lawyer or accountant who violates these professional rules may be subject to disciplinary sanctions including the suspension or revocation of a licence. If the Supervisor suspects that a BSP has breached the abovementioned Disciplinary rules, the Supervisor may notify the Bar Association or the Accountants/Auditors Council and request the initiation of a disciplinary procedure against the BSP in question (s.11M1 of the PMLL). See also c.35.1 for additional analysis/other deficiencies.

Criteria 28.5 – There is no specific provision in Israeli laws stipulating that supervision of DNFBPs should be performed on a risk-sensitive basis. That said, supervisors of BSPs and dealers in precious stones have taken limited steps to perform AML/CFT supervision (e.g. on-site/off-site inspections) on a risk basis.

Weighting and Conclusion

Covered DNFBPs (lawyers, accountants, and dealers in precious stones) have designated competent authorities responsible for monitoring and ensuring compliance with AML/CFT requirements. They also have the necessary powers to perform their functions and monitor compliance, and take measures to prevent criminals or their associates from owning or controlling such entities. The supervisors partly take into account the risk-based approach. Real estate agents, dealers in precious metals, and TCSPs are not covered for AML/CFT.

Recommendation 28 is rated partially compliant.

Recommendation 29 - Financial intelligence units

In its previous assessment, Israel was rated compliant with former Recommendation 26.

Criterion 29.1 – The Israel Money Laundering and Terror Financing Prohibition Authority (IMPA) serves as the designated FIU for Israel (s.29(a) of the PMLL). IMPA is responsible for the management and maintenance of a database of reports received under the PMLL and the CTL. As such, IMPA receives reports from obliged entities, centralises, analyses and disseminates the disclosure of both CTRs and UARs, information from other sources and the results of the analysis.

Criterion 29.2 –

(a) IMPA receives unusual activity reports (UARs) on transactions that the reporting entities deem to be unusual or that they believe or suspect are related to ML/TF activity (s.7(a)(2), 8A(a)(2) of the PMLL and relevant AML/CFT Orders – see R. 20 and 23).

(b) Under the PMLL and the Orders, IMPA also receives currency transaction reports (CTRs) from banking corporations, insurers, insurance companies, provident funds, MSBs, Postal Bank and TASE members. The subject of the reports from the banking corporations may be cash transactions, deposits, issuance of bank cheques, purchase of travellers' cheques or overseas wire transfers (s.7 PMLL and the Banking Corporation Order), and cash transactions from the dealers in precious stones (s.8A(a)2 PMLL and the Dealers in Precious Stones Prohibition of Money Order).

Criterion 29.3 –

(a) IMPA is authorised to request additional information from any reporting entities as needed to complete a report received in its database, or which is connected with such a report and relates to a person in relation to whom the report was received (s.31(c) PMLL).

(b) IMPA has direct and indirect access to various databases and information sources which include financial, banking, tax, administrative and law enforcement information (incl. intelligence, customs), the criminal registry as well as government and private database and open sources. Since 2013 IMPA also has a designated, permanently based police officer working on premises with direct access to intelligence maintained in the police database.

Criterion 29.4 –

(a) IMPA conducts reactive and proactive operational analysis. The analysis is conducted using IMPA's electronic information processing system called "Black and White" (B&W DPS), which stores UARs, CTRs, cross-border declarations and enriched information gathered from government, commercial or public sources. The system is based on two sub-systems: 1) Collection and data entry sub-system, and 2) a Case Management Tactical and Strategic Analytical sub-system that supports the monitoring, collation, analysis and dissemination of financial intelligence to law enforcement, security agencies and information sharing with FIUs.

IMPA conducts operational analysis by using available and obtainable information to provide intelligence on specific targets, identify ML/TF patterns and indicators, predicate offences, and identify assets for seizure and confiscation.

(b) IMPA has a dedicated section for strategic analysis staffed with expert analysts and equipped with supporting IT tools. Different types of strategic analysis are conducted by IMPA, including the development of red flags, ML/TF-related trends, patterns, and typologies. These typologies and indicators are then monthly disseminated within IMPA, and otherwise used to support other functions (such as providing feedback and outreach to reporting entities).

Criterion 29.5 – IMPA disseminates financial information and intelligence from its database only in accordance with section 30 of the PMLL. As such, the PMLL authorises IMPA to disseminate information upon request to the Israel Police (s.30(b)(1)), the tax authority (s.30(b1)) and all Security Agencies (s.30(c) and (c1)), when there are grounds to suspect ML and FT. IMPA is also authorised to spontaneously disseminate information from the database to competent authorities under the law (s.30(e)).

This information is delivered via protected and secured channels, as per s.7-11 of the Money Laundering Regulations (2002), which set up the rules for the use of secure and protected channels for the safe dissemination of the information).

Criterion 29.6 – IMPA protects the information it holds in accordance with the law, as follows:

(a) Specific data protection regulations were enacted under the PMLL – (*Rules for Conduct of Data Base and Protection of Information Therein*) in 2002. IMPA is subject to security instructions from the Information Protection Department at the National Security Authority. In addition, IMPA has detailed written procedures regarding security of information.

(b) IMPA staff are required to obtain security clearances from the National Security Authority and from the Inspector General of the INP (s.29(c)) before accessing IMPA's database. Employees are also subject to a strict screening procedure before their employment. The law also requires IMPA's staff to maintain confidentiality of information (s.31A(a)). Failure to do so is punishable by up to three years imprisonments or a fine. All staff receive security refresher training at least every 12 months to reinforce and recall their understanding on information security and data protection procedures.

(c) Access to the information in the databases is granted only to IMPA's employees that have been authorised by the Head of IMPA and cleared by the Inspector General of the INP (s.29(d) PMLL). IMPA developed procedures and guidelines for ensuring the security of all of its facilities. Premises are secured (incl. visual monitoring) and physical access is limited to appropriately authorised officers.

Criterion 29.7 –

(a) IMPA is established by law as part of the MOJ and separately funded by the State budget. IMPA is the only body that collects, analyses and disseminates reports received from reporting entities. As such, it operates as an autonomous body, free of any adverse influence and independent in its operations and decision-making. According to an Israeli government decision, the head of IMPA is appointed by the Minister of Justice (s.29(a) of the PMLL), on the basis of a suggestion by a professional (non-political) search committee that includes a public representative. This person must have the prerequisite qualification of a district court judge in addition to other qualifications determined by the MoJ, and as specified in PMLL Regulations (*Qualifications of the Head of the Assigned Authority*).

(b) Sections 30 and 31 of the PMLL enable IMPA to exchange information directly with the INP, ITA and security agencies under the conditions stipulated. ISA cannot obtain information directly from IMPA, instead must go through the INP. IMPA may both initiate the exchange and do so upon request. IMPA can exchange information directly with a foreign counterpart FIU (s.30(f)). IMPA may also independently sign MOUs with counterpart FIUs.

(c) As the only authority in charge of receiving, analysing and disseminating reports to domestic competent authorities and foreign counterparts, IMPA has distinct core functions from those of the MOJ (see c.29.7(a)).

(d) IMPA has a distinct budget under the MOJ budget, and is able to obtain and deploy the resources needed to carry out its functions. Rules are in place to ensure that IMPA's employees are operating independently and without undue influence (i.e. Civil Service (discipline) Law and Regulation (Chapter 42-43); Civil Service Regulation and Rules of Ethics for State Employees 5769-2008).

Criterion 29.8 – IMPA is a member of the Egmont Group since 2002.

Weighting and Conclusion

Recommendation 29 is rated compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Israel was rated largely compliant for these requirements in Israel's last MER, only due to effectiveness.

Criterion 30.1 – The Israeli National Police (INP) is the primary law enforcement agency with the responsibility of investigating ML/TF and predicate offences. The Financial Enforcement Unit (FEU) (in the Department of Investigations and Intelligence of the INP) is comprised of several specialised units, including: an asset forfeiture unit, a ML/TF squad, a financial analysis unit, a FIU Unit (which acts as liaison within the INP, with ITA and IMPA) and a Special Intelligence Team (SIT) (recently established to deal with the analysis of financial documents). In particular, the ML/TF Squad is in charge of the identification of ML/TF cases and the investigation of large scale ML cases. The FEU also operates in the eight districts of Israel, in the Israel Border Police and in the *Lahav* 433 Unit (which reviews all districts cases to determine whether it should be subject to financial enforcement). The *Shin-Bet*, the national authority designated for safeguarding national security in Israel, also conducts terrorism and TF investigations.

There are also specialised authorities in charge of investigating certain ML-related offences. The Israeli Tax Authority (ITA) conducts ML investigations connected to predicate offences under the Customs Ordinance, VAT law, Income Tax Ordinance and Land Taxation Law (e.g. cross-border transportation of cash). The Israel Securities Authority (ISA) deals with complex financial investigation cases (e.g. trading and securities fraud).

Criterion 30.2 – LEAs are authorised to investigate ML/TF offences during a parallel financial investigation where the predicate offence(s) occurred in Israel or is in connection with Israel (s.3 of the National Police Ordinance; s.12 – 13 of the Criminal Code). This can be done within the framework of a Joint Investigation Team (JIT). ITA and ISA also conduct parallel financial investigations (SOP 03.300.606).

