Financial Intelligence Centre

DRAFT PUBLIC COMPLIANCE COMMUNICATION

PUBLIC COMPLIANCE COMMUNICATION 44A

GUIDANCE ON THE IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS IN SOUTH AFRICA

PCC SUMMARY

The Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act) places certain obligations on accountable institutions and other persons to implement measures in relation to the asset freeze requirements of the United Nations Security Council (UNSC) resolutions and South African domestic implementation of targeted financial sanctions (TFS) against individuals and entities so designated.

This PCC provides guidance to accountable institutions regarding their obligations to implement UNSC resolutions and domestic designations asset freezing requirements of TFS, which are aimed at combating the financing of terrorism (CFT) and of combating the financing of proliferation (CFP) of weapons of mass destruction (WMD). TFS obligations in terms of the Financial Intelligence Centre Act (FIC) include scrutinising client information against TFS lists to identify designated persons and entities directly or indirectly linked to clients, freezing property of designated persons and entities, filing terrorist property and suspicious and unusual transaction reports with the Financial Intelligence Centre (Centre), as well as obligations regarding de-listing and unfreezing of individuals and entities no longer designated by the UNSC resolution.

In addition, this PCC provides guidance to accountable institutions on examples of terrorist and proliferation financing risks they might face and provides recommendations for the application of a risk-based approach (RBA) to combat both terrorist and proliferation financing.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the users' legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

OBJECTIVE

The PCC provides guidance to accountable institutions on the implementation of TFS aimed at CTF and CPF. The PCC sets out examples of terrorist and proliferation financing risks accountable institutions might face and provides recommendations regarding the implementation of a risk-based approach RBA to CFT and CFP.

CONSULTATION

Before issuing guidance to accountable institutions, supervisory bodies and other persons regarding their performance, duties and obligations in terms of the FIC Act or any directive made in terms of the FIC Act, the Centre must in accordance with section 42B of the FIC Act:

- Publish a draft of the guidance by appropriate means of publication and invite submissions; and
- Consider submissions received.

PCC 44 was issued on 22 March 2022, and PCC 54 was issued on 30 September 2022. The final version of PCC 44A will replace both PCC 44 and 54.

The amendments in this draft PCC 44A address updates to the targeted financial sanctions approach as set out in the FIC Act and Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) (POCDATARA Act), through the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022 (Act 22 of 2022) (GLA Act) and the POCDATARA Amendment Act 2023 (Act 23 of 2023).

The paragraph numbering has been updated throughout the document, to accommodate new insertions as well as changes in existing paragraph positioning.

Commentators are invited to comment on the amendments on this draft guidance by submitting written comments via the online comments submission link only.

Any questions or requests relating to this draft PCC may be sent to the Centre only through the online consultation link. Submissions will be received until **Thursday, 11 January 2024,** by close of business.

1. INTRODUCTION

1. South Africa implements the TFS that originate from the UNSC resolutions under Chapter VII of the Charter of the United Nations. By virtue of South Africa's United Nations membership, it applies all UNSC resolutions, which relate to among other aspects, the prevention and suppression of terrorism and terrorist financing, as well as the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans and financial or commodity restrictions.

2. The Financial Action Task Force (FATF) Recommendations 6 and 7 require the implementation of UNSC resolutions on targeted financial sanctions for all FATF member countries.

3. South Africa's TFS obligations require accountable institutions to scrutinise information concerning clients against TFS lists, apply freezes to the assets of designated persons or entities, and file terrorist property regulatory reports with the Centre. Furthermore, no persons may provide or make available funding to designated persons or entities.

4. In addition to TFS obligations, accountable institutions must adopt a risk-based approach to ensure their controls are proportionate to the TF and PF risks, and that sufficient resources are focused on heightened risks of TF and PF. The risk-based approach is intended to reinforce and complement the rules-based controls that accountable institutions have in place for TFS.

5. This PCC must be read together with Guidance Note 6A that provides guidance on the terrorist property reporting obligation, the South African National Terrorism Financing Risk Assessment [1], and the FIC TFS manual as available on the Centre's website.

[1] As at date of publication of PCC 44A the South African National Terrorism Financing Risk Assessment as published on 31 March 2022 factors was incorporated. https://www.fic.gov.za/wp-content/uploads/2023/11/2022.03-NRA-2022-Terrorist-Financing-National-Risk-Asssessment.pdf. Accountable institution must rely on the latest versions of National Risk Assessments.

6. This PCC applies to all accountable institutions and other persons.

7. Further information regarding the implementation of the asset freeze requirement of relevant UNSC resolutions can be found in FATF guidance available on its website (https://www.fatf-gafi.org/). Information on the UNSC consolidated list is available on the UNSC website (https://www.un.org/securitycouncil/sanctions/information).

8. This PCC consists of three parts:

Part A – Targeted financial sanctions aimed at combating TF and PF

Part B – Risk-based approach to combating terrorist financing risks

Part C – Risk-based approach to combating proliferation financing risks

PART A – TARGETED FINANCIAL SANCTIONS AIMED AT COMBATING TERRORIST FINANCING AND PROLIFERATION FINANCING

9. The application of UNSC resolutions and FATF Recommendations by South Africa are reflected in sections 26A, 26B, 26C and 28A of the FIC Act and section 4, 15, and 23 of the POCDATARA Act, which collectively sets out TFS obligations for accountable institutions and all other persons in South Africa.

10. Section 26B read together with section 49A of the FIC Act, prohibits the financing of persons or entities who are subject to TFS in terms of section 26A of the FIC Act. The prohibitions relating to TFS regimes are absolute and must be applied by all persons in respect of designated person or entities. No person may directly, indirectly, in whole or in part enter into or facilitate a transaction for persons or entities that are listed on the UNSC resolutions.

11. This prohibition in section 26B of the FIC Act is applicable, but not limited to, all instances where the designated person or entity is:

11.1. The client;
11.2. The person acting on behalf of the client;
11.3. The client acting on behalf of another person;
11.4. A beneficial owner of the client; or
11.5. A party to a client's transaction, including a party who benefits in any way from a client's transaction.

12. The targeted financial sanctions prohibition extends beyond the specific person or entity designated by the UNSC and could include instances where the clients are acting on behalf of another person, or where another person is acting on behalf of the client, or where the client is linked to a sanctioned person or entity.

