INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF
TERRORISM & PROLIFERATION

The FATF Recommendations

Updated June 2026

FINANCIAL ACTION TASK FORCE

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 (CFT) standard.

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

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.

Citing reference:

FATF (2012-2026), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

© 2012-2026 FATF/OECD. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING
OF TERRORISM & PROLIFERATION

THE FATF RECOMMENDATIONS

ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012

Updated June 2026

CONTENTS

List of the FATF Recommendations 4

Introduction 7

FATF Recommendations 10

Interpretive Notes 31

Note on the legal basis of requirements on financial institutions and DNFBPs 123

Glossary 125

Table of Acronyms 142

Annex I: FATF Guidance Documents 143
Annex II: Information on Updates made to the FATF Recommendations 144

© 2012-2026

THE FATF RECOMMENDATIONS

© 2012-2026

Number	Old Number[1]	
		A – AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination *
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism and terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence *
11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies *
16	SRVII	Payment transparency *
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *

© 2012-2026

		E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs *
		Operational and Law Enforcement
29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *

1. *The 'old number' column refers to the corresponding 2003 FATF Recommendation.*

* *Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.*

Version as adopted on 15 February 2012.

INTRODUCTION

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996, the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

© 2012-2026

Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.

The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are proportionate to the nature of risks, in order to focus their efforts in the most effective way.

Combating terrorist financing is a very significant challenge. An effective AML/CFT system, in general, is important for addressing terrorist financing, and most measures previously focused on terrorist financing are now integrated throughout the Recommendations, therefore obviating the need for the Special Recommendations. However, there are some Recommendations that are unique to terrorist financing, which are set out in Section C of the FATF Recommendations. These are: Recommendation 5 (the criminalisation of terrorist financing); Recommendation 6 (targeted financial sanctions related to terrorism & terrorist financing); and Recommendation 8 (measures to prevent the misuse of non-profit organisations). The proliferation of weapons of mass destruction is also a significant security concern, and in 2008 the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction. To combat this threat, the FATF has adopted a new Recommendation (Recommendation 7) aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

© 2012-2026

The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation, and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

© 2012-2026

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are proportionate to the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they should allow and encourage simplified measures as appropriate.

Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7. Countries should take proportionate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose. Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are proportionate to the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective and risk-based action to mitigate their money laundering, terrorist financing and proliferation financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT/CPF policies, informed by the risks[1] identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with

[1] Proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

© 2012-2026

each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

© 2012-2026

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should ensure that they have policies and operational frameworks that prioritise asset recovery in both the domestic and international context.

Taking into account the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption, and the Terrorist Financing Convention, countries should have measures, including legislative measures, to enable their competent authorities to:

a) identify, trace and evaluate criminal property and property of corresponding value;

b) suspend or withhold consent to a transaction;

c) take any appropriate investigative measures;

d) expeditiously carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of criminal property and property of corresponding value;

e) confiscate criminal property and property of corresponding value through conviction-based confiscation;

f) confiscate criminal property through non-conviction based confiscation;

g) enforce a resulting confiscation order; and

h) ensure effective management of property that is frozen, seized or confiscated.

© 2012-2026

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing *

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation *

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations *

Countries should identify the organisations which fall within the FATF definition of non-profit organisations (NPOs) and assess their terrorist financing risks. Countries should have in place focused, proportionate and risk-based measures, without unduly disrupting or discouraging legitimate NPO activities, in line with the risk-based approach. The purpose of these measures is to protect such NPOs from terrorist financing abuse, including:

(a) by terrorist organisations posing as legitimate entities;

(b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

(c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

© 2012-2026

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are payments or value transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

© 2012-2026

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

© 2012-2026

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and source of funds; and

(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking *

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) clearly understand the respective responsibilities of each institution; and

(e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

© 2012-2026

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services *

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Payment transparency *

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on payments or value transfers and related messages. This information should be structured to the extent possible and should remain with such payment or value transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor payments or value transfers for the purpose of detecting those which lack required originator and/or beneficiary information and take appropriate measures.

Countries should ensure that, in the context of processing payments or value transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security

© 2012-2026

Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing, and resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties *

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries *

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

© 2012-2026

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries *

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions *

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

(a) protected by law from 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, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence *

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

© 2012-2026

(b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

© 2012-2026

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

© 2012-2026

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons *

Countries should assess the risks of misuse of legal persons for money laundering or terrorist financing, and take measures to prevent their misuse. Countries should ensure that there is adequate, accurate and up-to-date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently by competent authorities, through either a register of beneficial ownership or an alternative mechanism. Countries should not permit legal persons to issue new bearer shares or bearer share warrants, and take measures to prevent the misuse of existing bearer shares and bearer share warrants. Countries should take effective measures to ensure that nominee shareholders and directors are not misused for money laundering or terrorist financing. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements *

Countries should assess the risks of the misuse of legal arrangements for money laundering or terrorist financing and take measures to prevent their misuse. In particular, countries should ensure that there is adequate, accurate and up-to-date information on express trusts and other similar legal arrangements including information on the settlor(s), trustee(s) and beneficiary(ies), that can be obtained or accessed efficiently and in a timely manner by competent authorities. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

© 2012-2026

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory 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. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs *

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

© 2012-2026

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize criminal property and property of corresponding value. Countries should also make use, when necessary, of permanent or

© 2012-2026

temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence. Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery.

Countries should ensure that competent authorities have timely access to a wide range of information, particularly to support the identification and tracing of criminal property and property of corresponding value. This may include, but is not limited to, basic and beneficial ownership information, information held by tax authorities, information held in asset registries (such as for land, property, vehicles, shares, or other assets), and information held in citizenship, residency, or social benefit registries.

In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

© 2012-2026

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

© 2012-2026

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

(a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

(b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

(e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

© 2012-2026

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation *

Countries should have measures, including legislative measures, to take expeditious action in response to requests by foreign countries seeking assistance to identify, trace, evaluate investigate, freeze, seize and confiscate criminal property and property of corresponding value. These measures should also enable countries to recognise and enforce foreign freezing, seizing, or confiscation orders. Further, countries should be able to manage property subject to confiscation at all stages of the asset recovery process and share or return confiscated property.

Countries should have in place the widest possible range of treaties, arrangements, or other mechanisms to enhance cooperation in asset recovery.

© 2012-2026

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

(a) ensure money laundering and terrorist financing are extraditable offences;

(b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

(c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

(d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation.

© 2012-2026

Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

© 2012-2026

INTERPRETIVE NOTES TO THE FATF RECOMMENDATIONS

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING ML/TF RISKS AND APPLYING A RISK-BASED APPROACH)

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial businesses and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are proportionate to the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, countries should allow and encourage[2] financial institutions and DNFBPs to take simplified measures. Countries should identify areas of lower risk, for example, through their national or sub-national risk assessments, to support financial institutions and DNFBPs to apply measures proportionate to those risks. Countries should provide guidance or information to financial institutions and DNFBPs on the possible approaches for the implementation of simplified measures where the risks are lower. However, simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in limited circumstances and where there is an assessed low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

[2] For example, encouragement can take the form of guidance issued by the government, supervisor or other competent authority to improve understanding of the circumstances when simplified measures may be appropriate and what form they may take, or outreach or other forms of engagement with financial institutions and DNFBPs.

© 2012-2026

ASSESSING PROLIFERATION FINANCING RISKS AND APPLYING RISK-BASED MEASURES

3. In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.[3] These obligations set out in Recommendation 7 place strict requirements on all natural and legal persons, which are not risk-based. In the context of proliferation financing risk, risk-based measures by financial institutions and DNFBPs seek to reinforce and complement the full implementation of the strict requirements of Recommendation 7, by detecting and preventing the non-implementation, potential breach, or evasion of targeted financial sanctions. In determining the measures to mitigate proliferation financing risks in a sector, countries should consider the proliferation financing risks associated with the relevant sector. By adopting risk-based measures, competent authorities, financial institutions and DNFBPs should be able to ensure that these measures are proportionate to the risks identified, and that would enable them to make decisions on how to allocate their own resources in the most effective way.

4. Financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks.[4] This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take proportionate measures to manage and mitigate the risks. Where the risks are lower, they should ensure that the measures applied are proportionate to the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

---

[3] Paragraphs 1 and 2 of the Interpretive Note to Recommendation 7, and the related footnotes, set out the scope of Recommendation 7 obligations; including that it is limited to targeted financial sanctions and does not cover other requirements of the UNSCRs. The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15 only. The requirements under Recommendation 1 for PF risk assessment and mitigation, therefore, do not expand the scope of other requirements under other Recommendations.

[4] Countries may decide to exempt a particular type of financial institution or DNFBP from the requirements to identify, assess, monitor, manage and mitigate proliferation financing risks, provided there is an assessed low risk of proliferation financing relating to such financial institutions or DNFBPs. However, full implementation of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

© 2012-2026

A. Obligations and decisions for countries

ML/TF risks

5. **Assessing ML/TF risks** - Countries[5] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources proportionate to the ML/TF risks by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

6. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

7. **Lower risk** - Countries should allow and encourage the use of simplified measures by financial institutions and DNFBPs for FATF Recommendations requiring financial institutions or DNFBPs to take risk-based actions, provided that a lower risk has been identified with due regard to the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 5.

   Independent of any decision by a country to specify certain lower risk categories in line with the first part of paragraph 7, countries should allow and encourage financial institutions and DNFBPs to apply simplified measures, subject to the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 9 below.

8. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

   (a) there is an assessed low risk of money laundering and terrorist financing; the exemption occurs in limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

   (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

---

[5] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

© 2012-2026

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

9 **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively and proportionately implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles, risk assessments and risk mitigation measures undertaken by financial institutions and DNFBPs, and take the result of this review into consideration.

PF risk

10. **Assessing PF risk** - Countries [6] should take appropriate steps to identify and assess the proliferation financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's CPF regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of CPF resources by competent authorities; and (iii) make information available for PF risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and SRBs, financial institutions and DNFBPs.