Criterion 30.3 – Within the INP, the FEU has a dedicated unit dealing with asset forfeiture (see c.30.1). This Forfeiture Unit oversees the nine Financial Enforcement Teams (FET) operating in the eight districts of Israel, the Border Police and the *Lahav* 433 Unit (see Chapter 1). Each district's financial enforcement team is responsible for the financial enforcement and ML matters occurring in the districts. FET officers, regardless of their duty station, are trained to detect, identify, seize and freeze criminal proceeds, as part of the general training on how to conduct proactive and reactive financial enforcement operations. FET officers can freeze property immediately (with the appropriate court warrant) in response to domestic and international requests (s.39 CPO; s.21-22 PMLL; Chapter 5 of the CTL, s.34 DDO; s.6 ILAL). The INP is also authorised to request IMPA to identify and locate assets, both in Israel and oversees, that are related to a suspect (s.30B of the PMLL).

Criterion 30.4 – As indicated in c.30.1, there are two other authorities, not LEAs *per se*, in charge of ML investigations. ITA is responsible for direct and indirect tax systems and tax monitoring, but it also has the authority to investigate ML offences connected to tax offences (as per the First Appendix to the PMLL). ITA has a dedicated unit (the *Yahalom* unit) in charge *inter alia* of ML or TF investigation and intelligence. Similarly, ISA also acts as an investigatory enforcement authority (in addition to its supervisory role in relation to securities).

Criterion 30.5 – While there is no specialised independent anti-corruption body in Israel, there are a number of anti-corruption units in place within the INP which are dealing with fraud and corruption matters (e.g. the *Yacha* is the National Fraud Investigations Unit in charge of exposing public corruption and *Yalac* is the National Financial Investigation Unit responsible for corruption). Within these units there are designated task forces comprised of representatives from INP, ITA, IMPA and SAO that investigate complex ML matters, including asset forfeiture. Assistance from other enforcement units of the FEU is possible during investigations. In addition, Israel has a number of specialised bodies and authorities dealing with the implementation of anti-corruptions measures (e.g. State Comptroller's Office, the Civil Service Commission, the State Control Committee (*Knesset*), the Ethics Committee (*Knesset*) and several units and divisions within the MoJ).

Weighting and Conclusion

Recommendation 30 is rated compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

Israel was previously rated compliant for R.28 (the predecessor to R.31).

Criterion 31.1 – Competent LEAs conducting investigations of ML, TF, and predicate offences are empowered exercise a variety of investigative powers, often requiring a court order, which include:

Production of records – There is no dedicated provision granting LEAs powers to request records and information from FIs, DNFBPs and natural or legal persons covered by the PMLL. These are derived from general rules set in s.43 of the Criminal Procedure Ordinance (CPO), which stipulates that a judge can summon the production of "any object" needed for purpose of investigation or trial. ISA and ITA are also empowered power to gather evidence (ISA: 56C of the Securities Law; ITA: s.108 and 109 of the VAT Law, s.140 of the Income Tax Ordinance and s.186 of the Custom Ordinance). Similarly, the generic power to receive and collect information is granted to the *Shin-Bet* for the conduct of TF investigations (s.8(a)(1) of the *Shin-Bet* Law).

Search of persons and premises – The PMLL enables LEAs (i.e. police and customs officers) to use the same search and seizure powers as provided in the CPO (s.26 and 27 of the PMLL). INP can conduct search of persons and premises (including of the non-suspect), provided a search warrant has been obtained before. Search of persons is possible before and after arrest (s.29 and 22 of the CPO), where there is reasonable ground to suspect that person is concealing evidence. Search can be conducted without a warrant in some cases provided in s.25 of the CPO (e.g. reasonable ground to believe a felony is being committed). Similar powers to search persons are given to ISA (s.56B(c), 56C(3)(a) and 56C(1)(b) of the Securities Law), ITA (s.109 VAT Law, s.184 and 187 of the Customs Ordinance, s.227 of the Income Tax Ordinance and s.26 and 27 of the PMLL) and the *Shin-Bet* (s.8(b) and 10 of the *Shin-Bet* Law). ISA also has the power to search of non-residential premises even without a search warrant (s.56B(b)(2) of the Securities Law).

Taking witness statements – INP, ITA, ISA and *Shin-Bet* all have the power to take witness statements (INP: s.2(2) of the CPO; ITA; s.109(a)(3) of the VTA Law, s.186 of the Customs Ordinance, s.227 of the Income Tax Ordinance; ISA: s.56C of the Securities Law and *Shin-Bet*: s.8(a)(3) of the *Shin-Be*t Law).

Seizing and obtaining evidence – The PMLL enables LEAs to seize proceeds of crime and terrorists assets. Seizure is possible before the beginning of the legal proceedings (s.26 of the PMLL). These powers are given to police and customs officers as well (s.27 of the PMLL). The CPO also provides a wide range of seizure powers, especially if it is likely that the item seized will serve as evidence in a legal proceeding (s.32 CPO). Under this provision, it is also possible to seize information from computers. ISA investigators also have the power to seize objects connected with the offence, during a search (s.56C of the Securities Law) or seize evidence during an investigation, even temporarily (s.56B(c)). Same applies to ITA (s.109 of the VAT law, s.186 of the Customs ordinance and s.27(b) of the PMLL) and *Shin-Bet* (s.8(b) of the *Shin-Bet* Law).

Criterion 31.2 – . LEAs (INP, ITA, ISA and *Shin-Bet*) benefit from a wide range of special investigative powers for the purpose of gathering evidence:

(a) Competent authorities can conduct undercover operations, such as ITA (s.108 of the VAT Law, s.135-141(b) and s.214 of the Income Tax Ordinance and s.30 of the PMLL) and *Shin-Bet* (s.10 *Shin-Bet* Law) INP officers can conduct any type of investigation upon suspicion of an offence (s.3 of the Police Ordinance and s.59 of the Criminal Procedure Law). This includes undercover investigations. There are other references to undercover operations in other laws (e.g. s.2B and 6 of the Wiretapping Law, and in different procedures on the use of undercover agents, use of intelligence and special covert investigations).

(b) and (c) Upon a (special investigation) court order, LEAs can intercept communications, conduct surveillance, and access computer data. These powers are set out in specialised laws (c.31.2 a: Wiretapping Law and c.31.2 b: Electronic Surveillance Law) but also more generally provided in the Criminal Procedure Ordinance, and the various laws regulating these agencies (Securities Law, Income Tax Law, *Shin-Bet* Law). Some powers can be used without a court in in case of emergency (e.g. for wiretapping – s.7 of the Electronic Surveillance Law).

(d) There is no specific legislation empowering LEAs to conduct controlled deliveries. Israeli authorities rely on the 1961 and 1988 UN Conventions. LEAs' powers to conduct controlled deliveries are an inherent part of their search, seizure and investigation powers (see c.31.2b). The prior approval of the district attorney is required. There are also procedures in place for controlled delivery for drug cases in the airport premises.

Criterion 31.3 – There are a number of mechanisms through which LEAs can identify whether natural or legal persons hold or control accounts, none of which require prior notification to the owner. As indicated above, INP and ITA can compel the production of any financial statement (s.43 of the CPO). MIVZAK is a digital system recently developed that can be used to compel FIs to produce information pertaining to bank accounts, including all owners registered on the account. LEAs have also the technological tools and access to a wide variety of databases, including open public registers (e.g. Registrar of Pledges, Land Registration Office). Police can also receive information on bank accounts and controlling persons or legal entities from IMPA, ITA and regulators (e.g. Companies Register). In addition to banks, ISA officers may also require information from Stock Exchange Members (s.56A and 56C of the Securities Law). The same applies for *Shin-Bet* (s.8 of the *Shin-Bet* Law).

Criterion 31.4 – LEAs (INP, ITA and *Shin-Bet*) investigating ML, TF, and associated predicate offences can receive all relevant information held by IMPA, both upon request and on IMPA's initiative (s.30 of the PMLL). This information, once received, can also be circulated to ISA for the

investigation of securities-related offences (S.3 of the Prohibition on Money Laundering Regulations (Rules for Use of Information Transferred to INP and *Shin-Bet* for Investigation of Other Offences and for Transferring it to Another Authority - 5766 – 2006).

Weighting and Conclusion

Recommendation 31 is rated compliant.

Recommendation 32 – Cash Couriers

Israel was rated largely compliant with former SR.IX in its 2008 MONEYVAL assessment. The main deficiencies were that not all bearer negotiable instruments were covered and that the threshold declaration regime was too high under immigrant rules.

Criterion 32.1 – Israel has a declaration system for currency and BNI (referred to as "monies"[61]) leaving or entering the borders, be it with a traveller or by way of mail and cargo (s.9 of the PMLL). This system was reviewed by MONEYVAL and has been improved following legislative changes to the PMLL that came into force on the 12 December 2017; these changes rectify the previous identified deficiencies and the system now fully meets this criterion.

Criterion 32.2 –. Israel has a written declaration system to detect funds that meet various thresholds depending on certain circumstances, all of which are within the thresholds set out in R.32. The minimum threshold is NIS 50 000 (EUR 11 680). The declaration regime is stronger when the border is one of those listed in Schedule 4 to the PMLL, referred to as "land border crossing points" or involves entry or exit via the Gaza area. There are five land border crossing points. The threshold at designated land border crossing points falls to NIS 12 000 (EUR 2 800). The declaration system applies the relevant threshold equally to instances of border crossing by way cargo / mail or traveller.