13. A designated person or entity refers to a specifically named person or entity pursuant to a UNSC resolution, e.g., a person or entity whose name is reflected on a TFS list.

14. Section 4 of the POCDATARA Act read together with section 15 of the POCDATARA Act criminalises the financing and facilitating of terrorist and related activity, which offence applies to everyone subject to South African law, not only accountable institutions.

15. Section 23 of the POCDATARA Act provides a freezing mechanism when there is reason to believe property is that of a designated person or entity, or where there is a reasonable belief terrorist activity is involved.

16. The TFS obligations in terms of the FIC Act include the requirements to scrutinise, freeze and file a regulatory report to the FIC.

Scrutinising client information

17. In terms of section 26A of the FIC Act, the Director of the FIC must give notice of persons or entities who have been designated as sanctioned persons or entities in a resolution of the UNSC. The notice as published by the Director of the FIC communicates updates to the TFS list and is published on the FIC website.

18. Section 28A(3) of the FIC Act requires that an accountable institution must scrutinise its information concerning clients with whom the accountable institution has a business relationship, against the TFS list, to determine if any persons are designated persons or entities or linked to designated persons or entities.

19. The Centre recommends that accountable institutions scrutinise information concerning clients with whom the accountable institution seeks to conclude a single transaction with against the TFS lists as published on the FIC website.

20. There can be no scenario where the accountable institution does not scrutinise information concerning a client when establishing a business relationship. Accountable institutions must scrutinise information concerning clients against the TFS list regardless of any unique factors (e.g., client being a South African national, or transaction is not cross-border etc.) or the level of the perceived risk considered to be low. Screening must be applied for both domestic and international transactions.

21. The results from scrutinising information concerning a client, must be used as a factor that informs the risk rating (e.g., a positive match on a TFS list informs an immediate high-risk rating for the client risk assessment and would result in a freezing and reporting obligation).

22. The accountable institution must apply adequate scrutinising at the appropriate frequency and intensity. Where there is an increased risk of breach of TFS, accountable institutions are cautioned to increase the frequency and amount of information sought to be scrutinised. The higher the TFS risk a particular client type, product, service, or geographic area poses to the institution, the greater the level of scrutiny required of the client's information.

23. Should the accountable institution fail to identify that a person is listed as or linked to a designated person or entity, the accountable institution will be found to be in contravention of the TFS obligation.

24. The accountable institution must obtain and scrutinise sufficient information to make a determination, with a certain level of confidence, that it does not inadvertently provide products or services to the benefit of a designated person or entity. The information concerning a client, includes but is not limited to information concerning the prospective client, existing client, person acting on behalf of the client, beneficial owner or party to a transaction (e.g., originator, intermediary and beneficiary etc.).

25. The information that should be used for scrutinising includes the person's name, identification number, place of birth, address, date of birth, nationality, entity's name and other information. Other information may include, but is not limited to, the country of residence in the case of a natural person.

26. Accountable institutions must have a process implemented and documented as part of its risk management and compliance programme (RMCP) for scenarios where a person or entity is a match on a TFS list, versus when a person or an entity is a false match.

27. The information relating to persons or entities who are linked directly or indirectly to clients, where available and to the extent to which it is known by the accountable institution, should be scrutinised by the accountable institution to determine if such an indirect person or entity is sanctioned.

28. Accountable institutions must scrutinise their information concerning a client:

28.1.1. At client onboarding

28.1.2. When conducting transactions, and

28.1.3. When the TFS list is updated. All existing information concerning clients must be scrutinised against the TFS lists as and when the TFS list is updated.

29. The Centre strongly advises accountable institutions to scrutinise information concerning a client against the TFS list published on the FIC website without delay. Accountable institutions are advised to regularly monitor the FIC website for updates to the TFS list.

30. When a UNSC resolution is adopted designating persons or entities, that resolution has immediate effect in South Africa, which includes for purposes of the application of sections 26B, 26C and 28A of the FIC Act.[2] Accountable institutions may therefore as good practices also scrutinise information concerning clients against the UNSC consolidated sanctions list, in addition to the TFS list as published on the FIC website.

31. It is not the expectation of the FIC that the accountable institution performs extensive monitoring with sophisticated or complex systems to scrutinise information concerning a client. The process adopted for purposes of scrutinising client information against the TFS list can be done manually or through an automated system.

32. Where an accountable institution uses a third-party service provider(s) to assist in scrutinising information concerning a client, the accountable institution remains accountable to comply with its obligation to scrutinise without delay. In the scenario where the third-party service provider incorporates the TFS list notifications as published

[2] The General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022 (Act 22 of 2022) (GLA Act) amended **section 26A(1)** of the FIC Act

on the FIC website in its internal screening tool lists, the accountable institution should consider any risk of delays where internal screening tool lists are not updated without delay. Refer also to PCC 12A which sets out guidance on outsourcing.

33. Where an accountable institution uses a third-party service provider(s) to assist with scrutinising, the accountable institution must document the process in its RMCP and be able to demonstrate that the third-party service provider(s) screening lists include the latest TFS list as published on the FIC website.

34. Failure to scrutinise information concerning a client in accordance with section 28A read together with section 26A of the FIC Act amounts to non-compliance, as accountable institutions remain responsible and cannot delegate their obligation to a third party.

35. The TFS list published on the FIC website is an up-to-date searchable list, that is downloadable and printable for audit records of all searches done. The Centre recommends that as part of the accountable institution's RMCP controls, it keeps record of the results of scrutinising information concerning a client against the TFS list. Further, where the accountable institution uses a third-party service provider(s) for scrutinising purposes, that accountable institution would still have to keep records of scrutinising. The records kept should indicate the date on which scrutinising was done.

Example – manual scrutinising

Accountable institution A scrutinises its client information against the TFS list on the FIC website, which returns "no results". The accountable institution proceeds to save the results as a PDF in the client records.

Example – automated scrutinising

Accountable institution B uses a third-party service provider's automated sanctions screening system, which incorporates the TFS list on the FIC website into its data to scrutinise information concerning clients automatically. Alerts are generated where possible matches are detected, the system has an audit trail of true matches and false matches, and the accountable institution can evidence scrutinising information concerning clients against the TFS list.