11. **Mitigating PF risk** - Countries should take appropriate steps to manage and mitigate the proliferation financing risks that they identify. Countries should develop an understanding of the means of potential breaches, evasion and non-implementation of targeted financial sanctions present in their countries that can be shared within and across competent authorities and with the private sector. Countries should ensure that financial institutions and DNFBPs take steps to identify circumstances, which may present higher risks and ensure that their CPF regime addresses these risks. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take proportionate measures to manage and mitigate these risks. Correspondingly, where the risks are lower, they should ensure that the measures applied are proportionate to the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

B. Obligations and decisions for financial institutions and DNFBPs

ML/TF risks

12. **Assessing MF/TF risks** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any

[6] Where appropriate, PF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

© 2012-2026

assessment of money laundering and terrorist financing risks should be appropriate and proportionate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

13. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those policies, controls and procedures, and apply proportionate measures in line with the risks. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be proportionate to the risks as identified and consistent with national requirements and with guidance from competent authorities and SRBs.

14. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.

15. **Lower risk** - Where lower risks are identified, financial institutions and DNFBPs should be allowed and encouraged to take simplified measures to manage and mitigate those risks.

16. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs should consider differentiating the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but simplified or enhanced CDD for ongoing monitoring, or vice versa) to mitigate the risk.

PF risk

17. **Assessing PF risk** - Financial institutions and DNFBPs should be required to take appropriate steps, to identify and assess their proliferation financing risks. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

18. **Mitigating PF risk** - Financial institutions and DNFBPs should have policies, controls and procedures to manage and mitigate effectively the risks that have been identified. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior

© 2012-2026

management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take proportionate measures to manage and mitigate the risks (i.e. introducing enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7). Correspondingly, where the risks are lower, they should ensure that those measures are proportionate to the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

Glossary of specific terms used in the context of this Recommendation	
Proportionate	in the context of the risk-based approach adopted by the FATF Recommendations, a proportionate or commensurate measure or action is one that appropriately corresponds to the level of identified risk and effectively mitigates the risks.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 2 (NATIONAL COOPERATION AND COORDINATION)

1. Countries should establish appropriate inter-agency frameworks for co-operation and co-ordination with respect to combating money laundering, terrorist financing and the financing of proliferation. These may be a single framework or different frameworks for ML, TF and PF respectively.

2. Such frameworks should be led by one or more designated authorities, or another mechanism that is responsible for setting national policies and ensuring co-operation and co-ordination among all the relevant agencies.

3. Inter-agency frameworks should include the authorities relevant to combating ML, TF and PF. Depending on the national organisation of functions, authorities relevant to such frameworks could include:

    a) The competent central government departments (e.g. finance, trade and commerce, home, justice and foreign affairs);

    b) Law enforcement, asset recovery and prosecution authorities;

    c) Financial intelligence unit;

    d) Security and Intelligence agencies;

    e) Customs and border authorities;

    f) Supervisors and self-regulatory bodies;

    g) Tax authorities;

    h) Import and export control authorities;

    i) Company registries, and where they exist, beneficial ownership registries; and

    j) Other agencies, as relevant.

4. Countries should ensure that there are mechanisms in place to permit effective operational co-operation, and where appropriate, co-ordination and timely sharing of relevant information domestically between different competent authorities for operational purposes related to AML, CFT and CPF, both proactive and upon request. These could include: (a) measures to clarify the role, information needs and information sources of each relevant authority; (b) measures to facilitate the timely flow of information among relevant authorities (e.g. standard formats and secure channels), and (c) practical mechanisms to facilitate inter-agency work (e.g. joint teams or shared data platforms).

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.

3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.

4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

5. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

7. Countries should ensure that:

   (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.

   (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.

   (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of

© 2012-2026

liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

(d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 4 (CONFISCATION AND PROVISIONAL MEASURES)

A. Prioritisation and asset recovery frameworks

1. Countries should review their asset recovery regime to ensure its ongoing effectiveness and provide sufficient resources to effectively pursue asset recovery.

2. Consistent with Recommendation 2, countries should ensure that they have the necessary domestic cooperation and coordination frameworks and agency structures to enable effective use of the measures below.

B. Criminal property and property of corresponding value

3. Criminal property and property of corresponding value extends to property owned or held by third parties, but without prejudicing the rights of bona fide third parties. Examples of circumstances where property is owned or held by non-bona fide third parties and could be criminal property or property of corresponding value include:

   (a) property under the effective control of the defendant or person under investigation and, for example, held or owned by family members, associates or legal persons and arrangements; or

   (b) where the property has been gifted or transferred to the third party for an amount significantly above or below market value.

C. Provisional measures

4. In response to relevant information, countries should enable the FIU or other competent authority to take immediate action, directly or indirectly, to withhold consent to or suspend a transaction suspected of being related to money laundering, predicate offences, or terrorist financing. The maximum duration of this measure should be specified and allow sufficient time to analyse the transaction and for competent authorities to initiate, where appropriate, an action to freeze or seize.

5. Countries should have measures, including legislative measures, to enable their competent authorities to expeditiously carry out provisional measures. This should include:

   (a) allowing the initial application to freeze or seize criminal property and property of corresponding value to be made ex parte or without prior notice;[7] and

   (b) ensuring that provisional measures do not have unreasonable or unduly restrictive conditions for effective action, such as in relation to demonstrating the risk of dissipation.

---

7 *Ex parte* proceedings may be subject to appropriate safeguards under domestic law, including the triggering of notice or an i*nter partes* review after the implementation of the provisional measure.

© 2012-2026

6. When necessary to act as expeditiously as possible, countries should enable competent authorities to freeze and seize criminal property and property of corresponding value without a court order, with such action reviewable through judicial proceedings within a period of time. If either or both freezing or seizing without a court order is inconsistent with fundamental principles of domestic law, a country may use an alternative mechanism if it enables their competent authorities to systematically take action quickly enough to prevent the dissipation of criminal property and property of corresponding value.

7. Countries should have measures, including legislative measures, that enable their competent authorities to take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or confiscate criminal property and property of corresponding value.

D. Confiscation

8. Countries need a comprehensive range of measures, including legislative measures, available to confiscate criminal property and property of corresponding value, including those measures in paragraphs (9)-(13) below. Which measures, or combination of measures, will be applied depends on the circumstances of the case. It is also important for such measures to be implemented in a manner which respects the substantive and procedural rights and safeguards that may be implicated by confiscation.

9. Countries should have measures, including legislative measures, to enable the confiscation of criminal property and property of corresponding value following the conviction of a person.

10. To the extent that such a requirement is consistent with fundamental principles of domestic law, countries should have measures, including legislative measures, which enable confiscation to be extended to other property of a person convicted of money laundering, predicate offences,[8] or terrorism financing where the court is satisfied that such property is derived from criminal conduct.[9]

11. Countries should have measures, including legislative measures, to enable the confiscation of criminal property without requiring a criminal conviction (non-conviction based confiscation) in relation to a case involving money laundering, predicate offences[10] or terrorism financing, to the extent that such a requirement is consistent with fundamental principles of domestic law. Countries have flexibility in how they implement non-conviction based confiscation.

12. Countries should consider adopting measures which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation.

---

8 Countries may limit the application of extended confiscation to serious offences consistent with Recommendation 3.

9 In determining whether the property in question is derived from criminal conduct, this could include, for example, whether the value of the property represents the proceeds of a criminal lifestyle or is disproportionate to the lawful income of the convicted person.

10 Countries may limit the application of non-conviction based confiscation to serious offences consistent with Recommendation 3.

© 2012-2026

E. Asset recovery and tax authorities

13. Countries should enable their competent authorities and tax authorities to cooperate and, where appropriate, coordinate and share information domestically with a view to enhancing asset recovery efforts and supporting the identification of criminal property. This could, in appropriate cases, where there is a tax liability, support the recovery of such liabilities by the tax authorities.

F. Asset management, return and disposal

14. Countries should have effective mechanisms for managing, preserving, and, when necessary, disposing of, frozen, seized, or confiscated property. Preservation of the value of property should include the pre-confiscation sale of property, where appropriate.

15. Countries should consider establishing an asset recovery fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

16. Countries should ensure that they have measures that enable them to enforce a confiscation order and realise the property or value subject to the confiscation order, leading to the permanent deprivation of the property or value subject to the order.

17. Countries should have mechanisms to return confiscated property to its prior legitimate owners or to use it to compensate victims of crime.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. Objectives

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. Characteristics of the terrorist financing offence

2. Terrorist financing offences should extend to any person who wilfully 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: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

3. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.

5. Terrorist financing offences should extend to any funds or other assets, whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.

8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.

9. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

10. It should also be an offence to attempt to commit the offence of terrorist financing.

11. It should also be an offence to engage in any of the following types of conduct:

© 2012-2026

(a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

12. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 6 (TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[11] or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions[12]; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)[13]. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

---

11 Natural or legal person.

12 Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

13 Based on requirements set, for instance, in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention) and the United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention), which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention) contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

© 2012-2026

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions[14]. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

   (a) Countries should identify a competent authority or a court as having responsibility for:

      (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

      (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

      (iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own

[14] The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

© 2012-2026

motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

(b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.

(c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.

(e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:

(i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;

© 2012-2026

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and

(iv) specify whether their status as a designating state may be made known.

(f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:

(i) follow the procedures for listing, as adopted by the 1988 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

(g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

© 2012-2026

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

5bis. When taking measures to implement asset freezes imposed by the United Nations Security Council or its Sanctions Committees under Chapter VII of the UN Charter, countries should comply with the provisions of resolution 2664 (2022), resolution 2761 (2024), and resolution 2615 (2021), as applicable.[15]

6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

   (a) Countries[16] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

   (b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or

---

15 The provisions of resolution 2664 concerning humanitarian activities apply to all existing and future asset freezes imposed or renewed by the Security Council, in the absence of an explicit decision by the Security Council to the contrary; however, as to Afghanistan, the specific provisions contained in paragraph 1 of resolution 2615 still apply with respect to the asset freeze measures contained in paragraph 1(a) of resolution 2255 (as confirmed by paragraph 4 of resolution 2664).