Criterion 32.3 - This criterion is not applicable because Israel has a written declaration system as noted above.

Criterion 32.4 - The Customs Authority is the competent authority in relation to the declaration system. As such, customs officials have the power to seek information in relation to a false declaration or non-declaration (s.27 of the PMLL). These powers are transferred to a customs investigator if it is suspected that an offence has been committed.

Criterion 32.5 – Section 10 of the PMLL sets out the criminal penalty regime for breaches of the obligation to report. The penalty for a false declaration or failure to declare is a term of imprisonment of up to six months or a fine in accordance with the maximum of the scale that can be imposed under the Criminal Code or, if it is greater, ten times the amount which was not reported. A fine, if one is issued, must be paid prior to the return of any funds not declared.

Section 3(b) of the PMLL sets a criminal penalty in severe cases of breaching the obligation to report. In cases in which the violation of the report was made in order to circumvent or prevent the

61. Monies are defined in section 1 of the PMLL as: cash, bank and travellers checks, bearer securities, negotiable notes, as well as payment cards and any other means of payment that is authorised by the issuer to be used by any person; in this definition, "payment card" - plate or other object, on which a monetary value may be accumulated, that is intended for the purchase of assets or services or for the withdrawal of cash.

submission of a report to IMPA or in order to cause an erroneous report, the penalty can reach up to five years imprisonment or a fine of eight times the fine specified in section 61(a)(4) of the Criminal Code.

A breach to reporting obligations under s.9 of the PMLL can also be subject to an administrative fine (s.15 PMLL). These fines are similar to those used in the criminal regime, but they also take into account if the circumstances could be considered as a repeated breach. If a person is found to have committed a breach under the administrative mechanism, and subsequently pays the sanction, he will not face criminal proceedings. The penalties involved appear to be proportionate. Section 12 of the Prohibition on Money Laundering (Financial Sanction) Regulations allows for a first violation, a fine of up to half the amount stipulated in section 15.

Criterion 32.6 – Reports relating to the declaration of cross border funds movements are transferred to IMPA (as per section 9(f) of the PMLL). The Prohibition on Money Laundering (Modes and Times for Transmitting Reports to the Database under Chapter Four of the Law) Regulations provide further instructions as to how and when such reports shall be transferred to IMPA. The Tax Authority, who may also undertake an investigation into allegations of breaches of the reporting obligation and upon completion of such an investigation, submits reports to the Competent Authority on the results of investigations.

Criterion 32.7 – The Implementation Committee (IAIC 2) is in charge of strategic co-operation. This co-operation appears to be moved to a tactical level through the various task force and AML units deployed in the field (see R. 2). ITA also co-operates closely with IMPA and the AML squads of the Israel National Police. In addition the joint intelligence centre (Intelligence Fusion Centre) (IFC) enables close co-operation and co-ordination of the INP, ITA and IMPA.

Criterion 32.8 – Customs investigators can seize objects in cases related to cash declarations, if these can be considered as potential evidence in matters relating to ML, TF or predicate offences by virtue of section 27(b)(5) of the PMLL. Such a seizure, if the retention was to extend beyond six months without the object actually being used as evidence, can be extended if an application to do so is made to a Magistrates Court.

In the case of non or false declaration, section 11(a) PMLL allows for the funds to be seized, without a court order, for an initial period of up to ten days. The court can extend this period by another ten days to allow a fine to be imposed following an administrative committee finding or an indictment filed. However, in the case of the funds being suspected of being evidence in an offence under the PMLL the entire amount may be seized, to enable further investigation, by virtue of section 27(b) of the PMLL.

Criterion 32.9 – Section 30(f) of the PMLL allows for the declarations or reports concerning non-declaration and false declarations to be shared with other jurisdictions, in instances that the information relates to property traceable to an offence as defined in section 2 PMLL or to terrorist property. In 2006, the AG issued specific guidelines which allow for a wide interpretation of section 2, including any suspicion of ML/TF/predicate offences. These guidelines expressly stipulate that ML typologies and patterns may serve as a reasonable basis for suspicion.

Criterion 32.10 – The reports are provided to the IMPA and, in accordance with the legislative requirements, held securely. They do not interfere in trade or capital movements.

Criterion 32.11 – Israel applies proportionate and dissuasive sanctions – criminal and administrative to persons carrying out a physical cross-border transportation of currency or BNIs (see criterions 32.5 and 3.9). These measures enable the confiscation of such currencies or BNIs.

Weighting and Conclusion

Recommendation 32 is rated compliant.

Recommendation 33 – Statistics

In its third mutual evaluation, Israel was rated largely compliant with these requirements. The main technical deficiencies were that statistics on judicial MLA and administrative international co-operation were respectively not comprehensive and incomplete.

Criterion 33.1 –

(a) STRs, received and disseminated – IMPA maintains statistics on the number of UARs (STRs) and CTRs received and disseminated (and, for CTRs, their amounts). There are also statistics on the number of requests for information received and transmitted, and on intelligence reports disseminated by IMPA broken down by areas of crime and typologies.

(b) - ML/TF investigations, prosecutions and convictions – The State Attorney's office (SAO) maintains and communicates statistics on ML/TF related indictments, prosecutions, convictions and confiscations to IMPA. The INP has a statistics unit which is generating data on the number of ML/TF investigations, prosecutions, convictions, scope of seized/frozen property, etc. with a breakdown by predicate offences. This data is disseminated to IMPA annually.

(c) - property frozen; seized and confiscated – The Asset Recovery and Forfeiture Management Office (ARFO) (see Rec. 4) collects and maintains data on seizures, forfeiture of assets and their management. The INP is required to submit monthly statistics on seizures and the number of cases they are involved in to the National Forfeiture Unit (located within the Financial Enforcement Unit in the INP – see R.30). Prosecution authorities also maintain data on criminal sanctions (i.e. seizures, fines and confiscations). ITA maintains statistics on the number of seizures of unreported cash at borders.

(d) - MLA or other international requests for co-operation made and received – Statistics are available at the Department of International Affairs of the SAO (on MLA outgoing requests and incoming and outgoing requests for extradition) and the Legal Assistance Unit of the INP (on MLA incoming requests). They can be disseminated to IMPA upon request. IMPA also has statistics on co-operation requests made and received from foreign FIUs.

Additional statistics – supervisory statistics:

- Banks are required to report data on the number of reports submitted and their amounts; number of accounts of customers and of high risk customers and the balance of the financial assets portfolio of accounts of customers and customers at high risk to the BoI, as well as the number and types of reports disseminate (Banking Directive 411). The BoI's Banking Supervision Department maintains these statistics as required by s.5 of the Directive 825.

- CMISA maintains and monitors inspection reports pertaining to financial services (e.g. insurers and pension funds).

Weighting and Conclusion

Recommendation 33 is rated compliant.

Recommendation 34 – Guidance and feedback

Israel was rated partially compliant in its last MER for these requirements due to insufficient CFT guidelines to the financial sector, insufficient case-specific feedback, as well as absence of guidelines for DNFBPs.

Criterion 34.1 –

Financial institutions

BoI issued the *Banking Directive 411*, which came into force in September 2002 (and the updated Directive in January 2018) and is considered as by-laws. The Banking Directive 411 provides general guidance to banking corporations on the implementation of the PMLL and the 2001 Banking Order (Prohibition of Money Laundering), especially in relation to STRs (UARs). This Directive is complemented by a number of circulars on specific issues, which also aim at clarifying the PMLL and the Order. BoI also holds regular contact with banks and banking coprorations, especially following on and off-site inspections. BoI's Banking Supervision Department also holds regular meetings (incl. forums, seminars) on AML/CFT issues.

ISA regulalry issues circulars and AML/CFT related guidelines for stock exchange members, trading platforms and portfolio managers. These guidelines are generally published on ISA website. Individual guidance of supervised entities is also provided on an ongoing basis, as well as guidance sessions for all new companies and new independent licensees. ISA also hold seminars and guidance sessions on AML/CFT theoretical and practical topics.

The ***Postal Bank*** supervisor issued a Directive for *Proper Conduct of the Postal Bank* (which came into force in November 2015), and a number of proper management directives (on risk management, record keeping, internal audit, etc) and circulars (e.g. in January 2016 on risk management of customers' cross-border activities). The Supervision Department of the Postal Bank also provides feedback, especially following audits.

CMISA issues booklets on AML/CFT related issues to insurance companies and provident funds which should be soon published . Two commissioner positions were also published in 2014 and 2016 as a result of in-depth AML/CFT inspections. A circular concerning insurers and provident funds ML/TF risk management was published in February 2018. As of June 2017, MSBs are placed under the authority of CMISA (it was previsouly supervised by the MSBs Registrar). Upon registration, MSBs receive a booklet on requirements of the PMLL and the 2014 MSB Order. Ministry of Finance also published questions and answers on the proper implementation of the MSB Order. CMISA held a dedicated AML/CFT seminar to the insurance sectors in July 2017.