36. Institutions that are not accountable institutions are advised to implement a process to scrutinise their client information to ensure that they do not provide products or services to designated persons or entities.

Applicable UNSC resolutions

37. The following UNSC resolutions currently form part of the targeted financial sanctions regime in terms of the FIC Act as at 10 December 2019.

- Somalia Sanctions Regime
- ISIL (Da'esh) and Al-Qaida Sanctions Regime
- Iraq Sanctions Regime
- Democratic Republic of the Congo (DRC) Sanctions Regime
- Sudan Sanctions Regime
- 1636 Sanctions Regime
- Democratic People's Republic of Korea (DPRK) Sanctions Regime
- Libya Sanctions Regime
- 1988 Sanctions Regime
- Guinea-Bissau Sanctions Regime
- Central African Republic (CAR) Sanctions Regime
- Yemen Sanctions Regime
- South Sudan Sanctions Regime
- Haiti Sanctions Regime
- 1540 Sanctions Regime

*These UNSC resolutions listed in the Government Gazette above relate specifically to financial sanctions that have an associated asset freeze obligation.

38. Accountable institutions are reminded that the UNSC resolutions have immediate effect in South Africa (the General Law (Anti-money Laundering and Combating of Terrorism Financing) Amendment Act 2022, amended section 26A of the FIC Act in this regard).

Domestic designation

39. Accountable institutions should note that the South African government may also propose persons or entities or other targets to the UNSC and its various sanctions committees, specifically regarding UNSC Resolution 1267(2001) or 1989(2011); and to the UNSC Resolution 1988 Committee. There is a set designation criterion that is required by the relevant sanctions committee that governments must follow in terms of presenting a statement of case to the UNSC in order to designate an individual or entity in this regard.

40. The importance of filing reports in terms of section 29 of the FIC Act, must be understood in the context of domestic designations. Where an accountable institution suspects that a person or entity may be involved in the financing of terrorism, proliferation of weapons of mass destruction, and/or related activity, the accountable institution must report this through to the Centre, providing as much information and use the most accurate report indicators.

Non-TFS lists

41. Accountable institutions can scrutinise information concerning their clients against other domestic, regional and unilateral sanctions lists published by other regulators or supervisory bodies (e.g. the United States Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons (SDN) list, the United Kingdom HM Treasury's Office for Financial Sanctions Implementation, European Union Sanctions lists etc.) in accordance with its risk-based approach and/or obligations that stem from its correspondent relationships or due to the geographic area in which it operates etc.

41.1. Where there are true matches against these other domestic, regional and unilateral sanctions TFS lists, the accountable institution must determine the course of action in accordance with its obligations and risk-based approach.

41.2. Section 26A, 26B, 26C and 28A of the FIC Act does not apply where the person or entity is not designated on the TFS list as published on the FIC website and UNSC Consolidated Sanctions list.

41.3. Accountable institutions are strongly encouraged to submit a section 29 suspicious and unusual transaction report, where there is a true match against other domestic, regional and unilateral sanctions lists.

41.4. Accountable institutions are advised to seek further guidance from the relevant regulator who published the relevant other domestic, regional and unilateral sanctions list in the case of true matches against those other domestic, regional and unilateral sanctions lists.

Targeted freeze of designated persons or entities property

42. Obligations relating to the freezing of TF and/or PF related funds include:

42.1. An automatic obligation to freeze in terms of section 26B of the FIC Act

42.2. An automatic obligation to freeze in terms of] section 4 of the POCDATARA Act, and

42.3. An *ex-parte* application for a freezing order in terms of section 23 of the POCDATARA Act.

Freeze in terms of section 26B of the FIC Act

43. The effect of the application of section 26B of the FIC Act, is that when an accountable institution identifies a designated person or entity, as its client or linked to its client, the accountable institution must immediately cease any activity in relation to that designated person or entity. This can include not releasing any property to the designated person or entity, and persons acting on behalf of the designated person or entity. This is viewed as and is commonly referred to as a “freeze”.

44. This action of freezing property is the process in which the prohibition can be practically adhered to and is considered an obligation in and of itself. Therefore, an accountable institution does not have to obtain any consent from either the Centre or through a court order to freeze the designated person’s or entity’s property in terms of section 26B of the FIC Act.

45. An accountable institution must have a process in place to ensure the freezing of a designated person’s or entity’s property immediately without delay where the accountable institution is in possession or control of such property. The freeze must also

be applied where it is found that a person is acting on behalf of or at the direction of a designated person or entity, and a freeze should be applied to the related funds.

46. Property also includes assets, any form of monetary value or funds, negotiable instruments (e.g., letters of credit, bills of lading, credit facility) that is owned, held, or controlled directly or indirectly for the benefit of a designated person or entity.

47. The freeze must be applied regardless of whether or not the funds are going to be used in a terrorist attack, an attempted terrorist attack or for the purposes of financing of the proliferation of weapons of mass destruction or related activities. The mere fact that the accountable institution has in its possession or control funds or other assets of a designated person or entity including a person who committed or attempted to commit a terrorist or proliferation activity, is reason sufficient to apply the immediate freeze.

48. An accountable institution must freeze the designated person's or entity's property immediately, without delay. As such an accountable institution must not wait to first report to the Centre that it has in its possession or control property of a designated person or entity or wait to receive any communication from the Centre to freeze such property.

49. Failure to adhere to the prohibition in terms of section 26B of the FIC Act constitutes an offence in terms of section 49A of the FIC Act.

50. The Centre does not prescribe the communication that an accountable institution provides to a client, person or entity upon determining that such client is a designated person or entity impacted by TFS and an asset freeze. The accountable institution can exercise its discretion when determining this communication.

51. The accountable institution must have a documented process in its RMCP to ensure the freezing of a designated person or entity's property immediately, without delay.

52. An accountable institution may not proceed to provide or release any property to a designated person or entity unless prior written permission for such a release has been

obtained from the Minister of Finance, or the Director of the Centre acting upon a delegation from the Minister of Finance, in terms of section 26C of the FIC Act.

53. The accountable institution must not lift the freeze unless the designated person is de-listed by the UNSC and communicated on the UNSC Consolidated List and the TFS list or a permit is obtained in terms of section 26C of the FIC Act. Only funds as allowed for in the permit can be made available to the designated person or entity. The application form for permitted financial services in terms of section 26C of the FIC Act can be found on the FIC website.