16 In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

© 2012-2026

other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Without prejudice to the obligation to implement the measures described above in (a) and (b) when such asset freezes are imposed by the Security Council or its Sanctions Committees, countries should apply the provisions of the resolutions referenced in 5bis.[17]

(d) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(e) Countries should require financial institutions and DNFBPs[18] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

(f) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988

---

17 This means that the provision, processing, or payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance or to support other activities that support basic human needs, are permitted and are not a violation of the asset freezes imposed by the UN Security Council or its Sanctions Committees. The permission applies to such humanitarian activities carried out by the actors described in UNSCR 2664, paragraph 1, and providers under UNSCR 2615, paragraph 1.

Countries have the obligation to apply these provisions when they implement sanctions issued by the UN Security Council or its Sanctions Committees. Countries may also apply these provisions to sanctions they may impose at the (supra-) national level, such as those pursuant to UNSCR 1373.

Countries have flexibility in how they implement the relevant UN resolutions. Recommendation 6 does not prescribe how countries should comply with these humanitarian provisions. Several approaches exist, including, but not limited to: exemptions, general licences, legislative carve-outs, or other measures, depending on the legal framework used by the country to implement UN sanctions.

18 Security Council resolutions apply to all natural and legal persons within the country.

© 2012-2026

Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

© 2012-2026

(a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**[19]:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof[20]; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

(b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions**:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

(c) **Security Council resolution 1373 (2001)**:

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

---

19 Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

20 OP2 of resolution 1617 (2005) further defines the criteria for being "associated with" Al-Qaida or Usama bin Laden.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[21] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person[22] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[23]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.[24] The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the

---

21 Recommendation 7 is focused on targeted financial sanctions. However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

22 Natural or legal person.

23 Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretive Note (October 2025), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). The Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction related to Iran are: resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010).

24 Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and UNSCR 1540 (2004) and 2325 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

© 2012-2026

Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) and 1737 (2006) provide that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

   (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

      (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions[25], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

      (ii) proposing to the 1737 Sanctions Committee, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 1737 (2006) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

   (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 1737 (2006), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

   (c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

   (d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent

[25] Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

© 2012-2026

authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

(e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the 1737 Sanctions Committee, pursuant to resolution 1737 (2006) and any future successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(f) having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

(a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[26]; and

(b) in the case of resolution 1737 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the 1737 Sanctions Committee of the Security Council, when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries[27] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons

[26] As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

[27] In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

© 2012-2026

and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBPs[28] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

(e) Countries should adopt effective measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

(f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures

[28] Security Council resolutions apply to all natural and legal persons within the country.

© 2012-2026

adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e., a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

9. Where countries have determined that the exemption conditions set out in resolution 1718(2006), resolution 1737 (2006) or resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 1737 (2006) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

    (a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in the relevant Security Council;

    (b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in 1737 (2006); and

    (c) the relevant countries have submitted prior notification to the 1737 Sanctions Committee of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.[29]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs,

[29] In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013.*

© 2012-2026

that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016)**:

(i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

(ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programmes, including through illicit means;

(iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[30];

(iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[31];

(v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

(vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

(b) **On Iran - Resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010):**

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;

(ii) any person or entity directly associated with or providing support for Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;

---

30 The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

31 Ibid.

© 2012-2026

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

(iv) any person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010);

(v) any entity owned or controlled, including through illicit means, by the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010);

(vi) any person or entity acting on behalf or at the direction of the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010);

(vii) entities owned or controlled, including through illicit means, by the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010); or

(viii) any person or entity determined by the United Nations Security Council or the Committee to have assisted designated persons or entities in evading sanction of, or in violating the provisions of, S/RES/1737 (2006), S/RES/1747 (2007), S/RES/1803 (2008), or S/RES/1929 (2010)

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of an NPO. This definition is based on those activities and characteristics of an organisation which may put it at risk of TF abuse, rather than on the simple fact that it is operating on a non-profit basis. For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Without prejudice to Recommendation 1, this Recommendation only applies to those organisations which fall within the FATF definition of an NPO. It does not apply to the entire universe of organisations working in the not-for-profit realm in a country.

2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important services, as well as the difficulty of providing assistance to those in need, including in high-risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism.

3. Some NPOs may be at risk of terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy public trust, which gives some access to considerable sources of funds, and in some contexts are cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, that may be within or near those areas that are most exposed to terrorist activity. In rare cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate NPOs and misuse funds and operations to cover for, or support, terrorist activity. Also, there have been cases where terrorists create sham NPOs or engage in fraudulent fundraising for these purposes. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity, but also undermines the confidence of donors and financial institutions and jeopardises the very integrity of NPOs.

4. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global effort to prevent and combat terrorism and a necessary step to preserve the integrity of NPOs, the donor community and the financial institutions they use. Measures to protect NPOs from potential terrorist financing abuse should be focused and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects

© 2012-2026

countries' obligations under the Charter of the United Nations and international law, in particular international human rights, international refugee law and international humanitarian law.[32]

B. OBJECTIVES AND GENERAL PRINCIPLES

5. The objective of Recommendation 8 is to ensure that NPOs are not abused by terrorists and terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

   (a) Past and ongoing terrorist financing abuse of NPOs requires countries to have in place focused, proportionate and risk-based measures in dealing with identified risks. A risk-based approach is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be at risk of terrorist financing abuse, the need to ensure that legitimate NPO activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

   (b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces and responds to the changing nature of the terrorist financing threat.

   (c) Focused, proportionate and risk-based measures adopted by countries to protect NPOs from terrorist financing abuse should not unduly disrupt or discourage legitimate NPO activities, in line with the risk-based approach. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community, the financial institutions and with the general public, that NPO funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.

   (d) Countries should identify and take effective and proportionate action against NPOs that either are exploited by, or are knowingly supporting, terrorists or terrorist organisations, taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose must respect the rule of law and should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of NPO activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate

[32] See also UNSC resolution 2462(2019) paras 6 and 23 and UNSC resolution 2664(2022) para.1.

© 2012-2026

interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

(e) Countries should develop an understanding of the different degrees of TF risk posed to NPOs and of the corresponding proportionate measures to mitigate these risks in line with the risk-based approach. Many NPOs may face low TF risk exposure, may have adequate self-regulatory measures and related internal control measures to mitigate such risks, and/or may already be subject to adequate levels of legal and regulatory requirements, such that there may be no need for additional measures.[33] Countries should be mindful of the potential impact of measures on legitimate NPO activities and apply them where they are necessary to mitigate the assessed TF risks, without unduly disrupting or discouraging legitimate NPO activities. It is not in line with Recommendation 8 to apply measures to organisations working in the not-for-profit realm to protect them from TF abuse when they do not fall within the FATF's functional definition of NPOs. It is not in line with Recommendation 8 to implement any measures that are not proportionate to the assessed TF risks, and are therefore overly burdensome or restrictive. NPOs are not reporting entities and should not be required to conduct customer due diligence.

(f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. RISK ASSESSMENT AND MITIGATING MEASURES

6. NPOs are at varying degrees of risk of TF abuse by virtue of their types, activities or characteristics and the majority may represent low risk. Without prejudice to the requirements of Recommendation 1:

(a) Countries should identify organisations which fall within the FATF definition of NPOs.

(b) Countries should conduct a risk assessment of these NPOs to identify the nature of TF risks posed to them.

(c) Countries should have in place focused, proportionate and risk-based measures to address the TF risks identified, in line with the risk-based approach. Countries may also consider, where they exist, self-regulatory measures and related internal control measures in place within NPOs.

[33] In this context, self-regulatory measures may include rules and standards applied by self-regulatory organisations and accrediting institutions.

© 2012-2026

(d) These exercises under letters (a) to (c):

(i) should use all relevant and reliable sources of information[34], including through engagement with NPOs,

(ii) could take a variety of forms and may or may not be a written product,

(iii) should be reviewed periodically

D. EFFECTIVE APPROACH IN IDENTIFYING, PREVENTING AND COMBATING TF ABUSE OF NPOS

7. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. For NPOs identified to be at low-risk of TF abuse, countries may focus only on undertaking outreach concerning terrorist financing issues, and may decide to refrain from taking additional mitigating measures. In other situations, an effective approach should involve all four of the following elements to protect NPOs from potential terrorist financing abuse., without unduly disrupting or discouraging legitimate NPO activities:

(a) Sustained outreach concerning terrorist financing issues:

(i) Countries should have clear policies to promote accountability, integrity and public confidence in the administration and management of NPOs.

(ii) Countries should undertake outreach and educational programmes as appropriate to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

(iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and thus protect them from terrorist financing abuse.

(iv) Countries should encourage NPOs to conduct transactions via regulated financial and payment channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and areas and the risks of using cash.

(b) Focused, proportionate and risk-based measures, including oversight or monitoring of NPOs:

Countries should take steps to promote focused, proportionate and risk-based oversight or monitoring of NPOs. A “one-size-fits-all” approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice:

(i) Countries should be able to demonstrate that they have in place focused, proportionate and risk-based measures applying to NPOs. It is also possible that existing regulatory and self-regulatory measures and related internal control

[34] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

© 2012-2026

measures in place within NPOs, or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a country, although terrorist financing risks to the sector should be periodically reviewed.

(ii) Appropriate authorities should monitor the compliance of NPOs with the focused, proportionate and risk-based measures being applied to them.

(iii) Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[35]

(c) Effective information gathering and investigation:

(i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.

(ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.

(iii) Countries should ensure that access to relevant information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

(iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.

(d) Effective capacity to respond to international requests for information about an NPO of concern: consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

[35] The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

© 2012-2026

E. RESOURCES FOR OVERSIGHT, MONITORING, AND INVESTIGATION

8. Countries should provide their appropriate authorities, which are responsible for oversight, monitoring and investigation of their NPOs, with adequate financial, human and technical resources.