MSBs: MOF and IMPA conduct training to newly registered MSBs on AML/CFT obligations. Upon registration, MSBs receive a booklet covering the main requirements of the PMLL and the MSB Order. The MOF website also has a list of Q&A regarding the implementation of these requirements.

DNFBPs

As supervisor of Precious Stones Dealers (PSDs), the Diamonds, Gemstones and Jewelry Administration (DGJA) issues AML/CFT related booklets and frequently asked questions on its

website. IMPA also published guidance regarding UARs and a "red flag" document on the activities of dealers in precious stones.

For lawyers and accountants, the BSP supervisor published a number of guidance and red flags indicators.[62]

IMPA

IMPA's website contains a number of relevant publications, such as: AML/CFT guidelines, legal updates, red flags indicators, typologies, booklets and a triennial newsletter on AML/CFT issues, which is also distributed to law enforcement authorities, supervisors and compliance officers within FIs and DNFBPs. IMPA also participates in conferences and training session to raise awareness in respect of AML/CFT issues - among FIs, DNFBPs and supervisory authorities. IMPA holds 'feedback meetings' on a routine basis.

IMPA provides feedback through the sending of letters to FIs on the quality of their submissions (to date, dealers in precious stones have not submitted reports). These letters can sometimes provide a detailed review of the reported transaction, with mention of the shortcomings and a request to revise or provide additional information.

Weighting and Conclusion

Recommendation 34 is rated compliant.

Recommendation 35 – Sanctions

In its previous assessment, Israel was rated compliant with former R.17.

Criterion 35.1 – A range of proportionate and dissuasive criminal and administrative sanctions are available, ranging from written warnings to fines and imprisonment.

Targeted Financial Sanctions (Recommendation 6)

Failure to apply the freezing obligations regarding a designated terrorist (pursuant to s.32(b) CTL) or of a terrorist organisation (pursuant to s.34(c)) is subject under s.32(a) to a criminal penalty of seven years imprisonment or a fine ten-times the fine prescribed in s.61(a)(4) of the CC: (NIS 2 260 000 or approximately EUR 528 000). Performing a property transaction with the intention of assisting or financing the activity of a terrorist organsation is also subject under s.31(a) to ten years' imprisonment or a fine twenty-times the fine prescribed in section 61(a)(4) of the CC (NIS 4 520 000 or approximately EUR 1 000 000).

NPOs (Recommendation 8)

The Registrar can initiate liquidation proceedings in court as a result of illegal or improper conduct by a NPO (s.49 of the Amutot Law). For NPOs that receive governmental support, the certificate of proper conduct may be cancelled or not renewed until the Registrar is satisfied that the misconduct has been remediated. NPOs can be liable to criminal liability. It is not clear whether the measures are fully proportionate and dissuasive.

62. http://www.justice.gov.il/Units/FBPS/Pages/default.aspx) and conducted). The supervisor also conducted lectures to BSPs

Preventives measures (Recommendations 9-23)

Criminal sanctions in the PMLL: apply to all FIs and covered DNFBPs

There are criminal sanctions in the PMLL for certain provisions, as follows:

- Failure to the confidentiality obligations in s.31A(a-b) could result in three years emprisonement or a fine according to s.61(a)(3) of the Criminal Code; if committed negligently, in one year imprisonment or a fine according to s.61(a)(3) of the Criminal Code: NIS 75 300 or approximately EUR 17 600.
- Failure to comply with tipping-off requirements (s.7(c))could be subject to one year's imprisonment and the same fine
- Engaging in a property transaction or providing false information regarding AML/CFT obligations in the PMLL in order to cause an erroneous report to be submitted: 10 years imprisonment and a fine of twenty times the amount set out in s61(a)(4)CC: NIS 4 520 000, approximately EUR 1 000 000 (s.3(b) of the PMLL).

Administrative sanctions in the PMLL: applies to all FIs and covered DNFBPs.

The PMLL enables the setting-up of an *administrative sanction committee* by each competent supervisor (s.13). Procedures pertaining to the funcitonning of these sanctions committees are laid out in the Prohibition on Money Laundering (Financial Sanction) Regulations.

Each Commitee is empowered to impose financial sanctions for breaching the AML/CFT obligations of the PMLL (s.14) and the AML/CFT Orders issued under those obligations pursuant to s.11M(c)(1). The AML/CFT requirements of the PMLL are: the general customer identification obligations, reporting obligations, record keeping (s.7(a)(3)), secrecy (s.7(c)), training and the manner in which the prescribed obligations will be fullfilled (s.7(b)) for FIs (s.7 and s.7A), and the general customer identification, and reporting obligations, record keeping (s.8A(a)(3), 8B(b)(2)), secrecy (s.8A(d)) and training (s.8A(f), 8B(e)) for dealers in precious stones (s.8A) and business service providers (s.8B). For FIs and DNFBPs who fail to comply with the these requirements, the Committee can issue a financial sanction for an amount up to ten times the amount of the fine specified in section 61(a)(4) of the Criminal Code: NIS 2 260 000 or approximately EUR 528 000 (s.14(a) of the PMLL). These sanctions can be imposed on the individual or the employing corporation.

The amount of the administrative fine is determined by different factors – e.g. whether it is a first, further or continuing violation, the seriousness and extent of the breech and the violator's co-operation (s.9(1)(A-F) of the Financial Sanction Regulations. The Committee can also impose upon a corporation (if it is an FI or a dealer in precious stones) the same fine for failure appoint a compliance officer (the requirements of s.8(a) and s.8A(f), respectively).

Other sanctions are available to the various supervisors throught their sectoral laws and ordinances, as follows. According to s.11N(d) of the PMLL, where the supervisor has been granted supervisory powers over the supervised body by another law, then he shall also be entitled to exercise them when discharging his supervisory functions pursuant to the PMLL. Therefore, supervisors have the power to sanction through sectoral laws below, when related to AML/CFT requirements.

Financial Institutions

Banking corporation / credit institutions / trust companies: Financial sanctions can be imposed by the BoI for an amount of NIS 1 million (EUR 234 000) if the supervisor has reasonable grounds to believe that the banking corporation committed any of the violations listed under s.14H of the Banking Ordinance (e.g. violation to the proper conduct of banking business directive). Failure to rectify identified deficiencies can result also in the suspension or removal of the office holder (s.8C

of the Banking Ordinance). Banking corporations can also de-licensed (s.8 of the Banking Licensing Law). Other remedials actions can be taken – such as appointing an external examiner, replacing the compliance officer or its manager, issuing written warnings or a demand to amend deficiencies (s.8a of the Banking Ordinance).

Trading platforms - ISA can suspend or revoke a license if there are doubts as to the personal reliability the company's officers or of its controlling shareholder (s.44M(c), s.44W(a) of the Securities Law). The Securities Law provides a list of circumstances for appreciating the reliability.

Portfolio managers - ISA can simialrly suspend or revoke a license in case of conviction or severe violations of AML/CFT obligations (s.10(a1) of the Investment Advice Law). Financial sanctions can also be imposed (sections 38A, 38H of the Advice Law), and directors and senior managers can be prohibited to serve as a senior officer (s.52(a) of the Securities Law).

Insurance / provident funds: CMISA can impose financial sanctions on insurance companies and provident funds (namely on their general manager or a partner, but excluding a limited partner) that have failed to comply with the provisions of the law (ss.43 and 47 Provident Funds Law; s.92M(b) of the Insurance law). CMISA can also revoke a licence (s.22 Insurance Law; s.8(b) Provident Funds Law)], remove an office holder from office (s.33A(c)(1) Insurance law), restrict its power or appoint a licensed administrator or a special supervisor.

Credit service providers: CMISA can revoke or suspend a license if the applicant provided false information, if the submitted information changed since the application, or for reasons of public interest (s.23(A) of the Supervision of Financial Services Law). Chapters 12 and 13 (Sections 71(2)-(3), 72(a)(2), 72(b)(9),(11),(14)-(16), 72(c)(4)-(5), 73, 94(b)(3), 95) can also impose sanctions on directors and senior manager. These sanctions include adminstrative financial sanctions or criminal fines.

Postal Bank: The Director General of the Ministry of Communications can apply on the Bank a monetary sanction (NIS 27 680/ EURUSD 6 470) in case of violations listed prescribed in the Postal Law (e.g. violations of any of the terms of its license) (s.109B(a)).

MSBs: The Registrar may delete an MSB provider or suspend its registration for failing to continue to meet its registration requirements (s.11I of the PMLL).

DNFBPs

BSPs (lawyers/accountants): The Bar Association and the Accountant Council have the power to initiate enforcement proceedings for any disciplinary violations under their respective legislation (e.g. disciplinary sanctions may include warning, reprimend, fine (for lawyers), or suspension or revocation of a license) (s.68, Bar Association Law, and s.12, Auditors Act). Lawyers and accountants receive personal licenses, therefore any sanction will always apply to them personally.

Diamond dealers: The 1979 Diamonds Inspection Order (s.9) authorises the Commissioner to suspend the license of a trader in precious stones.

While the above measures are generally very broad, some DNFBPs (real estate agents, TCSPs, and dealers in precious metals) are not covered by AML/CFT obligations, and lawyers and accountants are not covered by certain AML/CFT obligations; consequently the related sanctions do not apply to them.