Example – Bank in possession of designated person's property

Bank C scrutinises information concerning their client against the TFS lists and finds that Mr T is a designated person on the TFS list in terms of section 26A of the FIC Act. Bank C holds various funds of Mr T in cheque and investment accounts. Bank C immediately ceases to release or facilitate any transactions on behalf of Mr T when it becomes aware Mr T is a designated person. Bank C must, in terms of
of its TFS obligations, apply an automatic freeze on Mr T's funds it has under its possession or control or linked to Mr T. Bank C must report Mr T as a true match and client, as well as the freezing of Mr T's and any links to Mr T's assets to the Centre.

Freezes in terms of the POCDATARA Act

54. Similar to section 26B of the FIC Act, section 4 of POCDATARA Act has the effect that when an accountable institution identifies a designated person or entity or terrorist related activity, the accountable institution must immediately cease any activity in relation to that designated person or entity or terrorist related activity. This can include not releasing any property to the designated person or entity, and persons acting on behalf of the designated person or entity.

55. Accountable institutions should note that section 23 of the POCDATARA Act provides a mechanism for the National Director of Public Prosecutions (NDPP) to apply for an order basically prohibiting any conduct and freezing property linked to a specified offence or designated person or entity, through an *ex-parte* application. The FIC will publish orders

made in terms of section 23 of the POCDATARA Act on the FIC website, for accountable institutions information.

UNSC resolution de-listing process

56. Where a person or entity is de-listed from a TFS list, an accountable institution that has property related to the person or entity now has an obligation to "unfreeze" the property. This can be done automatically, where an accountable institution requires further guidance regarding the proposed action, it may contact the Centre. Refer to the FIC website for further information on de-listing.

Reporting

57. All persons are referred to Guidance Note 6A regarding terrorist property reports (TPRs) and Guidance Note 4B for guidance on suspicious and unusual transaction reports (STRs), as issued by the Centre.

58. The Centre strongly urges persons who are approved to deal in controlled goods or activities to gain an understanding of the various TF and PF typologies and to implement enhanced controls to monitor transactions to identify suspicious and unusual transactions that relate to TF or PF. Where such suspicious and unusual activity is identified, such persons must report this to the Centre in terms of section 29 (STR) of the FIC Act. A reminder that all business has a duty to report STRs to the Centre.

Example of an activity that requires scrutiny

Bank C has a client who is a diplomat, or a national, or legal person of a high PF risk geographic area, and the client is not designated on a TFS list. However, the client's transaction activity is suspicious and unusual. The accountable institution should consider the risk of PF in this scenario and the filing of a STR with the Centre.

59. Accountable institutions must report activity or transactions suspected of being linked to TFS as soon as possible without delay to the Centre in a report in terms of section 29 of the FIC Act, this include instances where a transaction was attempted but not completed.

60. Where a TPR is filed with the Centre, the accountable institution must monitor the designated person's or entity's property and file further TPRs where further transactions are attempted concerning the property.

61. Accountable institutions must report TPRs regardless of the fact that a transaction was not concluded. The mere attempt at making a transaction linked to a designated person or entity, warrants reporting of a TPR.

Risk management and compliance programme

62. The accountable institution's RMCP must provide for the manner in which its will comply with its TFS obligations, including but not limited to:

62.1. The manner in which and processes by which it will scrutinise client information,
62.2. and freeze designated persons and entities' property, and
62.3. The process for reporting to the FIC include filing the TPR in terms of section 28A, as well as filing a terrorist financing transaction report (TFTR) or terrorist financing activity report (TFAR), where there is a suspicion that a transaction or property may involve terrorist financing.

63. The accountable institution's RMCP must provide for the manner in which and processes by which it will identify, access, monitor, mitigate and manage TF risks in terms of section 42 of the FIC Act. The accountable institution's risk-based approach to combating TF must be documented in its RMCP.

64. Accountable institutions must conduct business risk assessments, client level risk assessments, as well as new product and process risk assessments to identify and assess the risk of TF, and implement controls to monitor, mitigate and manage the risk of TF.

65. The Centre strongly encourages accountable institutions to consider the South African National Terrorism Financing Risk Assessment when developing its risk-based approach to CTF. Accountable institutions should consider sector risk assessments and the FIC's published case studies and indicators, when conducting TF risk assessments, which may aid in identifying areas of concern.

66. When assessing the ML, TF, and PF risks, accountable institutions should consider the factors as set out in this draft PCC as well as Guidance Note 7. The list of TF specific risk factors as highlighted below is not an exhaustive list and accountable institutions may determine further risk factors. The accountable institution must be able to demonstrate that it considered risk factors unique to ML, TF and PF, although the risk assessments need not necessarily be separated.

Raising, moving, storing and using funds for terrorist activity

67. To identify risks, the accountable institution should understand the manner in which terrorists raise, move, store and use funds. Terrorist financing usually takes place through three phases. All three phases constitute terrorist financing. The diagram below provides a broad outline of some factors to consider, which include, but are not limited to, the terrorist financing phases.

Raising and sourcing of funds	Moving of the funds	Use of the funds
Criminal activity - proceeds of crimes	Banks	Carrying of attacks

Crowd-funding, donations from the public, charities and non-profit organisation, etc.	Money and value transfer service providers (both formal and informal)	Operational costs of terrorist organisations or persons, including business operational costs, housing, food, transport etc.
Abuse of business entities	Cash movement	Training costs
Abuse of non-profit organisations	Mobile money	Recruitment costs
Other avenues of raising funds?	Crypto asset service providers	Arms and ammunition costs

*FATF report - Ethnically or racially motivated terrorism financing. June 2021. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html

Terrorist financing methods – raising finance for terrorism

68. With terrorist financing, the source of funds could be either legitimate or illegal, this is different to money laundering, where the funds are always from the proceeds of crime. With money laundering, the knowledge and suspicion would predominantly be focused on the source of the funds which is illegal. To identify terrorist financing, accountable institutions must analyse both the source of funds, as well as the intended use of the funds.