Glossary of specific terms used in the context of this Recommendation	
Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or NPO	refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
Self-regulatory measures	include rules and standards applied by self-regulatory organisations and accrediting institutions.
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   (a) normally seek to identify and verify the identity[36] of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

   (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements[37], financial institutions should be required to identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control

[36] Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

[37] In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

© 2012-2026

structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

  (i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

  (ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

  (iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures[38] to verify the identity of such persons, through the following information:

  (i) For legal persons[39]:

    (i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest[40] in a legal person; and

    (i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

---

38 In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

39 Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

40 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

© 2012-2026

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries [41], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

[41] For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

© 2012-2026

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers[42] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

---

42 Existing customers as at the date that the national requirements are brought into force.

© 2012-2026

H. RISK BASED APPROACH[43]

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:[44]

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

---

43 The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

44 Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

© 2012-2026

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions where appropriate risk mitigation measures have not been implemented.
- Payment received from unknown or un-associated third parties.

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, the country should allow and encourage [45] its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

    (a) Customer risk factors:

    - Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
    - Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
    - Public administrations or enterprises.

    (b) Product, service, transaction or delivery channel risk factors:

    - Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
    - Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.
    - A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.

---

45 For example, encouragement can take the form of guidance issued by the government, supervisor or other competent authority to improve understanding of the circumstances when simplified measures may be appropriate and what form they may take, or outreach or other forms of engagement with financial institutions and DNFBPs.

© 2012-2026

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.

© 2012-2026

- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions should be allowed and encouraged to implement simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be proportionate to the lower risk factors (e.g. the simplified measures could relate to customer acceptance measures, aspects of ongoing monitoring, or both). Examples of possible measures are:

    - Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
    - Reducing the frequency of customer identification updates.
    - Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
    - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

    Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

© 2012-2026

Ongoing due diligence

23. Financial institutions should be required 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, particularly for higher-risk categories of customers.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the payout of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 13 (CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 15 (NEW TECHNOLOGIES)

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering, terrorist financing and proliferation financing risks[46] emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are proportionate to the risks identified. Countries should take appropriate steps to manage and mitigate the proliferation financing risks that they identify. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created[47]. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory 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 VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk- based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure

46 "Proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

47 References to creating a legal person include incorporation of companies or any other mechanism that is used.

© 2012-2026

compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

   (a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.

   (b) R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[48] on virtual asset transfers, submit [49] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

[48] As defined in INR. 16, paragraph 9, or the equivalent information in a virtual asset context.

[49] The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 16 (PAYMENT TRANSPARENCY)

A. OBJECTIVE

1. Recommendation 16 has the objective of preventing terrorists, perpetrators of money laundering and associated predicate offences (e.g., fraud), and other criminals from having unfettered access to payments or value transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary[50] of payments or value transfers is immediately available:

   (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

   (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and

   (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing, and resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.[51]

2. To accomplish these objectives, countries should have the ability to trace all payments or value transfers. Due to the potential terrorist financing threat posed by small payments or value transfers, countries should minimise thresholds, while taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system or financial inclusion.

B. SCOPE

3. Recommendation 16 applies to cross-border and domestic payments or value transfers, including serial payments and cover payments. Differentiated obligations apply to different types of transactions, as set out in Section C.

---

50 The terms "originator" and "beneficiary" are used in Recommendation 16 and its Interpretive Note. These terms are interchangeable with the terms "debtor" and "creditor" respectively, which are used in certain messaging standards such as ISO 20022.

51 Recommendation 16 does not specify whether or how the information transmitted should be screened against sanction lists, given that various mechanisms may ensure compliance with applicable targeted financial sanctions.

© 2012-2026

4. Information accompanying cross-border and domestic payments or value transfers should be structured, to the extent possible, in accordance with the established standards of the system used such as ISO 20022, and should be sufficiently detailed to enable identification of the originator and beneficiary.

C. INFORMATION REQUIREMENTS

5. This section sets out the applicable information requirements for domestic and cross-border transfers including differentiated requirements for certain categories of payments or value transfers.

6. For purposes of implementation of Recommendation 16, the payment chain starts at the financial institution that receives the instructions from the originator for transfer of funds to the beneficiary. The end point of the payment chain is the financial institution that services the account of the beneficiary or provides cash to the beneficiary.

7. Information in the payment message should make it possible for all institutions and authorities referred to in paragraph 1 to identify which financial institution is servicing the account of the originator and beneficiary respectively and in which countries these institutions are located. Financial institutions should ensure that account numbers should not be used to disguise the identification of the country where the financial institution that services the account resides.

Cross-border payments and value transfers

De-minimis threshold for cross-border payments and value transfers

8. Countries may adopt a *de minimis* threshold (no higher than USD/EUR 1 000) for cross-border payments or value transfers (other than cash withdrawals). Below this threshold, countries should ensure that financial institutions include with such transfers:

   (a) the name of the originator and beneficiary; and

   (b) the account number of the originator and beneficiary, where such an account is used to process the transaction.[52] In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction.

Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

Payments and value transfers above the de minimis threshold

9 Information accompanying all cross-border payments or value transfers above the applicable threshold should always contain:

   (a) the name of the originator and beneficiary;

[52] In cases where the funds are drawn from a financial institution other than the ordering financial institution, the account number and the name of financial institution from where the funds are drawn should be included.

(b) the account number of the originator and beneficiary where such an account is used to process the transaction.[53] In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction;

(c) the address of the originator [54] and the country and town name (or the nearest alternative) of the beneficiary;

(d) where the originator is a natural person, the date of birth of the originator[55]; and

(e) where the originator and/or beneficiary is a legal person, the following information, where this exists: (i) the connected business identifier code (BIC), or (ii) the Legal Entity Identifier (LEI), or (iii) the unique official identifier of the originator and/or beneficiary.

Domestic payments and value transfers

De-minimis threshold for domestic payments or value transfers

10. Countries may also adopt a de minimis threshold (no higher than USD/EUR 1 000), for domestic payments or value transfers. Below this threshold, countries should ensure that financial institutions include with such transfers:

(a) the name of the originator; and

(b) the account number of the originator, or a unique transaction reference number which will permit the transaction to be traced back to the originator or the beneficiary.

Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

Payments or value transfers above the de-minimis threshold

11. Information accompanying domestic payments or value transfers should include originator information as indicated in paragraph 9 for cross-border payments or value transfers (or in paragraph 10 above for payments and value transfers below the threshold), unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

12. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary or intermediary financial

53 In cases where the funds are drawn from a financial institution other than the ordering financial institution, the account number and the name of financial institution from where the funds are drawn should be included.

54 In the absence of standardised postal address information for the originator, the country and town name (or the nearest alternative) suffice.

55 When full information of the date of birth is not available, only the year of birth is required.

© 2012-2026

institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

Exceptions and Differentiated Requirements

Financial institution-to-financial institution transfers, net settlements and batch transactions

13. No information is required to accompany financial institution-to-financial institution transfers and settlements, where both the originator and the beneficiary are financial institutions acting on their own behalf.

14. The settlement of payment or value transfers may happen under a net settlement arrangement. Where any net settlement results from payments or value transfers transactions carried out on behalf of customers, information about the underlying transactions is not required to accompany the net settlement. Nevertheless, the relevant requirements of Recommendation 16 do apply to the underlying transactions themselves.

15. Where several individual cross-border payments or value transfers from a single originator are bundled in a batch file for transmission to beneficiaries they may be exempted from the requirements of paragraphs 8 and 9 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 9(b)), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

Card payments

16. With respect to any transfers that flow from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services,[56] the credit or debit or prepaid card number should accompany all transfers flowing from the transaction and the name and location of the card issuing and merchant acquiring financial institutions[57] should be made available upon request.[58]

17. When a credit or debit or prepaid card is used to effect other types of payment or value transfer (e.g., a person-to-person transfer), the transaction is subject to the applicable requirements above for domestic or cross-border payments or value transfers.

Cash withdrawals

18. No information beyond the account number or card number is required to accompany domestic cash withdrawals.

---

56 The purchase of goods or services refers to purchases from individuals/entities who are onboarded by the relevant financial institution to accept card payments following the required CDD in respect of such activity.

57 Card issuer and merchant acquirer information should make it possible for all institutions and authorities referred to in paragraph 1 to identify which financial institutions are in possession of the full cardholder and merchant information, and in which countries these institutions are located.

58 Information should be made available (e.g., with the direct or indirect assistance of the relevant card network) to all other financial institutions in the payment chain and through them to competent authorities. Information should be available in a timely manner.

© 2012-2026

19. With respect to cross-border cash withdrawals (using a credit or debit or prepaid card through a different financial institution)[59] the following requirements apply:

    (a) The card number should accompany cash withdrawal

    (b) The name of the cardholder should be sent to the acquiring financial institution upon request, within three business days of receiving the request.

D. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS[60] INCLUDING MVTS[61]

Ordering (debtor) financial institution

20. The ordering financial institution should ensure that cross-border payments or value transfers above the de minimis threshold contain required and accurate originator information, and required beneficiary information.

21. The ordering financial institution should ensure that cross-border payments or value transfers below the de minimis threshold contain the name of the originator and the beneficiary and an account number for each, or a unique transaction reference number.

22. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

23. The ordering financial institution should not be allowed to execute the payments or value transfer if it does not comply with the requirements specified above.

Intermediary financial institution

24. For all cross-border payments or value transfers, financial institutions processing an intermediary element of such chains of transfers should ensure that all originator and beneficiary information that accompanies a payment or value transfer is retained with it

25. Where technical limitations prevent the required information accompanying a cross-border payment or value transfer from remaining with a related domestic payment or value transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

---

59 These requirements do not apply to withdrawals from ATMs operated by the same institution where the account is held, provided the information required in paragraph 19 is available under other means under Recommendation 18.

60 The terms "ordering financial institution (s)" and "beneficiary financial institution (s)" are used in Recommendation 16 and its Interpretive Note. These terms are interchangeable with terms “debtor agent” and “creditor agent” respectively, which are the terms used in certain messaging standards such as ISO 20022.

61 The responsibilities set out in this section do not apply to cash withdrawals and card payments for purchase of goods or services.

© 2012-2026

26. An intermediary financial institution should take reasonable measures to identify cross-border payments or value transfers that lack required information. Such measures should be consistent with straight-through processing.

27. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a payment or value transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary (creditor) financial institution

28. A beneficiary financial institution should take reasonable measures to identify cross-border payments or value transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

29. For cross-border payments or value transfers above the de minimis threshold, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

30. For cross-border payments or value transfers above the de minimis threshold, information received on the intended beneficiary should inform beneficiary financial institution's monitoring, with the objective of detecting misdirected payments (e.g. due to possible money laundering, fraud, or error). Beneficiary financial institutions should take measures to mitigate the risk of transfers being made to an unintended beneficiary. Such measures should include at least one of the following (a), (b), or (c):

    (a) the beneficiary financial institution should, for each transaction, check the extent to which the name and account number of the beneficiary in the payment message aligns[62] with the information held by the beneficiary financial institution; or

    (b) the beneficiary financial institution should conduct holistic ongoing monitoring to identify anomalous accounts, transactions, and activity, including misaligned beneficiary information, following a risk-based approach; or

    (c) if the beneficiary and ordering financial institutions both participate in a pre-validation mechanism such as confirmation/verification of payee to check, for each transaction, that the name and account number of the beneficiary in the payment message aligns with the information held by the beneficiary financial institution, then this pre-validation may be used instead of (a) or (b) above.

31. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a payment or value transfer lacking required originator or required beneficiary information or when they identify potentially misdirected payments in the implementation of the requirements under paragraph 30; and (ii) the appropriate follow-up action.

62 Alignment does not imply that there must be an exact match. The expected degree of alignment may vary based on the risk and context.

© 2012-2026

Money or value transfer service operators

32. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls, or is part of a MVTS network controlling both the ordering and the beneficiary side of a payment or value transfer, the MVTS provider:

    (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

    (b) should file an STR in any country affected by the suspicious payments or value transfers, and make relevant transaction information available to the Financial Intelligence Unit.

Glossary of specific terms used in this Recommendation	
Accurate	is used to describe information that has been verified for accuracy.
Address	refers to the physical location of a residence or business.
Batch transfer	is a transfer comprised of a number of individual payments or value transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested payments or value transfer in a chain of payments or value transfers.
Beneficiary Financial Institution	refers to the financial institution that services the account of the beneficiary or remits cash to the beneficiary. The beneficiary financial institution is the end point in a payment chain.
Connected Business Identifier Code	BIC refers to a universal business identifier code based on the ISO 9362 standard assigned to financial and non-financial institutions. Connected BICs are those used by financial institutions, for instance to access the SWIFT network.
Cover Payment	refers to a payment or value transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

© 2012-2026

Glossary of specific terms used in this Recommendation	
Cross-border payment or value transfer	refers to any *payment or value transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *payments or value transfers* in which at least one of the financial institutions involved is located in a different country.
Domestic payment or value transfers	refers to any *payment or value transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *payments or value transfers* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *payments or value transfers* that takes place entirely within the borders of the European Economic Area (EEA)[63].
Intermediary financial institution	refers to a financial institution in a payment chain that receives and transmits a payment or value transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
Legal Entity Identifier	refers to a unique alphanumeric reference code based on the ISO 17442 standard assigned to an entity by the Global LEI System.
MVTS Network	refers to any or a combination of the two following elements: (i) an MVTS and its agents, or (ii) two or more MVTS bound by one or several agreements to proceed to payments or value transfers, including but not limited to the net settlement of those transfers.
Ordering financial institution	refers to the financial institution that receives the instructions from the originator for transfer of funds to the beneficiary. The ordering financial institution is the start point of the payment chain.
Originator	refers to the account holder who requests the payment or value transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the payment or value transfer.
Serial Payment	refers to a direct sequential chain of payment where the payments or value transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial

[63] An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

© 2012-2026

Glossary of specific terms used in this Recommendation	
	institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique official identifier	refers to an identification scheme that is issued by the public sector in the relevant jurisdiction and that ensures that a given identifier refers to a unique person, entity or legal arrangement, and that a given person, entity or legal arrangement only has one identifier in that scheme.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the payments or value transfer.
Payment(s) or value transfer	refers to any transaction carried out on behalf of an originator through an ordering financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same. This includes cash withdrawals.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.
2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.
3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:

   (a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;

   (b) an ongoing employee training programme; and

   (c) an independent audit function to test the system.

2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

3. Compliance management arrangements should include the appointment of a compliance officer at the management level.

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including, as appropriate, requesting the financial group to close down its operations in the host country.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

   (a) Requiring financial institutions to apply specific elements of enhanced due diligence.

   (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

   (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.

   (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

   (e) Limiting business relationships or financial transactions with the identified country or persons in that country.

   (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.

   (g) Requiring financial institutions to review and amend, or if necessary, terminate, correspondent relationships with financial institutions in the country concerned.

   (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.

   (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

   There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.
2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.
4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called “indirect reporting”), is not acceptable.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:

   - Casinos (under Recommendation 22) - USD/EUR 3,000
   - For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

   Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. For the purposes of R.23, the requirements referring to 'financial groups' in R.18 apply to DNFBP groups operating under the same structure as financial groups. In addition, countries should consider applying the requirements for group-wide programmes to DNFBPs operating in other structures sharing common ownership, management or compliance control to the extent that those structures could better mitigate ML/TF risks by applying group-wide programmes. The type and extent of measures to be taken should be appropriate to the business conducted, the risk of money laundering and terrorist financing and the size of the business. For example, as set out in INR.18, countries may determine the scope and extent of information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

3. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.

2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

1. Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

3. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.

4. Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and up-to-date information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[64]) that are created[65] in the country, as well as those that present ML/TF risks and have sufficient links[66] with their country (if they are not created in the country). Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. Countries should utilise a combination of mechanisms to achieve the objective.

2. As part of the process described in paragraph 1 of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

   (a) identify and describe the different types, forms and basic features of legal persons in the country;

   (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

   (c) make the above information publicly available;

   (d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country, and take appropriate steps to manage and mitigate the risks that they identify; and

   (e) assess the money laundering and terrorist financing risks to which their country is exposed, associated with different types of foreign-created legal persons, and take appropriate steps to manage and mitigate the risks that they identify[67]

---

64 ***Beneficial ownership information*** for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (determined based on the jurisdiction's assessment of risk, with a maximum of 25%).

65 References to creating a legal person, include incorporation of companies or any other mechanism that is used.

66 Countries may determine what is considered a *sufficient link* on the basis of risk. Examples of sufficiency tests may include, but are not limited to, when a company has permanent establishment/branch/agency, has significant business activity or has significant and ongoing business relations with financial institutions or DNFBPs, subject to AML/CFT regulation, has significant real estate/other local investment, employs staff, or is a tax resident, in the country.

67 This could be done through national and/or supranational measures. These could include requiring beneficial ownership information on some types of foreign-created legal persons to be held as set out under paragraph 7.

© 2012-2026

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company[68] are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.[69] Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company[70] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

   (a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors, and unique identifier such as a tax identification number or equivalent (where this exists);[71] and

   (b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[72] and categories of shares (including the nature of the associated voting rights).

5. The company registry[73] should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

B. BENEFICIAL OWNERSHIP INFORMATION

7. Countries should follow a multi-pronged approach in order to ensure that the beneficial ownership of a company can be determined in a timely manner by a competent authority. Countries should decide, on the basis of risk, context and materiality, what form of registry or

---

68 Recommendation 24 applies to all forms of legal persons. The requirements are described primarily with reference to companies, but similar requirements should be applied to other types of legal person, taking into account their different forms and structures - as set out in Section E.

69 "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

70 The information can be recorded by the company itself or by a third person under the company's responsibility.

71 This information should be made public, as set out in paragraph 11.

72 This is applicable to the nominal owner of all registered shares.

73 Or another public body in the case of a tax identification number.

alternative mechanisms they will use to enable efficient access to information by competent authorities, and should document their decision. This should include the following:

(a) Countries should require companies to obtain and hold adequate, accurate and up-to-date information on the company's own beneficial ownership; to co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, including making the information available to competent authorities in a timely manner; and to co-operate with financial institutions/DNFBPs to provide adequate, accurate and up-to-date information on the company's beneficial ownership information.

b) (i) Countries should require adequate, accurate and up-to-date information on the beneficial ownership of legal persons to be held by a public authority or body (for example a tax authority, FIU, company registry, or beneficial ownership registry). Information need not be held by a single body only.[74]

b) (ii) Countries may decide to use an alternative mechanism instead of (b)(i) if it also provides authorities with efficient access to adequate, accurate and up-to-date BO information. For these purposes reliance on basic information or existing information alone is insufficient, but there must be some specific mechanism that provides efficient access to the information.

c) Countries should use any additional supplementary measures that are necessary to ensure the beneficial ownership of a company can be determined; including for example information held by regulators or stock exchanges; or obtained by financial institutions and/or DNFBPs in accordance with Recommendations 10 and 22.[75]

8. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

C. TIMELY ACCESS TO ADEQUATE, ACCURATE AND UP-TO-DATE INFORMATION

9. Countries should have mechanisms that ensure that basic information and beneficial ownership information, including information provided to the company registry and any available information referred to in paragraph 7, is adequate, accurate and up to date.

---

74 A body could record beneficial ownership information alongside other information (e.g. basic ownership and incorporation information, tax information), or the source of information could take the form of multiple registries (e.g. for provinces or districts, for sectors, or for specific types of legal person such as NPOs), or of a private body entrusted with this task by the public authority.

75 Countries should be able to determine in a timely manner whether a company has or controls an account with a financial institution within the country.

© 2012-2026

Adequate information is information that is sufficient to identify[76] the natural person(s) who are the beneficial owner(s), and the means and mechanisms through which they exercise beneficial ownership or control.

Accurate information is information, which has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable, independently sourced/obtained documents, data or information. The extent of verification measures may vary according to the specific level of risk.

Countries should consider complementary measures as necessary to support the accuracy of beneficial ownership information, e.g. discrepancy reporting.

Up-to-date information is information which is as current and up-to-date as possible, and is updated within a reasonable period (e.g. within one month) following any change.