Criterion 35.2 – The range of criminal and administrative sanctions under the PMLL described above applies to financial institutions, covered DNFBPs as well as directors and senior management. Israel indicated that in practice the criminal penalties in ss.3(b) has been applied for failures by managers to comply with their AML/CFT obligaitions through case law (criminal case no. 40156/07, *State of Israel v. Yitshak Martsiano*). A number of the sanctions available in the sectoral laws described above, can also be applied to institutions as well as directors and senior management. While these measures are broad, there are not AML/CFT requirements for certain DNFBPs.

Weighting and Conclusion

Overall Israel has broad measures to apply criminal and adminstrative sanctions for non-compliance with AML/CFT measures. However, some DNFBPs (real estate agents, TCSPs, and dealers in precious metals) are not covered by AML/CFT obligations, and lawyers and accountants are not covered by certain AML/CFT obligations; consequently the related sanctions do not apply to them. It is also unclear if sanctions for NPOs are fully proportionate and dissuasive.

Recommendation 35 is rated largely compliant.

Recommendation 36 – International instruments

Israel was rated largely compliant for these requirements in its last MER. The deficiencies identified then were related to the 1999 TF Convention (lack obligations on other professionals involved in financial transactions, and concerns about the effectiveness). Since then, Israel has updated its TF-related legislation.

Criterion 36.1 – Israel signed and ratified the following international instruments:

	Signature date	Ratification date	Implementing legislation
Vienna Convention	20 December 1988	20 March 2002	Mostly through the 1973 Dangerous Drugs Ordinance
TF Convention	11 July 2000	10 February 2003	Mostly through the 2016 Counter-Terrorism Law (CTL)
Palermo Convention	13 December 2000	27 December 2006	Mostly through the 2003 Combating Criminal Organisation Law
Merida Convention	29 November 2005	4 February 2009	Mostly through the CC

Criterion 36.2. Israel passed a number of implementing legislations related to TF, especially the CTL in 2016.

Weighting and Conclusion

Recommendation 36 is rated compliant.

Recommendation 37 - Mutual legal assistance

Israel was previously rated **compliant** with former Recommendation 36 and Special Recommendation V.

Criterion 37.1 – Israel has several legal mechanisms enabling competent authorities to rapidly provide the widest range of MLA – namely the International Legal Assistance Law (ILAL, section 2),

the Securities Law (chapter 9B of the Securities law), and a number of bilateral MLA treaties (incl. with the United States, Canada; Australia; India and Hong Kong, China). Israel is also a signatory to the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe as well as the Second Additional Protocol (see also Chapter 1). Based on the "principle of reciprocity", Israel may grant or seek legal assistance from another country even in the absence of a convention.

Criterion 37.2 – Israel does not have one central authority for the transmission and execution of requests. Rather, an established official mechanism is in place where three authorities, relating to ingoing and outgoing requests, share the responsibility for mutual legal assistance - namely Directorate of Courts, the Legal Assistance Unit (LAU) in the Israel National Police (INP) and the Department of International Affairs (DIA) in the State Attorney's Office (SAO) in the MOJ.

The Directorate of the Courts serves as the address for all incoming requests. Requests are then transferred to the LAU who is the main body that deals *incoming requests*. The LAU then designates the specific police unit to handle the request, and oversees the police unit and sets timeframes for response. Requests requiring investigation by a specialised body are transferred to the relevant authority. Requests that involve violations of securities laws are transferred to the ISA directly from its foreign counterpart. Both the LAU and the ISA have internal procedures to support the processing of MLA requests, which includes prioritisation of requests. They also each have an internal case management system to register and to monitor the progress of executing and responding to requests until they are fully addressed. Police Guideline No. 03.300.07 prescribes that MLA requests be executed in a timely manner and without undue delay. Requests asking for immediate assistance or marked as urgent are prioritised in order for them to be dealt with immediately.

The DIA is responsible for most *outgoing requests* of legal assistance. DIA drafts and submits request for MLA on behalf of Israel, and also advises INP and other units regarding incoming requests. MOJ has procedures, including a case management system, to monitor outgoing requests.

Criterion 37.3 – The existing legislation does not subject requests to unreasonable or unduly restrictive conditions (s.5 of the ILAL; s.53K3, 54K5(c) and 54K6 of the Securities Law.

Criterion 37.4 –

(a) Under the law, requests can be refused on the ground that it also involves fiscal matters. "Fiscal matters" is listed under s.5(a)(4) of the ILAL as a possible ground of refusal. However, Israeli authorities do not interpret this as meaning that requests can be refused solely on the basis that they involve fiscal matters. There are guidelines to enable the provision of such assistance on the basis that a fiscal office is related to fraud, and in practice Israel regularly grants legal assistance requests in fiscal matters if the fiscal offence is an integral part of a criminal act involving other types of offences.

(b) Assistance is not refused on the grounds of laws that impose secrecy or confidentiality requirements on FIs or DNFBPs. There are no extra bars imposed on obtaining or transmitting confidential information because the information or evidence is obtained pursuant to a valid request by a foreign state (s.8 and s.12 ILAL). There is an exception for items subject to legal professional privileges, including information and documents and compelling of witnesses to attend an interview (s.8 ILAL; s.1A(3) Accountants Regulations (Conduct unbecoming the profession); s.90 Bar Association Law; s.48 Evidence Ordinance). These privileges apply equally to both local and foreign investigations.

Criterion 37.5 – There is a legal requirement to keep the foreign state's request (including contents or information about it, as well as documents and information attached to it) and its results confidential. This is conditioned to Israel being requested to do so (s.11(a) ILAL). The confidentiality is also subject to the provisions of Israel Law (s.23C of the Privacy Protection Law). If it is not possible to carry out the request while maintaining confidentiality, Israel must inform the requesting state accordingly and carry out the request only with the approval of that state (s.11(b)). Similar confidentiality requirements apply to information provided to the ISA by foreign authorities (s.13 and 56E of the Securities Law).

Criterion 37.6 – Where the assistance sought is not coercive, there is no requirement for dual criminality. Dual criminality applies if the request relates to freezing and confiscation. It also applies for coercive measures involving ML and other investigations. This rule is not required for offences related to terrorism, conspiracy to commit offences related to terrorism, and ML (s.2(b) and 2(c) PMLL and s.54k4(a) of the Securities Law). Coercive actions specifically mentioned therein in relation to securities could be employed only if the violation stipulated in the request for assistance could possibly be the subject of a criminal investigation in Israel (s.54K4 of the Securities Law). This applies only when these coercive measures (as opposed to non-coercive measures) are involved.)

Criterion 37.7 – Israel focuses on the underlying criminal act and not the terminology.

Criterion 37.8 –

(a) Israel may execute a wide range of MLA requests, including the production, search and seizure of information, documents, or evidence (including financial information) from financial institutions or individuals or other legal entities, and carrying out investigative act which includes taking a statement. ISA has the power to search, seize, arrest, request a temporary order for seizure of property, or to provide communications data for requests where the subject could possibly be the subject of a criminal investigation in Israel (s.54K4(a) of the Securities Law).

(b) The INP is able to employ a wide range of investigative techniques which includes interrogation techniques, use of "agents" and policemen, detainees or prisoners used to interrogate suspects, and other technological means as deemed necessary, in response to a request for mutual legal assistance. Wiretapping can also be carried out for foreign jurisdictions through court order (s.31 of the ILAL).

Weighting and Conclusion

Israel meets or mostly meets most of the technical criteria for Recommendation 37. There is a minor deficiency in that there is the possibility to refuse MLA requests technically on the ground that it involves fiscal matters.

Recommendation 37 is rated largely compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its last MER, Israel was rated largely compliant for these requirements. This was due to the limited range of offences contained in Schedule 2 of the 1998 law (predicate offences which Israel could seize and confiscate pursuant to foreign requests), and concerns over effectiveness. Since then, Israel amended Schedule 2 to expand the range of offences.

Criterion 38.1 –

The Israeli courts are empowered, with respect to certain designated crimes and subject to certain procedures and pre-conditions, to freeze assets and enforce forfeiture orders executed in foreign courts for crimes committed outside of Israel.

Confiscation

The ILAL enables the enforcement of a foreign confiscation order issued by a court of the requesting State concerning property in Israel connected to criminal offences to be enforceable provided that the Competent Authority (the head of the DIA of the office of the State Attorney in the DoJ) determines that the property was used or intended to be used for an offence, or was obtained directly or indirectly from the offence, or is an instrumentality (s.33(a)(2) of ILAL)). The law does not specifically cover value-based confiscation.[63] The offences for which assistance may be provided are those listed Schedule 2 (s.33(a)(1)). These offences include: drug offences, ML offences, and TF offences, predicate offences as enumerated in the PMLL, as well a number of other offences.

Identification and freezing

When another state submits a request to discover evidence or an object, or to seize and transfer them to it for the purposes of a criminal matter in that state, then the Competent Authority may – in order to locate the evidence or the object – apply to the Court for an order to present the object, or for a warrant to search a certain place or to conduct a body search of a person or a body search of a suspect. It may also apply for an order to seize the evidence or the object and to transfer them as requested (ILAL s.29(a)).