69. An important part of combating terrorist financing is understanding the terrorist financing methods. In this way accountable institutions can proactively develop controls aimed at identifying transactions or activity that pose a heightened TF risk. The following financing methods are generally used to fund terrorism. Refer also to the FATF guidance on emerging terrorist financing methods:

69.1. Terrorists receive funds directly from private donors such as wealthy individuals or entities making direct donations. (e.g., caution should be exercised where funds are transferred from private, wealthy clients to high-risk geographic areas etc.).

69.2. Terrorists often abuse non-profit organisations (NPOs) for terrorist financing by a) diverting donations to illegitimate actors, b) criminally abusing legitimate NPOs within the NPO sector, c) establishing fake NPOs or d) affiliating their terrorist organisation under a name similar to a legitimate NPO name, in high-risk geographic areas.

69.3. Organised crime and the proceeds of criminal activity are used to fund terrorist activity. FATF has highlighted credit card fraud, smuggling of precious metals and stones as well as drug trafficking as some of the predicate crimes where the proceeds of crime are channelled toward terrorist activity. The predicate crimes may vary and, therefore, constant analysis of emerging trends in this regard is recommended. Terrorists also loot and steal goods.

69.4. There may be instances where members of a terrorist organisation are charged membership fees, and certain communities may also be subject to a levy.

69.5. Fundraising events such as concerts or market days have been used by certain terrorists.

69.6. Diaspora or foreign émigré nationals who are from geographic areas with a heightened TF risks face extortion by terrorists in their homes or countries of origin. Accountable institutions must conduct enhanced monitoring on cross-border transfers to high-risk geographic areas by such foreign nationals.

69.7. Kidnapping for ransom is another method used to raise funds by terrorists. Large amounts of cash are often transferred across borders as payment for kidnapping ransoms. Accountable institutions should consider as a red flag large cash withdrawals and negative media reports that highlight possible ransom payments.

69.8. Terrorists may also create legitimate businesses to generate proceeds which are then used in terrorist activity. The use of front or shell companies by terrorists poses a heightened risk from a TF perspective. This highlights the importance of accountable institutions identifying and taking reasonable steps to verify beneficial owners. When funds are sent across borders in a manner that is not aligned to the business, this should raise red flags.

69.9. Fundraising through social media, crowd-funding platforms, public donations etc. Funds are raised on public platforms where clients publish account information or crypto addresses to solicit funds form the public. The accounts that receive such funds should be monitored for suspicious and unusual activity. Some typologies in this regard have shown that the terrorists publish their account information on public platforms but do not indicate the purpose for collecting funds. In this way, they attract funds without disclosing or attracting attention to their intended use of the funds.

*The method in which funds are raised, together with the geographic area the funds are destined for, are key risk factors the accountable institution must consider when assessing the risk of TF.

Moving terrorist finances

70. There are various ways in which funds are moved by terrorists which may include:

70.1. **Traditional banking** – Banks enable the fast transfer of funds, domestically and across borders. The large volume of transactions through the banking system makes it difficult to identify often small or negligible amounts destined for TF. An accountable institution's transaction monitoring therefore plays a pivotal role in the fight against TF. Refer to the FIC Directive 5 read together with PCC 45.

Example – client profile monitoring is an important control in identifying suspicious and unusual transactions

Factors which accountable institutions can consider when accessing suspicious and unusual transactions, include, but are not limited to, instances where various micro loans are obtained, the purchase of flight tickets to high-risk regions, the use of funds in and small transfers to or from high-risk geographic areas. Other indicators may be the use of cellular services to and from high-risk regions, which do not match the client's profile, and instances where the client is a South African national with no links to the foreign high-risk region.

Cellular service providers and airlines as businesses have an obligation in terms of section 29 of the FIC Act and are urged to file reports when they become aware of suspicious and unusual transactions.

70.2. **Money value and transfer services (MVTS)** are susceptible to abuse for TF, especially in high-risk geographic areas as more reliance is placed on these services due to the non-availability of formal banking. Accountable institutions must conduct enhanced monitoring of transactions made to high-risk geographic areas. A distinction should be drawn between formally registered and informal MVTS or hawaladars. The risk of TF increases when dealing with informal MVTS providers like hawaladars as there is a lack of regulatory oversight over these alternative or informal funds transfer service providers. Accountable institutions are encouraged to determine whether a client's transaction patterns are indicative that the client provides informal MVTS, and apply enhanced monitoring to these client accounts. Activity indicating a client may possibly be operating an informal MVTS includes pooling of funds followed by large

cross-border transfers. This type of activity should be considered a red-flag indicator. Accountable institutions should apply enhanced monitoring of MVTS transactions through high-risk corridors, which include high-risk geographic areas.

70.3. **Crypto currency** – New technologies including crypto assets are increasingly being used for TF due to the pseudonymous (e.g., transactions can be traced, but not the identity of the parties involved etc.) nature of the crypto assets, the ease of conducting domestic and cross-border transfers, and the fact that crypto transactions are subject to less scrutiny.

70.4. **Cash** – Cash payments enable anonymous transfers, are easily transferable, and leave no audit trail. Money mules, and cash couriers are often used by terrorists to transit funds. Transportation of cash to high-risk areas, numerous cash payments followed by transfers to high-risk geographic areas, and withdrawal of cash in high-risk areas that does not match the client's profile, may be indicators of possible TF. Cash-based economies enable anonymity and the risk of operation of terrorists within high cash-based geographic areas is heightened.

70.5. **Third-party payment providers (TPPPs)** – Accountable institutions should remain aware of the potential abuse of TPPPs as intermediaries for MVTS transfers. The accountable institution should monitor transactions for red-flag indicators, including:

- User or merchant device not recognisable
- Expiration of a device user's immigration permits or visas
- Beneficial ownership information is lacking
- Merchant devices have possibly been used by multiple individuals or more than one operator has access to device
- Excessive remittances over a short period
- Excessive remittances from the same geographical location, as it is common practice to rotate operation of the different "TPPPs"
- The entity's physical address is non-existent

70.6. **Alternative payment methods** – Including contactless payment, pre-paid cards, and mobile money face a heightened risk of being misused for TF. Accountable institutions

should consider examples of how these types of payments methods have been misused or could potentially be exploited for purposes of TF, to identify controls aimed at mitigating the risk of TF.