10. Competent authorities, and in particular law enforcement authorities and FIUs, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties, including rapid and efficient access to information held or obtained by a public authority or body or other competent authority on basic and beneficial ownership information, and/or on the financial institutions or DNFBPs which hold this information. In addition, countries should ensure public authorities at national level and others as appropriate have timely access to basic and beneficial ownership information on legal persons in the course of public procurement.

11. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above and to beneficial ownership information held pursuant to paragraph 7 above, and could consider facilitating public access to this information.

D. OBSTACLES TO TRANSPARENCY

12. Countries should take measures to prevent and mitigate the risk of the misuse of bearer shares and bearer share warrants[77] by prohibiting the issuance of new bearer shares and bearer share warrants; and, for any existing bearer shares and bearer share warrants, by applying one or more of the following mechanisms within a reasonable timeframe[78]:

---

76 Examples of information aimed at identifying the natural person(s) who are the beneficial owner(s) include the full name, nationality(ies), the full date and place of birth, residential address, national identification number and document type, and the tax identification number or equivalent in the country of residence.

77 Or any other similar instruments without traceability.

78 These requirements do not apply to newly issued and existing bearer shares or bearer share warrants of a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership.

© 2012-2026

(a) converting them into a registered form; or

(b) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary, with timely access to the information by the competent authorities; and

(c) during the period before (a) or (b) is completed, requiring holders of bearer instruments to notify the company, and the company to record their identity before any rights associated therewith can be exercised.

13. Countries should take measures to prevent and mitigate the risk of the misuse of nominee shareholding and nominee directors, by applying one or more of the following mechanisms:

(a) requiring nominee shareholders and directors to disclose their nominee status and the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register, and for the information to be obtained, held or recorded by the public authority or body or the alternative mechanism referred to in paragraph 7. Nominee status should be included in public information;

(b) requiring nominee shareholders and directors to be licensed[79], for their nominee status and the identity of their nominator to be obtained, held or recorded by the public authority or body or alternative mechanism referred to in paragraph 7 and for them to maintain information identifying their nominator and the natural person on whose behalf the nominee is ultimately acting[80], and make this information available to the competent authorities upon request;[81].or

(c) enforcing a prohibition of the use of nominee shareholders or nominee directors.

E. OTHER LEGAL PERSONS

14. In relation to foundations, Anstalt, Waqf [82] and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.

15. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate

79 A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions or DNFBPs (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform nominee activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

80 Identifying the beneficial owner in situations where a nominee holds a controlling interest or otherwise exercises effective control requires establishing the identity of the natural person on whose behalf the nominee is ultimately, directly or indirectly, acting.

81 For intermediaries involved in such nominee activities, reference should be made to R.22 and R.28 in fulfilling the relevant requirements.

82 Except in countries where Waqf are legal arrangements under R.25.

© 2012-2026

levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and up-to-date by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

16. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

17. Countries should rapidly, constructively and effectively provide the widest possible range of international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries 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. Consistent with Recommendations 37 and 40, countries should not place unduly restrictive conditions on the exchange of information or assistance e.g., refuse a request on the grounds that it involves a fiscal, including tax, matters, bank secrecy, etc. Information held or obtained for the purpose of identifying beneficial ownership should be kept in a readily accessible manner in order to facilitate rapid, constructive and effective international co-operation. Countries should designate and make publicly known the agency(ies) responsible for responding to all international requests for BO information.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust and persons holding an equivalent position in a similar legal arrangement, that are residents in their country or that administer any express trusts or similar legal arrangements in their country, to obtain and hold adequate, accurate, and up-to-date beneficial ownership information[83] regarding the trust and other similar legal arrangements. This should include information on the identity of: (i) the settlor(s), (ii) the trustee(s), (iii) the protectors (if any); (iv) each beneficiary(ies) or, where applicable, the class of beneficiaries[84] and objects of a power, and (v) any other natural person(s) exercising ultimate effective control over the trust. For a similar legal arrangement, this should include persons holding equivalent positions. Where the parties to the trusts or other similar legal arrangements are legal persons or arrangements, countries should require trustees and persons holding an equivalent position in a similar legal arrangement to also obtain and hold adequate, accurate, and up-to-date basic and beneficial ownership information of the legal persons or arrangements. Countries should also require trustees and persons holding an equivalent position in a similar legal arrangement that are residents in their country or that administer trusts or similar legal arrangements in their country to hold basic information on other regulated agents of, and service providers to, the trust and similar legal arrangements, including but not limited to investment advisors or managers, accountants, and tax advisors.

2. Countries with express trusts and other similar legal arrangements governed under their law should have mechanisms that:

   (a) identify the different types, forms and basic features of express trusts and/or other similar legal arrangements;

   (b) identify and describe the processes for: (i) the setting up of those legal arrangements; and (ii) the obtaining of basic[85] and beneficial ownership information;

   (c) make the above information referred to in (a) and (b) publicly available.

3. Countries should assess the money laundering and terrorist financing risks associated with different types of trusts and other similar legal arrangements:

   (a) governed under their law;

---

83 Beneficial ownership information for legal arrangements is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(ii) and the Glossary.

84 Where there are no ascertainable beneficiaries at the time of setting up the trust, the trustee should obtain and hold information on the class of beneficiaries and its characteristics, and objects of a power. Following a risk-based approach, countries may decide that it is not necessary to identify the individual beneficiaries of certain charitable or statutory permitted non-charitable trusts.

85 In relation to a legal arrangement, basic information means the identifier of the legal arrangement (e.g. the name, the unique identifier such as a tax identification number or equivalent, where this exists), the trust deed (or equivalent) and purposes, if any, the residence of the trustee/equivalent or of the place from where the legal arrangement is administered.

© 2012-2026

(b) which are administered in their country or for which the trustee or equivalent resides in their country; and

(c) types of foreign legal arrangements that have sufficient links[86] with their country

and take appropriate steps to manage and mitigate the risks that they identify.[87]

4. Countries should take measures to ensure that trustees or persons holding equivalent positions in similar legal arrangements disclose their status to financial institutions and DNFBPs when, in their function, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees or persons holding equivalent positions in similar legal arrangements should cooperate to the fullest extent possible with, and not be prevented by law or enforceable means from providing competent authorities with necessary information relating to the trust or other similar legal arrangements.[88] Countries should also ensure that trustees or persons holding equivalent positions in similar legal arrangements should not be prevented by law or enforceable means from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust or legal arrangement to be held or managed under the terms of the business relationship.

5. In order to ensure that adequate, accurate and up-to-date information on the basic and beneficial ownership of the trusts or other similar legal arrangements, trustees and trust assets, is accessible efficiently and in a timely manner by competent authorities, other than through trustees or persons holding an equivalent position in a similar legal arrangement, on the basis of risk, context and materiality, countries should consider using any of the following sources of information as necessary:

(a) A public authority or body holding information on the beneficial ownership of trusts or other similar arrangements (e.g. in a central registry of trusts; or in asset registries for land, property, vehicles, shares or other assets that hold information on the beneficial ownership of trusts and other similar legal arrangements, which own such assets). Information need not be held by a single body only.[89]

(b) Other competent authorities that hold or obtain information on trusts/similar legal arrangements and trustees/their equivalents (e.g. tax authorities, which collect

---

86 Countries may determine what is considered a *sufficient link* on the basis of risk. Examples of sufficiency tests may include, but are not limited to, when the trust/similar legal arrangement or a trustee or a person holding an equivalent position in a similar legal arrangement has significant and ongoing business relations with financial institutions or DNFBPs, has significant real estate/other local investment, or is a tax resident, in the country.

87 This could be done through national and/or supranational measures. These could include requiring beneficial ownership information on some types of foreign legal arrangements to be held as set out under paragraph 5.

88 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

89 A body could record beneficial ownership information alongside other information (e.g. tax information), or the source of information could take the form of multiple registries (e.g. for provinces or districts, for sectors, or for specific types of legal arrangements), or of a private body entrusted with this task by the public authority.

information on assets and income relating to trusts and other similar legal arrangements).

(c) Other agents or service providers, including trust and company service providers, investment advisors or managers, accountants, lawyers, or financial institutions.

6. Countries should have mechanisms that ensure that information on trusts and other similar legal arrangements, including information provided in accordance with paragraphs 4 and 5, is adequate, accurate and up-to-date.[90] In the context of legal arrangements:

- *Adequate* information is information that is sufficient to identify the natural persons who are the beneficial owner(s), and their role in the legal arrangement[91].
- *Accurate* information is information, which has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable documents, data or information. The extent of verification measures may vary according to the specific level of risk.
- *Up-to-date* information is information which is as current and up-to-date as possible, and is updated within a reasonable period following any change.

7 Countries should ensure that competent authorities, and in particular law enforcement authorities and FIUs, should have all the powers necessary to obtain timely access to the information held by trustees, persons holding equivalent positions in similar legal arrangements, and other parties, in particular information held by financial institutions and DNFBPs on: (a) the basic and beneficial ownership of the legal arrangement; (b) the residence of the trustees and their equivalents; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees or their equivalents with which they have a business relationship, or for which they undertake an occasional transaction.

8. Trustees and persons holding equivalent positions in similar legal arrangements should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust or similar legal arrangement ceases. Countries are encouraged to require the other authorities, persons and entities mentioned in paragraph 5 above to maintain the information for at least five years.

9 Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and up-to-date, and the information should be updated within a reasonable period following any change.

---

90 For beneficiary(ies) of trusts/similar legal arrangement that are designated by characteristics or by class, trustees/equivalent are not expected to obtain fully adequate and accurate information until the person becomes entitled as beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights, as per the risk-based approach.

91 Settlor(s), trustee(s), protector(s) (if any), beneficiary(ies) or, where applicable, the class of beneficiaries, and objects of a power, and any other person exercising ultimate effective control over the trusts. For a similar legal arrangement, this should include persons holding equivalent positions. Where the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.