The Competent Authority may transmit a request from a foreign country to the Court to issue a temporary order to secure property located in Israel, in connection with a legal proceeding which is or will soon be in progress before a foreign judicial authority for an act covered by Schedule Two. This order provides for seizure for a period of six months, but may be extended another six months (ss.39 and 40). The Competent Authority shall transmit the request only if the requesting state gave sufficient undertakings for the payment of compensation (in the event that the property is not ultimately confiscated), although this requirement may be waived on a case-by-case basis for particular reasons.

Criterion 38.2 – Israel has the authority to provide assistance to requests for co-operation made on the basis of non-conviction based confiscation proceedings and related provisional measures. The definition of "foreign confiscation order" includes an order to confiscation property made by a foreign judicial authority (including any government authority competent to issue a confiscation order), either in a criminal or in a civil proceeding. Civil forfeiture can be obtained through several mechanisms without a conviction – e.g. s.22(a)(2) of the PMLL (which covers the absence of a perpetrator) and s.14 of the Combatting Criminal Organisations Law (which covers the property of a criminal organisation). Israel can also secure property temporarily, prior to a conviction being obtained abroad, under certain circumstances.

Criterion 38.3 – Israel has measures in place for co-ordinating seizure and confiscation actions with other countries and mechanisms for managing, and when necessary disposing of, property frozen, seized, or confiscated (ILAL s.41 and DDO s.36H(a)).

63. Israel has indicated that an amendment to the ILAL is underway which will enable the confiscation/freezing of property of corresponding value in response to requests by foreign countries. The draft amendment was published for public comment on 25 June 2018.

Criterion 38.4 – The MOJ may prescribe the property confiscated, or part of it, or its consideration may be transferred to a foreign country which made the foreign confiscation order (ILAL s.42).

Weighting and Conclusion

The ILAL and other domestic laws enable Israel to take expeditious action in response to requests by foreign countries to identify, freeze, seize, and confiscate laundered property, proceeds of crime, and instrumentalities used and intended for use in ML, predicate offences, and TF. While the law is generally broad, it does not cover property of corresponding value.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its last MER, Israel was rated compliant with the requirements of this Recommendation on extradition.

Criterion 39.1 –

(a) Both ML and TF are extraditable offences under Israel law. The Extradition Law permits extradition in respect of all offences for which the punishment is one-year imprisonment or greater (s.2a). There must also be an extradition agreement between the requesting state and Israel (s.2A(a)(1)). Israel has signed over 40 treaties, bilateral and multilateral agreements on MLA and extradition. Israel is also party to the 1957 Council of Europe Convention on Extradition, with reservations. In addition, Israel can conclude special ad hoc agreements for extradition (s.2A(c)(2)).

(b) Requests are dealt as quickly as possible by the Department of International Affairs (DIA) of the State Attorney's Office. DIA uses a case management system to execute these requests. The DIA has processes for prioritisation to process urgent requests.

(c) The legal provisions of the Extradition Law do not place unreasonable or unduly restrictive conditions on the execution of requests (s.2B(a)) - e.g. the restrictions related to offences of a political character, racial or religious discrimination).

Criterion 39.2 – Israel can extradite its own nationals, under specific conditions set out in s. 1A.(a). A national can be extradited for trial; for serving sentence the extradited person has the choice between proceedings in the other country or Israel. Extradition of a national will be granted conditional to receiving from the requesting state's promise that, to the extent that the national is convicted and sentenced to prison, the extradited person will be returned to serve his sentence in Israel. These restrictions have been explicitly stated in the 2015 judgement of the Supreme Court, *Rosenstein v State of Israel*. In the event that Israel will not extradite a national, there are procedures in place to prosecute the case domestically.

Criterion 39.3 – Dual criminality is required for extradition (s.2(a)). However, this requirement is deemed to be satisfied regardless of the technical differences in the laws of the requested and requesting states, as Israel focuses on the underlying criminal act. Extradition is also provided for connected offences even if they would not have been extraditable on their own (s.2(b)).

Criterion 39.4 – The Extradition Law sets up the possibility for simplified extradition (e.g. – when a person requests to be returned to the requesting state - s.9 (b)). In urgent cases, Israel can order the

provisional arrest of a requested person, even prior to the receipt of the extradition request, if provided with assurances that an extradition request is forthcoming shortly and will be supported by the necessary supporting documents (s.2B(6)).

Weighting and Conclusion

Recommendation 39 is rated compliant.

Recommendation 40 – Other forms of international co-operation

Israel was rated largely compliant for these requirements in its previous MER, mainly due the restricted access to law enforcement information.

General remarks:

The *Shin-Bet* has authority to share TF information with its counterparts in foreign countries (s.8 of the *Shin-Bet* Law). Authorities indicated that internal procedures cannot be disclosed at this stage for confidential reasons.

- There are no legal provisions regulating international co-operation regarding the Postal Bank and dealers in precious stones. Authorities indicated that in practice there are no legal provisions preventing the exchange of information with foreign counterparts.

Criterion 40.1 – Competent authorities in Israel, including LEAs and supervisory authorities, can provide a wide range of information on their foreign counterparts. IMPA and ITA can share information both simultaneously and upon request. In some cases, authorities use general rather than specific provisions; these generic provisions are sufficient.

Criterion 40.2- IMPA, LEAs (INP, ISA, ITA) and supervisory authorities (BoI, CMISA) have a legal basis to exchange information with authorities in other countries (IMPA: s.30(f) PMLL; INP: Interpol procedure , s.32 ILAL; ISA: s.54K-54K9; CMISA: s.50C of SFS of Insurance Law; BoI: s15A1 of the Banking Ordinance; ITA (on income tax matters) s.196, s.214b, s.214c of the Income Tax Ordinance and Tax treaties; MSB: s.99 of the SFSL).This can be done for instance through the signature of bilateral/multilateral agreements (ITA: Israel is signatory to 55 treaties on tax matters and ratified the Multilateral Convention on Mutual Administrative Assistance in Tax Matters on August 31, 2016) and MOUs (IMPA, ISA). INP can also be contacted through Interpol or police attachés. BoI can exchange AML/CFT related information on the basis of informal contacts within foreign supervisory authorities.

(b) There are no legal provisions preventing authorities from using the most efficient means to co-operate. ISA handle requests for assistance in an effective manner in accordance with internal procedures and certain variables (such as the urgency of the request).

(c) ISA, IMPA, INP and ITA use clear and secure mechanisms and channels for the transmission and execution of requests. There are no specific provisions regarding other authorities.

(d) Both departments responsible for the execution of requests within ISA have relevant internal procedures in place relating to the handling of requests. BoI prioritises requests received on a case by case basis. For the police, inquiries received through Interpol are prioritised based on the urgency of the request. Both IMPA and INP have relevant internal procedures. There are no specific provisions regarding other authorities.

(e) IMPA, INP and ISA are safeguarding information sent and received using servers and databases. For example, the INP stores information transmitted in the *Tali* system or in the *Malehet Mahshevet* intelligence system. There are no specific provisions regarding other authorities. As such, MoUs signed by the BoI have provisions relating to confidentiality, and the information received by CMISA is maintained on the *Maor* system (a MoF's secure computer system).

Criterion 40.3 – Most of the authorities that are authorised to exchange information with their foreign counterparts do not need to sign an MOU in order to do so. ISA requires the authorisation of the MFA, MOJ to sign an international MoU, and in certain cases, also of the MOF, the Cabinet and the Parliament (as per MFA guidance). ISA is currently a party to 52 bilateral agreements and to the IOSCO MOU (and its 114 signatories), and exchanges information with partners to the agreements only. When negotiating new MOUs, ISA can speed up the process in case of urgent needs. For IMPA – see c.40.9.

Criterion 40.4 – INP provides feedback upon request but there is no a formal procedure regarding the timeliness. ISA is not prevented from sharing that feedback upon request, and BoI can do so as per MoU it has signed. For IMPA, please refer to c.20.10. There are no specific provisions regarding other authorities.

Criterion 40.5 –

(a) – ISA and ITA normally do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance with foreign counterparts. ITA will exchange information only in accordance with the requirements of Art.26 of the OECD Model Tax Convention. The INP can also provide a joint response with the ITA for requests received through CARIN. BoI and CMISA can share information in accordance with the wording of their respective legislation (see c.40.2). There are no specific provisions regarding other authorities.

(b) - Israel does not refuse legal assistance requests on the basis of "banking secrecy" or confidentiality, except where professional secrecy between lawyer and client applies.

(c) – There are no provisions prohibiting or unreasonably and unduly restricting the provision of assistance in case of an ongoing enquiry or investigation. In exceptional cases, if the transmission of the information risks exposing or disrupting the investigation, the request will be carefully reviewed, sometimes with the participation of the requesting country itself.

(d) - ISA can provide assistance regardless of the nature or status of the requesting competent authorities, as long as it is in accordance with the Securities Laws. IMPA can exchange information with counterparts, regardless of their nature or status. Financial supervisors are authorised to exchange information with their foreign counterparts. There is no information on DNFBPs supervisors.