Storing or using terrorist finances

71. The terrorist finances raise could be used for different purposes which include but are not limited to:

71.1. Supporting terrorists living costs, food, rental, mortgage, petrol, and operations costs.

71.2. Carrying out the terrorist activity, the purchase of goods used for terrorist activity (Business entities that provide controls goods or services must gain an understanding of the terrorist activity risks, examples of dual-use goods include, but are not limited to 3D printers, drones, audio visual components, navigation devices, recreational shooting ranges, chemical products, etc.)

71.3. Recruitment of new members for the terrorism

71.4. Marketing expenses, spread of propaganda e.g., certain publications have been used for terrorism propaganda.

TERRORIST FINANCING RISK ASSESSMENT

72. When assessing TF risk, an accountable institution must consider what areas of their business are vulnerable to TF abuse (e.g., products, services, controls or employees etc.) and the consequences if the terrorist activity would take place through the use of the accountable institution.

73. The consequences of terrorist financing activities are devastating to accountable institutions directly and to the broader society. Accountable institutions should therefore implement the necessary controls required, for a zero tolerance risk based approach to mitigate TF financing risks.

74. Risks associated with TF are constantly changing, and accountable institutions must adapt their risk-based approach to ensure that it is adequate to mitigate new and emerging TF risks.

Client risk factors

75. The outcome of scrutinising client information against the TFS list must be considered when assessing TF risk on a client level. Where a client is found to be designated on a TFS list, this would result in an automatic high-risk rating, and the accountable institution would have to freeze the client assets and report.

76. Different clients pose varying levels of TF risk. To risk rate clients from a TF perspective, the accountable institution should gain an understanding of the different types of:

76.1. Terrorists, terrorist organisations and geographic areas in which the terrorists operate.

76.2. Terrorist behaviour, and terrorist ideologies

76.3. Client types including natural and juristic persons, including beneficial owners that are vulnerable to terrorist behaviour or adhering to terrorist ideology. Various client factors can be taken into account including, but not limited to, nationality and age etc.

77. Trends have shown that terrorist organisations use complex legal structures to evade detection, highlighting the importance of identifying the beneficial owners of clients.

78. There are certain instances of state-sponsored terrorism, dealing with foreign politically exposed persons should be considered as high-risk for this reason, especially where the foreign politically exposed person is from a geographic area which poses a heightened TF risk.

79. Foreign terrorist fighters (FTFs) include natural persons who possibly act alone, or in small groups, as opposed to the larger more advanced terrorist organisations that conduct terrorist activity. FTFs are based in various geographic areas. Developing a client profile which might mirror that of an FTF could aid in identifying TF risk and mitigating that risk.

80. A possible indicator that a person is a lone actor, self-radicalised individual or foreign terrorist fighter, includes where the person travels to or intends to travel to high-risk TF geographic areas. Accountable institutions may identify this red flag from transactional activity to and from that high-risk TF geographic area. As part of the planning or preparing for participating in or supporting a terrorist activity, lone actors, self-radicalised individuals, or FTFs draw funding from various sources (e.g. obtaining numerous credit

loans with different institutions, possibly defaulting on repayments, in a short period of time, followed by transfers to high-risk TF geographic areas etc.).

81. Nationals from geographic areas associated to or susceptible to terrorism pose a heightened risk for TF, especially where such a client(s) submits funds back to their country of nationality. Where an accountable institution identifies fraudulent use of identity, visa, permit documents etc, this might be a red-flag indicator in combination with other sets of facts of possible TF.

82. Certain sectors are high risk from a TF perspective (e.g., trading in precious metals and stones etc.). Accountable institutions may consider conducting enhanced due diligence and request further certifications relating to the relevant trade.

83. The accountable institution should gain an understanding of what type of persons would sympathise with terrorist organisations or extremist ideologies, and this type of information could be factored into the client profiling.

Geographic risk factors

84. A holistic assessment of TF risk must be conducted by the accountable institution, taking into account international risks, risks on a regional level and risks on a domestic level. Accountable institutions should consider regional TF hotspots and developments in countries bordering South Africa.

85. Refer to PCC 49 for further guidance on geographic area risks. Accountable institutions are required to assess the inherent TF risk of a geographic area. FATF guidance, open-source information on terrorism, international case studies, regional conflict zones, academic publications, adverse media reports, credible third-party publications and political instability should be considered in this regard.

86. There are geographic areas that pose a heightened risk of TF, due to funds and resources being diverted through these areas to other geographic areas where terrorism occurs. These geographic areas pose a heightened risk for potential TF financing due to

their proximity to countries where terrorism occurs, infrastructure and financial systems could be exploited by terrorist.

87. According to the South African National Terrorism Financing Risk Assessment, South Africa faces TF risk as a country, due to:

87.1. The presence of FTFs and persons returning from high-risk geographic areas where terrorism occurs,

87.2. The support for foreign terrorist organisations,

87.3. The solicitation of support within South Africa and using the country as a transit hub and base for planning and logistics of terrorist attacks,

87.4. Further growing regional terrorist attacks, and threats of retaliation should South Africa act with regard to regional terrorist activity, and

87.5. The country's porous borders.

88. Geographic areas with high levels of organised crimes, are susceptible to TF risk.

Products and services

89. Different business units within accountable institutions face different levels of TF financing risk. The accountable institution must assess the TF financing risk, each business unit faces. The following are examples of products and services that may pose a heightened risk of being used for TF:

89.1. Cash intensive products,

89.2. Products that provide cross-border transfer of funds,

89.3. Trade finance products

89.4. Product or services that enable transfer of funds easily

90. The accountable institution's RMCP must provide for the manner in which and processes by which it will identify, access, monitor, mitigate and manage PF risks in terms of section 42 of the FIC Act. The accountable institution's risk-based approach to combating PF must be documented in its RMCP.

Risk-based approach

91. In addition to the TFS obligations to scrutinise, freeze and report, the Centre recommends that an accountable institution should adopt a risk-based approach to ensure sufficient resources are focused on heightened risks of PF. This could enhance the accountable institution's ability to apply the broader activity-based financial sanctions.

92. Accountable institutions should conduct business risk assessments, client level risk assessments, as well as new product and process risk assessments to identify and assess the risk of PF, and implement controls to monitor, mitigate and manage the risk of PF.