© 2012-2026

10. Countries should consider measures to facilitate access to information that is held on trusts or other similar legal arrangements by the other authorities, persons and entities referred to in paragraph 5, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

11. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 4, 8, 9 and 13 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

International Cooperation

12 Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts. Consistent with Recommendations 37 and 40, countries should not place unduly restrictive conditions on the exchange of information or assistance e.g., refuse a request on the grounds that it involves fiscal (including tax) matters, bank secrecy, etc. To facilitate rapid, constructive and effective international cooperation, where possible, countries should designate and make publicly known the agency(ies) responsible for responding to all international requests for beneficial ownership information, consistent with countries' approach to access to beneficial ownership information. To this end, countries should consider keeping information held or obtained for the purpose of identifying beneficial ownership in a readily accessible manner.

Liability and Sanctions

13. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees or persons holding equivalent positions in similar legal arrangements are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 4, 8 and 9; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.[92] Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 8.

[92] This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.

2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group. The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.

3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.

4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional

© 2012-2026

standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

© 2012-2026

(c) Dissemination

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION

(a) Obtaining Additional Information from Reporting Entities

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

© 2012-2026

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of criminal property and property of corresponding value.

2. A 'financial investigation' means an enquiry into the financial affairs related to criminal activity, with a view to:

   - identifying the extent of criminal networks and/or the scale of criminality;
   - identifying and tracing criminal property and property of corresponding value; and
   - developing evidence which can be used in criminal and/or confiscation proceedings.

3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money, for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of criminal property and property of corresponding value.

7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.

© 2012-2026

8. Law enforcement authorities and prosecutorial authorities, including those authorities responsible for asset recovery, should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical cross-border transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

   (a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a “yes” or “no” box).

   (b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

© 2012-2026

(c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

(a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

(b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use.

(c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious cross-border transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.

(d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

(e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

(f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of money

© 2012-2026

laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

(g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

© 2012-2026

Glossary of specific terms used in this Recommendation

Physical cross-border transportation	refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Related to terrorist financing or money laundering	when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should be able to take expeditious action in response to requests for cooperation in the widest possible range of circumstances. This should include requests made on the basis of conviction and non-conviction based confiscation proceedings and related provisional measures, as set out in Recommendation 4.[93]

2. In recognising and enforcing foreign freezing, seizing or confiscation orders, requested countries should be able to rely on the findings of fact in the foreign order. Enforcement should not be made conditional on conducting a domestic investigation. Further, courts in the requested country may review the foreign order and issue any orders necessary to give it effect with regard to property located in the requested country.

3. Where the requested country requires a court order to provide assistance due to fundamental principles of domestic law or other considerations, requesting countries should ensure that their courts have authority to issue freezing, seizing, and confiscation orders for property located abroad or, if applicable, mechanisms for domestic judicial review and validation of orders to be submitted for enforcement.

4. Countries should also ensure they have the authority to provide further related assistance on an initial request, without requiring a supplemental request, in appropriate cases.

5. Countries should have effective mechanisms for managing, preserving, and, when necessary, disposing of, frozen, seized or confiscated property as set out in Recommendation 4.

6. Countries should be able to share confiscated property with other countries, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions. Countries should be able to make arrangements, where appropriate, to deduct or share substantial or extraordinary costs incurred when enforcing a freezing, seizing, or confiscation order.

7. Countries should have measures to enable informal communication with other countries in asset recovery cases, including facilitating assistance before a request is made and updating countries, as appropriate, on the status of their requests.

[93] The reference to Recommendation 4 incorporates references to fundamental principles of domestic law which may relate to certain types of confiscation. With regard to requests made on the basis of non-conviction based confiscation proceedings, countries should have the authority to provide assistance, at a minimum, in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, to the furthest extent that such assistance is consistent with fundamental principles of domestic law.

© 2012-2026

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

   (a) the request is also considered to involve fiscal matters; and/or

   (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

   (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

Safeguards on information exchanged

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.

4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[94], consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of information should take place in a secure way, and through reliable channels or mechanisms. Requested competent

[94] Information may be disclosed if such disclosure is required to carry out the request for cooperation.

© 2012-2026

authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, predicate offences and terrorist financing.

8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

9. FIUs should have the power to exchange:

   (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and

   (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

10. Countries should ensure that the FIU or other competent authority is able to take immediate action, directly or indirectly, to withhold consent to or suspend a transaction suspected of being related to money laundering, predicate offences, or terrorist financing, in response to a relevant request from a foreign counterpart. If the competent authorities having this power in the requesting and the requested countries are not counterparts, countries should ensure that the FIU is able to send or receive such requests.

Exchange of information between financial supervisors[95]

11. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at

[95] This refers to financial supervisors which are competent authorities.

© 2012-2026

facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

12. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

    (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.

    (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

    (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

13. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

14. Any dissemination of information exchanged or use of that information for supervisory and non- supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

15. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing.

16. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol,

© 2012-2026

Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

17. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

18. Law enforcement authorities should be able to exchange domestically available information for intelligence or investigative purposes and cooperate with foreign counterparts to identify and trace criminal property and property of corresponding value, and in support of the freezing, seizing, and confiscation of such property through the formal mutual legal assistance process. Law enforcement authorities should be able to commence domestic investigations or proceedings based on such information received from foreign counterparts, in appropriate cases.

19. Law enforcement authorities should be able to spontaneously share relevant information regarding criminal property and property of corresponding value with foreign counterparts without a prior request, in appropriate cases. In addition, in appropriate cases, law enforcement authorities should be able to spontaneously identify and trace criminal property and property of corresponding value if they suspect that such property relating to a foreign investigation may be located in their jurisdiction. Law enforcement authorities have discretion on when and under what conditions to share such information, for example, so as not to prejudice domestic investigations.

20. Countries should take part in and actively support multilateral networks to better facilitate rapid and constructive international cooperation in asset recovery. Countries should apply for membership in a relevant Asset Recovery Inter-agency Network (ARIN) or other body supporting international cooperation in asset recovery.

Exchange of information between non-counterparts

21. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

22. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

© 2012-2026

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS AND VASPS

1. All requirements for financial institutions, DNFBPs or VASPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

      (i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

© 2012-2026

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions, DNFBPs and VASPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

© 2012-2026

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Address	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Asset recovery	The term *asset recovery* refers to the process of identifying, tracing, evaluating, freezing, seizing, confiscating and enforcing a resulting order for, managing, and disposing of (including returning or sharing), criminal property and property of corresponding value.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares and bearer share warrants	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. It does not refer to dematerialised and/or registered forms of share certificate whose owner can be identified. *Bearer share warrants* refers to negotiable instruments that accord entitlement to ownership in a legal person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability. It does not refer to dematerialised and/or registered form of warrants or other instruments whose owner can be identified. It also does not refer any other instruments that only confers a right to subscribe for ownership in a legal person at specified conditions, but not ownership or entitlement to ownership, unless and until the instruments are exercised.

© 2012-2026

Terms	Definitions
Beneficial owner	In the context of legal persons, *beneficial owner* refers to the natural person(s) who ultimately[96] owns or controls a customer[97] and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.[98] In the context of legal arrangements, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement.[99] In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are or may become entitled to the benefit of any trust arrangement. A beneficiary can be a natural person or a legal person, or a legal arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries when they are set up but only a class of beneficiaries and objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined

96 Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

97 This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

98 The ultimate beneficial owner is always one or more natural persons. As set out in R.10, in the context of CDD it may not be possible to verify the identity of such persons through reasonable measures, and, to the extent that there is doubt about whether a person with a controlling ownership interest in a legal person is the ultimate beneficial owner, or where no natural person exerts control through ownership interests, the identity should be determined of the natural persons (if any) exercising control of the legal person through other means. Where no natural person is identified in that role, the natural person who holds the position of senior managing official should be identified and recorded as holding this position. This provision of R.10 does not amend or supersede the definition of who the *beneficial owner* is, but only sets out how CDD should be conducted in situations where the beneficial owner cannot be identified.

99 Reference to "ultimate effective control" over trusts or similar legal arrangements includes situations in which ownership/control is exercised through a chain of ownership/control.

© 2012-2026

Terms	Definitions
	period, known as the accumulation period, or following exercise of trustee discretion in the case of a discretionary trust. The accumulation period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Connected Business Identifier Code	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities [100] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of property by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that generally transfers the ownership of specified property to the State. In this case, the natural or legal person(s) that held an interest in the specified property at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited property. Confiscation also includes deprivation through an order for corresponding value, where receipts from the sale of property rather than title are transferred to the State.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and

[100] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Criminal property	The term *Criminal property* refers to the following categories: a) proceeds of money laundering or predicate offences (including income or other benefits derived from such proceeds); b) instrumentalities used in or intended for use in, money laundering or predicate offences; c) property laundered; d) property that is used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organisations; e) the proceeds of the financing of terrorism, terrorist acts, or terrorist organisations.
Cross-border payment or value transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering;

© 2012-2026

Terms	Definitions
	■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods; ■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime (for example, criminal harvesting, extraction or trafficking of protected species of wild fauna and flora, precious metals and stones, other natural resources, or waste); ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[101] b) Real estate agents. c) Dealers in precious metals.

[101] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

© 2012-2026

Terms	Definitions
	d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person or entity	The term designated person or entity refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and any future successor resolutions by the

© 2012-2026

Terms	Definitions
	Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006) (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.
Designation	The term *designation* refers to the identification of a person[102], individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 1737 (2006) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.
Domestic payment or value transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result

[102] Natural or legal.

Terms	Definitions
	from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[103] 2. Lending.[104] 3. Financial leasing.[105] 4. Money or value transfer services.[106] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 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. 8. Participation in securities issues and the provision of financial services related to such issues.

103 This also captures private banking.

104 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

105 This does not extend to financial leasing arrangements in relation to consumer products.

106 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

© 2012-2026

Terms	Definitions
	9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[107]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority or a court. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against asset flight. In all cases, the frozen property remains the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions.
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or

[107] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
	expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.