Criterion 40.6 – Competent authorities (IMPA, INP, ISA and ITA) have the necessary confidentiality safeguards in place to ensure that information exchanged is used only for the intended purpose (ISA: s.54k5(c) of the Securities Law; BoI: s.15(a)1 of the Banking Ordinance; ITA: Art.26 of the OECD Model Tax Convention; INP: s.10 and 32(a) of the ILAL, IMPA: s.30 of the PMLL). There are no specific provisions regarding other authorities.

Criterion 40.7 –. Competent authorities are required to maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations

concerning confidentiality, privacy, and data protection (INP: s.11 ILAL; ITA: s.214B(a)(4) Income Tax Ordinance; ISA: s.56E Securities Law; BoI - s.15A1(b)(2); CMISA- s.50C(2) of the Control of Financial Services (Insurance) Law; MSBs - and s.99(b)(2)(3) of the SFSL). The general requirement for the requested competent authority is set out in the Data Protection Regulations (s.5(d)), subject to the provisions of the ILAL (s.11-12). Information from foreign counterparts is protected in the same manner as information from domestic sources.

Criterion 40.8 – Competent authorities, including INP, ISA, ITA, can investigate on behalf of a foreign counterpart all offences under Israeli law (s.2(a) and 28 ILAL). For tax/customs, ITA can do so only as part of a MLA request or under the Customs Agreements and MOUs. The ISA can provide assistance to a foreign authority and use its investigatory powers on its behalf, including issue warrants for search and seizure, interrogate and provide communications data (s.54K4(a) Securities Law). BoI's MoUs provide for co-operation mechanisms, including on AML issues, with foreign counterparts, such as on-site visits. For insurers, CMISA is authorised to provide information to authorised foreign counterparts (s.50C of the Insurance Supervision Law (ISL)). Similar provisions are in place for financial services providers (s. s.99 of the SFSL). For CMISA, see also c.40.15.

Exchange of information between FIUs

Criterion 40.9 – IMPA has a legal basis for sharing the information of its database to a foreign counterpart regardless of its nature (s.30(f) of the PMLL). IMPA will co-operate on ML/TF matters and any offence, provided the request for information relates to suspected proceeds of crime. While the signing of MOUs is not required for the purpose of sharing information, IMPA signed 66 MOUs with foreign counterparts.

Criterion 40.10 – IMPA provides feedback to foreign counterparts regularly and upon request on whether the provided information contributed to the investigation.

Criterion 40.11 – IMPA can use all its investigative powers to provide, directly or indirectly, the information from databases it has access to. This includes for instance information from FIs that is of a confidential nature. In addition to the police and security service information already stored on IMPA's database, IMPA also has indirect access to this information.

Exchange of information between financial supervisors

Criterion 40.12 – Financial supervisors (BoI, ISA, CMISA and MSB Registrar) rely on a general broad provision under their respective sectoral legislation for co-operation with their foreign counterparts (regardless of their nature or status) for AML/CFT purposes. (BoI: s.15a1(a) Banking Ordinance; ISA: s.54K1[64] to 54K9 of the Securities Law; CMISA: s.50C of SFS of Insurance Supervision Law; MSB Registrar (MSBs providing non-bank lending services, deposit and credit services and operator of peer-to-peer systems): s.99 of the Financial Services Business Law (SFSL)).

Criterion 40.13 – Financial supervisors are able to exchange with foreign counterparts information domestically available to them, including information held by FIs, in a manner proportionate to their respective needs. Information will be exchanged provided that it is for the purpose of fulfilling the

64. The Securities Law defines "foreign authority" as a body charged with the implementation and enforcement of securities laws in a foreign country and supervision of their execution, which signed a Memorandum of Understanding with the Authority.

functions of the foreign competent authority, and upon confirmation that the requesting country has similar confidentiality requirements (see legal basis under c40.12).

Criterion 40.14 – As indicated in c.40.12, financial supervisors rely on the broad provisions under their respective sectoral legislations to exchange information with a competent foreign authority. These sectoral legislations do not clearly distinguish the type of information that can be exchanged. Thus, any type of information (regulatory, prudential, and AML/CFT information) can be shared provided all legal prerequisites are met (see c.40.13).

Criterion 40.15 – ISA can exercise its powers to demand information and documents (s.56A), inquiries into stock exchange transactions (s.56A1) and audit powers (s.56F) if the request is made for supervisory purposes, and if there is an MOU in place. There are no specific provisions for other FIs governing the conduct of inquiries on behalf of foreign counterparts. Section 15A1 of the Banking Ordinance provides BOI with general powers to co-operate with foreign counterparts. For insurers, CMISA has supervisory and administrative investigative powers (e.g. make inquiries and request information) pursuant to s.49-50 of the ISL, if there is a suspicion of a violation of supervisory instructions in Israel. Similar provisions are in place for credit services providers (s.64-70 of the SFSL). For BoI, see c.40.8.

Criterion 40.16 – Financial supervisors (ISA and CMISA) in Israel are authorised to disseminate information received only with the prior agreement of the requested financial supervisor. Information received by the Israeli supervisors is otherwise protected by secrecy and confidentiality provisions in the relevant laws (see c.40.6 and 40.7). ISA is legally compelled to disclose the information received for trial purposes, at the demand of the Attorney General or of a Court (s.54K(9)(a) and 56E(a) of the Securities Law). There are no specific provisions relating to BOI.

Exchange of information between law enforcement authorities

Criterion 40.17 – INP (through its *Operational Co-ordination Department*, within the Intelligence Division) can exchange domestically available information with foreign counterparts for ML, TF and predicate offences-related intelligence and investigations. Request for information exchange can be made by foreign police authorities to their counterpart in INP (police-to-police) at the early intelligence stage, or through the Interpol channel. If compulsory measures are necessary (i.e. evidence), the foreign country must go through formal MLA procedure. Israel can also exchange information informally on the basis of the 1988 Vienna and 2000 Palermo Convention, and whenever there is a bilateral agreement for co-operation regarding law enforcement (Israel has MOUs with 39 countries). Israel is also an observer to CARIN (one contact point from INP, one from ITA), and as such can also use this channel for inquiries relating to the identification and tracing of the proceeds and instrumentalities of crime. ISA can provide assistance to foreign securities authorities, regardless of its role as supervisor or as LEA, provided there is a signed MoU. In its law enforcement capacity, ITA can exchange ML information domestically with foreign counterparts in the framework of MLA requests. As for predicate offenses, related to tax offenses or goods smuggling, the ITA is authorised to exchange information by virtue of double taxation treaties and the Customs MOU's and agreements or within the framework of its membership in CARIN, AMON or the ARO Platform of Experts of the EU. Information collected domestically by *Shin-Bet* can also be shared with foreign counterparts (s8(a)(2)of the *Shin-Bet* Law).

Criterion 40.18 – INP can carry out an investigative act (which includes investigation and execution of a confiscation order) once it has been approved by the competent authority (INP: s.28(a) ILAL;

Shin-Bet – (s.8(a)(1),(3), (4) of the *Shin-Bet* Law). The ISA does not need such approval and can carry out investigative act in assistance to a foreign authority subject to the conditions in s.54K2. ITA can conduct criminal tax investigations on behalf of the requesting state, pursuant to MLA requests. In addition, ITA can co-operate under the framework of existing customs agreements and income tax treaties on tax and customs matters.). Requested LEAs respect conditions on use as prescribed by agreements between Interpol or Europol.

Criterion 40.19 – INP (in co-ordination with the international department of the State Attorney's office) is able to form joint investigative teams to conduct co-operative investigations (as per article 20 of the Second *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, ratified by Israel in 2006). The establishment of a bilateral or multilateral arrangement to enable the conduct of joint investigations is not needed. Information can be exchanged police-to-police, and through formal MLA if coercive measures are entailed (see c.40.17). Co-ordination in the conduct of joint operations occurs through Israeli agents posted abroad and foreign agents from counterpart authorities posted in Israel. ISA can initiate an investigation in parallel to an investigation launched by a foreign authority in the context of legal assistance requests initiated under the IOSCO MMOU or in accordance with the ILAL. The ITA can do so as well, if it is indicated in the MLA request. Section 8 of the *Shin-Bet* Law provides the authority with broad powers, including the forming joint investigation teams.

Exchange of information between non-counterparts

Criterion 40.20 –

IMPA can exchange information indirectly with non-counterpart (s.30 of the PMLL) (i.e. information provided to a counterpart can be disseminated to a non-counterpart upon consent). ISA can also exchange information indirectly with agencies in the absence of an MoU via the Israeli MOJ (in accordance with the ILAL). The broad phrasing of section 8(a)(2) enables *Shin-Bet* to pass on information to 'other bodies', which is assumed to also include non-counterparts. There is no legal provision prohibiting the INP to exchange information with non-counterparts LEAs and this is done in practice (see IO.2). It Other than the ISA, other supervisory authorities (BOI, CMISA) cannot exchange information with non-counterparts.

Weighting and Conclusion

Most shortcomings relate to the legal framework for international co-operation between Israeli financial supervisors and their foreign counterparts and non-counterparts, namely the absence of legal provisions regulating international co-operation regarding the Postal Bank (and a lack of relevant information relating to BoI and CMISA). There is also a lack of information on DNFBP supervisors.