Heightened PF risks

93. A key risk relating to PF, is the evasion of TFS through the use of legal persons. Designated persons or entities employ different methods in their attempts to avoid detection, or distance themselves from certain transactions, and often attempt to hide behind legal persons, trusts and partnerships. Shell or front companies are used to obscure either the identity of the beneficial owner, the goods and activities being provided, or the geographic area to which goods or activities are destined.

94. A second key PF risk relates to the particular industry in which a client operates and the associated nature of the client's goods and activities offerings. This risk can be further heightened given the nature of the accountable institution's product offering in support of their client.

95. In addition to the risk factors as set out in FIC Guidance Note 7, when assessing the inherent risk of PF, the accountable institutions should have regard to the risk factors

described in this PCC, and any other additional risk factors deemed relevant. The below list is not an exhaustive list and accountable institutions may consider other risk factors.

Client risk factors

96. Whether any person including the client, the person acting on behalf of the client, beneficial owner, party to a transaction is a:

96.1. Designated person or entity (this would be a clear indicator that the business relationship or single transaction poses a high PF risk)

96.2. National of or based in a geographic area that is subject to PF TFS (e.g., Consider the UNSCR 2397(2017), which requires member states to repatriate income earning North Koreans, with few exemptions); or

96.3. National of or based in a geographic area that is a concern due to possible diversion of funding or resources to a PF TFS country.

97. The client, beneficial owner, or person acting on behalf of the client is a foreign prominent influential person, high-risk domestic prominent influential person or government entity dealing in a high-risk sector such as arms and ammunitions or trading in other controlled goods and activities (dual-use goods or technology).

98. The client is represented by a third party in a manner that is not aligned to the client profile or that does not make business sense or seems unnecessary. Where there is an unusual or unexplained third party acting on behalf of the client this may be an indicator of a high-risk transaction.

99. The client's legal structure appears overly complex, which may be an attempt to hide beneficial owners that are subject to PF TFS.

100. The client is a legal person but functions as a shell or front company and does not have actual operations in an industry that may indicate a heightened PF risk. Some indicators of shell or front companies include but are not limited to: unrelated companies that have the same employees, and often transact with one another, unrelated companies share the same addresses, phone numbers or similar

registration information and transact with the same third parties, there is a notable lack of online presence, where a large entity has no website, and the entities name is very generic and could easily be mistaken for another well-known entity.

101. The use of joint ventures by legal persons to evade TFS (e.g., Consider the UNSCR 2375 (2017), which requires member states to prohibit joint ventures with North Korea, with few exemptions).

102. There are clients who offer certain products and services that face a heightened risk of being abused for PF. Examples of these may include but are not limited to import and export businesses (e.g. freight forwarders, airlines, road couriers, warehouses, vessels, shipping companies, maritime companies, clearing agents, import and export insurance companies, credit and insurance providers, among others), ports of entry, chemical manufacturing companies, precious metal dealers, as well as arms and ammunition manufacturers.

103. The nature of the client's business, including the industry in which the client operates, or the type of products and services the client provides are linked to controlled goods and activities (dual-use goods).

104. Where a client deals in controlled goods or activities and does not have approval from the relevant regulatory authority to do so, this may be an indicator that that client poses a heightened PF risk.

Controlled goods and activities

Accountable institutions are urged to consult and scrutinise the list of controlled goods and activities as published by the South African Council for the Non-Proliferation of Weapons of Mass Destruction (Non-Proliferation Council), which may serve as a guide to accountable institutions for purposes of determining and assessing the PF risks relating to the client's sector, and the goods and activities in which the client deals.
Controlled goods and activities include goods that have "*dual-purpose capabilities" relating to technology, expertise, service, material, equipment and facilities 'which' can*

contribute to the proliferation of weapons of mass destruction, but which can also be used for other purposes, including conventional military, commercial or educational use[3]" (e.g., include technologies like drones).

The reader may refer to the NPWMD guidance products available on the Non-Proliferation Council's website for further information.

There are various other lists that may apply, given the parties to a transaction and correspondent obligations. In addition, the UNSC publishes a list of prohibited items.

List of sources of controlled goods, activities and/or dual-use goods

http://non-proliferation.thedtic.gov.za/

https://www.un.org/securitycouncil/sanctions/1718/prohibited-items

https://www.gov.za/sites/default/files/gcis_document/201409/35272gon321.pdf

Geographic area risk factors

105. The geographic area in which either the client, the person acting on behalf of the client, beneficial owner, or persons who are party to the transaction are based is a geographic area that is:

105.1. Subject to PF TFS (e.g., the Democratic Republic of Korea (DPRK) or North Korea is specifically listed as being high-risk for PF concerns). The Centre's PCC 49 provides further guidance on geographic risks;

105.2. An area of concern due to the diversion of funds or resources to a geographic area subject to PF TFS (e.g., where the country is not listed but supports or aids sanctioned countries), also consider the proximity to the high risk geographic; or

105.3. An area of concern due to weak AML, CFT and CFP laws or export control laws and enforcement.

[3] The Non-Proliferation of Weapons of Mass Destruction Act 87 of 1993

106. Controlled goods and activities that are provided to geographic areas that do not seem to have the required skill or technology to deal with the controlled goods and activities, is a red-flag indicator of possible evasion of TFS.

Product risk factors

107. There are certain product risk factors that could increase the vulnerability of accountable institutions and could result in heightened PF risks. These may include:

107.1. **Trade finance** which involves the financing of the import and export of goods and can include controlled goods or activities.

107.2. Trade finance transactions may be complex and involve the movement of funds to or from geographic areas that present a high PF risk.

107.3. There are various parties to a trade finance transaction, who may be subject to PF TFS. The use of front or shell companies by bad actors in trade finance arrangements remains a heightened risk.

107.4. There are various trade finance transaction red-flag indicators which include but are not limited to inconsistencies in information or documentation provided, false documentation, over-invoicing, under-invoicing, and circular type transactions where the beneficiary turns out to be the originator of that same transaction.

107.5. Accountable institutions should gain an understanding of the trade patterns and the sector's high-risk geographic areas to better understanding and mitigate the risks. (e.g., North Korean front companies may deal in certain import and export of textiles, garments, fish, other seafood industries, etc.)

Example – Abuse of trade finance transactions for PF

Bank Y is financing a trade agreement where, following the review of the bill of lading, it is found that the shipping vessel is subject to PF TFS. Bank Y's client is not a designated person or entity, however, the agreement will financially benefit a designated entity. Therefore, Bank Y cannot proceed with the payment.