© 2012-2026

Terms	Definitions
Legal arrangements	*Legal arrangements* refers to express trusts and other similar legal arrangements. Examples of other similar arrangements[108] (for AML/CFT purposes) may include but are not limited to fiducie, certain types of Treuhand, fideicomiso and Waqf.[109]
Legal Entity Identifier	Please refer to the IN to Recommendation 16.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
MVTS network	Please refer to the IN to Recommendation 16.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures of criminal property in circumstances where no criminal prosecution or conviction is required.
Nominator	*Nominator* is an individual (or group of individuals) or legal person that issues instructions (directly or indirectly) to a nominee to act on their behalf in the capacity of a director or a shareholder, also sometimes referred to as a "shadow director" or "silent partner".

108 Similarity is assessed having regard to Article 2 of the Hague Convention on the law applicable to trusts and their recognition on the basis of whether legal arrangements have a similar structure or perform a similar function to an express trust

109 Except in countries where Waqf are legal persons under Recommendation 24.

© 2012-2026

Terms	Definitions
Nominee shareholder or director	*Nominee* is an individual or legal person instructed by another individual or legal person ("the nominator") to act on their behalf in a certain capacity regarding a legal person. A *Nominee Director* (also known as a "resident director") is an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct or indirect instructions of the nominator. A Nominee Director is never the beneficial owner of a legal person. A *Nominee Shareholder* exercises the associated voting rights according to the instructions of the nominator and/or receives dividends on behalf of the nominator. A nominee shareholder is never the beneficial owner of a legal person based on the shares it holds as a nominee.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Payment(s) or value transfer	Please refer to the IN to Recommendation 16.
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

© 2012-2026

Terms	Definitions
	Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are proportionate to the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

© 2012-2026

Terms	Definitions
Serial Payment	Please refer to the IN to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN to Recommendation 16.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [110]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A terrorist act includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful

[110] Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

© 2012-2026

Terms	Definitions
	Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.

© 2012-2026

Terms	Definitions
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[111]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or a non-professional who is not in the business of being a trustee (e.g. a person acting on behalf of family).
Unique official identifier	Please refer to the IN to Recommendation 16.
Unique transaction reference number	Please refer to the IN to Recommendation 16.
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets;

111 Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

© 2012-2026

Terms	Definitions
	iii. transfer[112] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

[112] In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

© 2012-2026

ANNEX I: FATF GUIDANCE DOCUMENTS

The FATF has published a large body of Guidance and Best Practices papers which can be found at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html in the section Guidance and Best Practices.

© 2012-2026

ANNEX II: INFORMATION ON UPDATES MADE TO THE FATF RECOMMENDATIONS

The following amendments have been made to the FATF Recommendations since the text was adopted in February 2012.

Date	Type of amendments	Sections subject to amendments
Feb 2013	Alignment of the Standards between R.37 and R.40	■ R.37(d) Insertion of the reference that DNFBP secrecy or confidentiality laws should not affect the provision of mutual legal assistance, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.
Oct 2015	Revision of the Interpretive Note to R. 5 to address the foreign terrorist fighters threat	■ INR.5 (B.3) Insertion of B.3 to incorporate the relevant element of UNSCR 2178 which addresses the threat posed by foreign terrorist fighters. This clarifies that Recommendation 5 requires countries to criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Existing B.3-11 became B.4-12.
Jun 2016	Revision of R. 8 and the Interpretive Note to R. 8	■ R.8 and INR.8 Revision of the standard on non-profit organisation (NPO) to clarify the subset of NPOs which should be made subject to supervision and monitoring. This brings INR.8 into line with the FATF Typologies Report on Risk of Terrorist Abuse of NPOs (June 2014) and the FATF Best Practices on Combatting the Abuse of NPOs (June 2015) which clarify that not all NPOs are high risk and intended to be addressed by R.8, and better align the implementation of R.8/INR.8 with the risk-based approach.

© 2012-2026

Date	Type of amendments	Sections subject to amendments
Oct 2016	Revision of the Interpretive Note to R. 5 and the Glossary definition of 'Funds or other assets'	■ INR. 5 and Glossary Revision of the INR.5 to replace "*funds*" with "*funds or other assets*" throughout INR.5, in order to have the same scope as R.6. Revision of the Glossary definition of "*funds or other assets*" by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.
Jun 2017	Revision of the Interpretive Note to R.7 and the Glossary definitions of "Designated person or entity", "Designation" and "Without delay"	■ INR. 7 and Glossary Revision of the INR.7 and consequential revisions of the Glossary definitions of *"Designated person or entity"*, *"Designation"* and *"Without delay"* to bring the text in line with the requirements of recent United Nations Security Council Resolutions and to clarify the implementation of targeted financial sanctions relating to proliferation financing.
Nov 2017	Revision of the Interpretive Note to Recommendation 18	■ INR.18 Revision of INR.18 to clarify the requirements on sharing of information related to unusual or suspicious transactions within financial groups. It also includes providing this information to branches and subsidiaries when necessary for AML/CFT risk management.
Nov 2017	Revision of Recommendation 21	■ R. 21 Revision of R. 21 to clarify the interaction of these requirements with tipping-off provisions.
Feb 2018	Revision of Recommendation 2	■ R. 2 Revision of R. 2 to ensure compatibility of AML/CFT requirements and data protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

© 2012-2026

Date	Type of amendments	Sections subject to amendments
Oct 2018	Revision of Recommendation 15 and addition of two new definitions in the Glossary	■ R. 15 and Glossary Revision of R.15 and addition of new definitions "virtual asset" and "virtual asset service provider" in order to clarify how AML/CFT requirements apply in the context of virtual assets.
June 2019	Addition of Interpretive Note to R. 15	■ INR. 15 Insertion of a new interpretive note that sets out the application of the FATF Standards to virtual asset activities and service providers.
Oct 2020	Revision of Recommendation 1 and Interpretive Note to Recommendation 1	■ R. 1 and INR. 1 Revision of R. 1 and INR. 1 to require countries, financial institutions and DNFBPs to identify and assess the risks of potential breaches, non-implementation or evasion of the targeted financial sanctions related to proliferation financing, as contained in FATF Recommendation 7, and to take action to mitigate these risks.
Oct 2020	Revision of Recommendation 2 and a new Interpretive Note to Recommendation 2	■ R. 2 and INR. 2 Minor consequential amendment in R.2 to insert reference to counter proliferation financing in the context of national co-operation and co-ordination. Insertion of a new interpretive note that sets out the inter-agency framework to promote domestic co-operation, co-ordination and information exchange.
June 2021	Revision of INR. 15	■ INR. 15 Revision of INR.15 to clarify the applicability of proliferation financing risk assessment and mitigation requirements to virtual asset activities and service providers.

© 2012-2026

Date	Type of amendments	Sections subject to amendments
Oct 2021	Revision of the Glossary definition of 'designated categories of offences'	■ Glossary Revision of the Glossary definition of 'designated categories of offences' to clarify the types of offences which fall within the 'environmental crime' category.
Oct 2021	Revision of INR.22/23, Glossary and consequential edits	■ INR 22 & 23, Glossary and INR 26 Revision of R.23 to clarify obligations on DNFBPs to apply group-wide programmes. Clarification that the Glossary definition of 'financial group' is not limited to Core Principles institutions and a minor consequential amendment to INR.26.
March 2022	Revision of Recommendation 24, INR.24 and Glossary, and addition of two new definitions in the Glossary	■ R.24, INR 24 and Glossary Revision of R.24 and the Glossary definition, with addition of new definitions "nominator" and "nominee shareholder or director", to strengthen the standards on beneficial ownership of legal persons.
Feb 2023	Revision of Recommendation 25, INR.25 and Glossary	■ R.25, INR.25 and Glossary Revision of R.25 and the Glossary definitions of "beneficial owner", "beneficiary" and "legal arrangements", to strengthen the standards on beneficial ownership of legal arrangements.
Oct 2023	Revision of Recommendations 4, 30, 31, 38 and INR.4, INR.30, INR.38 and INR.40 and Glossary	■ R.4, 30, 31 and 38 and INR.4, 30, 38 and 40 & Glossary Revision of FATF's asset recovery Standards and Glossary definitions related to asset recovery.
Oct 2023	Revision of Recommendation 8 and INR.8	■ R.8 and INR.8 Clarificatory amendments to R.8 and INR.8 to strengthen the implementation of focused, targeted and risk-based measures on non-profit organisations.

© 2012-2026

Date	Type of amendments	Sections subject to amendments
Feb 2025	Revision of Recommendation 1 and INR.1, INR.10 and INR.15, Introduction and Glossary	■ R.1 and INR.1, INR.10 and INR.15, Introduction, and Glossary Revisions to FATF's standards related to the risk-based approach to increase focus on proportionality of measures and require countries to allow and encourage simplified measures in lower risk areas.
June 2025	Revision of Recommendation 16 and INR.16 and consequential edits	■ R.16 and INR.16, INR.15, and Glossary ■ Revisions to FATF's standards related to payment transparency to adapt the Standards to the changes in payment business models and messaging standards, as well as to the evolving risks and vulnerabilities. New definitions in the Glossary of specific terms in R.16. As a consequential amendment, footnote 46 for paragraph 7 of INR.15 is updated to refer to applicable paragraph number of R.16.
Oct 2025	Clarification of Recommendation 7 via its Interpretive Note and consequential edits to the Glossary	■ INR. 7, and Glossary Reference updates to refer to the appropriate UN Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction related to Iran, following re-application of UN Security Council Resolutions.
Oct 2025	Factual clarification to Interpretive Note of Recommendation 16	■ INR.16 Minor factual update at Paragraph 31 to clarify that a beneficiary financial institution should have effective risk-based policies and procedures for determining when to execute, reject, or suspend anypayment or value transfer lacking required originator or required beneficiary information (regardless of whether it is above or below the applicable threshold) or when they identify potentially misdirected payments "in the implementation of the requirements under paragraph 30".

© 2012-2026

Date	Type of amendments	Sections subject to amendments
June 2026	Revision of INR.6	■ INR.6 Updates to Recommendation 6 of the FATF Standards to incorporate the humanitarian exemption contained in the United Nations Security Council resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing, UNSCRs 2664 and 2761, as well as UNSCR 2615.

© 2012-2026

www.fatf-gafi.org