Recommendation 40 is rated largely compliant.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• A few sectors are excluded from the scope of the AML/CFT legal framework, which were not based on the NRA results. • Certain sectors are excluded from all or some AML/CFT requirements, and not based on proven low risk.
2. National co-operation and co-ordination	C	
3. Money laundering offences	LC	• The minor shortcomings relating to thresholds.
4. Confiscation and provisional measures	LC	• Israel's legislative framework does not have a generic value-based confiscation system. • There are some restrictions on the extent of provisional measures in relation to certain stand-alone predicate cases.
5. Terrorist financing offence	C	
6. Targeted financial sanctions related to terrorism & TF	LC	• The process allows discretion for the MoD not to make permanent the automatic designations from the UN. • Designations made pursuant to requests from third countries and pursuant to UNSCR designations cannot cover individuals who are Israeli citizens or Israeli residents. • There are not procedures for submitting de-listing requests to the 1267/1989 or the 1988 Sanctions Committees, or procedures to facilitate review by the 1988 Committee, or procedures for informing designated persons and entities of the availability of the UN Office of the Ombudsperson. The CTL does not have comprehensive measures to cover access to frozen funds for basic and extraordinary expenses.
7. Targeted financial sanctions related to proliferation	LC	• There is discretion for the Minister to not make a UN designation permanent (in which case the prohibition on financial activity would lapse), or to revoke a declaration even if the UNSC does not de-list it. • It is also not clear that the prohibitions apply to all funds that are wholly or jointly owned or controlled, directly or indirectly, by the designated person or entity; or the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly. • There are no official procedures for submitting de-listing requests to the UN Security Council in the case of designated persons and entities that, in view of the country, do not or no longer meeting the criteria for designation and there are no provisions with regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to TFS.
8. Non-profit organisations	LC	• There are no clear written policies in place on promoting accountability, integrity and public confidence. • The ICA's overall approach is not risk-based and sanctions are not wholly proportionate. • There is a gap with regard to whole of government co-ordination.
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• There is no general beneficial ownership requirement for MSBs.

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
		• FIs other than banks are not required to verify beneficial ownership information for trusts. • No specific provisions permitting banks and the Postal Bank not to pursue the CDD process. • Simplified due diligence are not based on adequate risk analysis. •
11. Record keeping	LC	• There is a threshold for record-keeping requirements for the MSB sector. • Trading platforms are not required to maintain business correspondence. • There is a lack of a specific requirement for trading platforms, part of the credit service providers sector, and the Postal Bank to ensure that records are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
12. Politically exposed persons	LC	• Portfolio managers, trading platforms, and part of the credit service providers sector do not have domestic PEP requirements. • The definition of PEP for the Postal Bank does not cover senior executives of state-owned corporations. • CDD deficiencies identified under R.10 (e.g. CDD verification is triggered only either by a threshold or when the transactions are repeated ones) also have implications on the CDD measures in relation to PEPs.
13. Correspondent banking	C	
14. Money or value transfer services	C	
15. New technologies	C	
16. Wire transfers	PC	• While Israel applies the basic requirements for originator and beneficiary requirements for cross-border transfers, Israel otherwise relies on general CDD obligations instead of providing specific requirements for wire transfers. • Particularly, MSBs whose business model often entails to a large extent the provision of wire transfers are not subject to specific obligations under c.16.3-c.16.7, c.16.9-c.16.14, and c.16.16. • Save for stock exchange members, no FIs are required by law to verify originator information.
17. Reliance on third parties	N/A	• Recommendation 17 is not rated as it is not applicable to the assessed country.
18. Internal controls and foreign branches and subsidiaries	PC	• Lack of requirements for specific AML/CFT internal control programmes for some covered FIs (particularly portfolio managers). • Obligations to implement group-wide AML/CFT controls and to ensure that branches and subsidiaries operating internationally apply AML/CFT measures consistent with home country requirements are required for banks, and to a certain extent exchange members and trading platforms, but not for other FIs including portfolio managers, MSBs, credit service providers, and insurers.
19. Higher-risk countries	LC	• The range of enhanced due diligence and counter-measures applied are not fully comprehensive with regard to the DPRK.
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	PC	• There are a number of deficiencies, and certain DNFBPs do not have AML/CFT obligations.
23. DNFBPs: Other measures	PC	• There are a number of deficiencies. While dealers in precious stones have reporting obligations, the other DNFBPs in Israel do not. There are also

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
		only some requirements for applying the requirements of R.18, 19, and 22.
24. Transparency and beneficial ownership of legal persons	LC	• The ML/TF risk assessments covered all types of legal persons but should be more comprehensive. • The approach taken by Israel, utilising complementary mechanisms available to ensure beneficial information is available and updated in a timely manner is substantial but complete coverage cannot be certain. • Coverage of nominee arrangements needs enhancement.
25. Transparency and beneficial ownership of legal arrangements	LC	• Shortcomings in relation to holding accurate and current information, as well as sanctions. • Absence of written policies or procedures on international co-operation.
26. Regulation and supervision of financial institutions	LC	• The frequency and intensity of on-site and off-site AML/CFT supervision of FIs is only partly based on risks. • There are also no requirements for supervisors to review the risk-based approach adopted by FIs regularly.
27. Powers of supervisors	C	•
28. Regulation and supervision of DNFBPs	PC	• The supervisors for the covered DNFBPs (lawyers, accountants, and dealers in precious stones) only partly take into account the risk-based approach. • Real estate agents, dealers in precious metals, and TCSPs are not covered for AML/CFT.
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	C	
32. Cash couriers	C	
33. Statistics	C	
34. Guidance and feedback	C	
35. Sanctions	LC	• Some DNFBPs (real estate agents, TCSPs, and dealers in precious metals) are not covered by AML/CFT obligations and lawyers and accountants are not covered by certain AML/CFT obligations; consequently the related sanctions do not apply to them. • It is unclear if sanctions for NPOs are fully proportionate and dissuasive.
36. International instruments	C	
37. Mutual legal assistance	LC	• There is the possibility to refuse MLA requests technically on the ground that it involves fiscal matters.
38. Mutual legal assistance: freezing and confiscation	LC	• The ILAL does not specifically cover value-based confiscation.
39. Extradition	C	
40. Other forms of international co-operation	LC	• Most shortcomings relates to the legal framework for international co-operation between Israeli financial supervisors and their foreign counterparts and non-counterparts, namely the absence of legal provisions regulating international co-operation regarding the Postal Bank.

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
		• There is also a lack of information on DNFBP supervisors.

Glossary of Acronyms[65]

AG	Attorney General
Amutot	Associations (singular Amuta)
ARFO	Asset Recovery and Forfeiture Management Office
ATA	Anti-Trust Authority
BO	Beneficial Ownership
BoI	Bank of Israel
BSP	Business Services Providers
CARIN	EU's Camden Asset Recovery Inter-Agency Network
CC	Criminal Code
CCOL	Combating Criminal Organisations Law, 5763-2003
CETS	Council of Europe Treaty Series
CINPL	Combat of the Iranian Nuclear Program Law
CMISA	Capital Markets, Insurance and Savings Authority
CTL	Counter Terrorism Law
CTR	Cash transaction report
DDO	Domestically Designated Organisation
DPRK	Democratic People's Republic of Korea
EAG	Eurasian Group
EC	European Commission
EDD	Enhanced Due Diligence
ESC	Executive Steering Committee
EUR	Euro
FIU	Financial Intelligence Unit
FSB	Financial Services Board
GDP	Gross Domestic Product
IAIS	International Association of Insurance Supervisors
IBA	Israel Bar Association
IC	Inter-Agency Implementation Committee
ICA	Israel Corporations Authority
ICO	International Co-ordination and Operations section of the INP
ICPA	Institute of Certified Public Accountants
IDF	Israel Defence Force
IDIA	Department of International Affairs of the State Attorney's Office in the MoJ
IFC	Intelligence Fusion Centre
IID	Investigations and Intelligence Division
ILAL	The International Legal Assistance Law
IMPA	Israel Money laundering and Terror Financing Prohibition Authority
INP	Israel National Police
IOSCO	International Organisation of Securities Commissions
ISA	Israel Securities Authority
ITA	Israel Tax Authority
Knesset	Israeli Parliament
LAU	Legal Assistance Unit

65. Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

MLA	Mutual Legal Assistance
MFA	Ministry of Foreign Affairs
MoD	Ministry of Defence
MoE	Minister Economy and Industry
MoF	Ministry of Finance
MoJ	Ministry of Justice
MMoU	Multilateral Memorandum of Understanding
MoU	Memorandum of Understanding
MSB	Money Services Businesses
NBCTF	National Bureau for Counter Terror Financing
NCFB	National Counter Financing Bureau
NIS	New Israeli Shekel
NRA	National Risk Assessment
NSC	National Security Council
OCG	Organised Criminal Groups
PTFL	Prohibition of Financing Terrorism Law
PMLL	Prohibition of Money Laundering Law
SAO	State Attorney's Office
SC	Subcommittee
TASE	Tel Aviv Stock Exchange
TIEA	Tax Information Exchange Agreements
UAR	Unusual Activity Report
UNSCR	United Nations Security Council resolution

www.fatf-gafi.org

December 2018

Anti-money laundering and counter-terrorist financing measures - Israel

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Israel as at the time of the on-site visit on 6-22 March 2018.

The report analyses the level of effectiveness of Israel's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.