108. **Correspondent banking** which is the provision of banking services by one bank to another bank, and services include international transactions and cash management. An accountable institution should assess whether their correspondent bank operates in or

has any links to geographic areas with heightened PF risks, or links to persons including beneficial owners who are designated persons or entities. Accountable institutions should understand the controls the correspondent bank has in place to combat PF.

109. **Foreign exchange** which refers to the conversion of one country's currency into another country's currency. Where foreign exchange payments are made to or received from countries that pose a heightened PF risk, accountable institutions should consider the risk of possible evasion of TFS.

110. **New technologies** including crypto assets are increasingly being used for PF due to the pseudonymous nature of the crypto assets, the ease of domestic and cross-border transfer, and the fact that crypto transactions are subject to less scrutiny.

111. **Cash payments** as it enables anonymous transfer of funds, is easily transferable and leaves no audit trail. For these reasons cash payments to or from accounts of clients that pose a high risk from a PF perspective, is a red flag.

Other risk factors

112. False documentation or documentation that seems unusual could indicate an attempt to evade sanctions. Criminals often attempt to obscure the true nature of goods, destination of goods, beneficiary, the originator, intermediary or vessel etc. through false documentation.

113. Adverse information relating to PF on the end use and end user of the controlled goods and activities.

114. Deceptive shipping practices which include but are not limited to:

114.1. Altering vessel names and numbers to conceal identity,

114.2. Conducting ship to ship transfers at sea, of controlled goods

114.3. Disabling or manipulating the shipping vessel's identification systems, so that vessel movement is not tracked.

115. Supply chain risks include but are not limited to:

115.1. Instances where suppliers outsource work to high-risk geographic areas without informing parties to the supply contract.

115.2. Excessive pricing in the form of low prices by high-risk entities

115.3. Sale of information technology goods and services from high-risk geographic areas or entities, which goods or services can be used for military and law enforcement purposes.

Customer due diligence

116. Information on who has approval to deal in controlled goods and services is not made available publicly. This information is held confidentially by the relevant regulatory bodies. The accountable institution should, in accordance with its risk-based approach, enquire whether the client who deals in controlled goods or activities has approval from the relevant regulatory body (e.g., Non-Proliferation Council).

Example – Enhanced due diligence for controlled goods and activities

Upon processing a trade finance transaction, Bank A becomes aware that the transaction involves controlled goods and activities. As part of Bank A's risk-based approach, it requests a self-declaration from the client, to determine whether or not the client is authorised to transact in the controlled good or activities.

117. Where a client poses a higher PF risk, an accountable institution must conduct enhanced due diligence, and is encouraged to obtain the following additional information:

117.1. Immediate family members and known close associates

117.2. Past nature of business or occupation

117.3. Information on financial statements

117.4. Information available on media, and the internet

117.5. End user information and end users of the controlled goods and activities; and information of the authorisation of the end user, and intermediaries to the transaction.

*This list of additional information is not exhaustive.

118. It is critical for an accountable institution to conduct ongoing due diligence and enhanced account monitoring on high-risk business relationships. This includes assessments of transactional information and documentation to be able to identify suspicious and unusual transactions and activities, including possible PF or evasion of PF controls and PF TFS.

119. As part of ongoing due diligence, an accountable institution should analyse whether transactions processed for clients presenting a heightened PF risk are consistent with any permits or authorisation issued to that client, and other documentation that forms part of the transactions.

120. When assessing a high-risk transaction, an accountable institution should request additional client, transactional and end-user information as is necessary, so as to not breach TFS obligations. The additional information may include but is not limited to the beneficial ownership information of all the parties to the transaction and end users.

121. Where additional information is required to clarify whether or not a transaction poses a PF risk, and such information is not provided, the accountable institution should consider submitting a report in terms of section 29 of the FIC Act.

122. The accountable institution may also scrutinise the client information against the TFS lists more frequently.

De-risking

123. In addition to the principles as set out in Guidance Note 7, it is not considered effective or adequate risk management if an accountable institution decides to de-risk a client for the mere fact that the business relationship or single transaction with the client poses a heightened PF/ TF risk. (When dealing with designated persons or entities directly or indirectly however, the accountable institution must freeze and report in compliance with its TFS obligations)

124. It is the Centre's view that where an accountable institution de-risks solely based upon the fact that there is a heightened risk, then that accountable institution has not complied with its obligation to follow a risk-based approach.

125. Where an accountable institution takes the decision to not onboard a certain category of clients, the accountable institution must be able to demonstrate the application of a risk-based approach in terms of which risk factors have been considered.

126. Ineffective application of de-risking can cause inadvertent consequences including the loss of valuable information through regulatory reporting to the Centre.

127. The Centre does not prescribe the circumstances under which an accountable institution should seek to terminate a business relationship, accountable institutions must exercise their discretion in this regard.

128. Accountable institutions are reminded of their obligations to not tip off a client where suspicious and unusual activity is suspected. Where a person or entity is designated on a TFS list, the person or entity would in all probability be aware of the designation, in this regard, freezing the client's funds and other assets would not amount to tipping the client off that they are listed on a TFS list.

129. An accountable institution must not process transactions where they are unable to determine accurately whether such transactions would breach TFS obligations. Where the accountable institution is uncertain whether a person or an entity is a designated person or entity, the accountable institutions may seek independent legal advice.

Issued By:

The Acting Director Financial Intelligence Centre

23 November 2023

List of resources

- The Financial Action Task Force Recommendations
- Financial Action Task Force, International best practices – Targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6), June 2015
- Financial Action Task Force, Guidance on Counter Proliferation Financing the Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, February 2018
- Financial Action Task Force, report – *Ethnically or racially motivated terrorism financing*, June 2021
- HM Treasury, Office of Financial Sanctions Implementation – UK Financial sanctions. General guidance for financial sanctions under the Sanctions and Anti-money Laundering Act 2018. August 2022
- HM Treasury, Office of Financial Sanctions Implementation – Maritime Guidance. December 2020
- HM Treasury, Office of Financial Sanctions Implementation – Importers and Exporters – Financial Sanctions frequently asked questions. December 2020
- HM Treasury, Office of Financial Sanctions Implementation – Charity sector guidance. December 2020