MAY 2025

REGCOUNSEL FINANCIAL SERVICES WHITE PAPER SERIES #4

Sanctions Policy Requirements

ABOUT THE AUTHORS

Mr. dr. drs. Jan Jans is a Dutch qualified lawyer specialized in financial regulatory law. He has a strong focus on the regulatory framework covering investment firms, banks, insurance companies, payment service providers, crypto-asset service providers and investment funds. Prior to joining Regulatory Counsel | Financial Services as Partner in 2022, Jan worked as a financial regulatory lawyer at various (international) law firms in the Netherlands.

Jan graduated from Nijmegen University in 2008. In addition to law, he studied financial economics and business administration. He completed the post-academic education Securities Law at the Grotius Academy in 2012. Jan publishes regularly in national law journals and successfully defended his PhD thesis on the level playing field between banks and non-banks in the European market for electronic payments in 2023.

Mr. drs. Jan-Jouke van der Meer is a Dutch qualified lawyer specialized in financial regulatory law. He advises clients on the full range of Dutch and EU financial regulatory laws (including MiFID, AIFMD, MiCAR, PSD2 and DORA), licensing issues, corporate governance (including integrity and suitability assessments), compliance and integrity-related issues (including AML and sanctions) and dealing with financial regulators. Prior to joining Regulatory Counsel | Financial Services as Managing Associate, Jan-Jouke worked as a financial regulatory lawyer at an international law firm in the Netherlands.

Jan-Jouke obtained a master's degree (LLM) in Corporate Law from VU Amsterdam in 2018, and holds a master's degree (MSc) in Financial Economics from Erasmus University Rotterdam (2018). He has also published various articles in the area of financial regulatory law.

Mr. Maarten Mol-Huging is a Dutch qualified lawyer specialized in financial regulatory law. He advises on (prudential) regulatory issues with regards to banks, investment firms, insurers, crypto-asset service providers and other financial sector entities.

Maarten graduated cum laude at the VU Amsterdam in International Business Law in 2022 on his thesis titled: The Biggest Challenge yet for EU Mortgage Lending: The Onset of Artificial Intelligence Tooling. In 2023, he furthermore completed the prudential regulation-oriented EBI Master in EU Banking and Financial Regulation in Frankfurt.

Recofise is a boutique law firm located in Amsterdam and specialises in financial regulation. Our clients consists of financial undertakings (e.g., banks, investment firms and funds, insurance companies, electronic money institutions, payment institutions and crypto-asset service providers) that are active on the Dutch and international financial markets. Recofise has extensive experience in advising and supporting clients with complex legal issues regarding prudential requirements, compliance, risk management, supervisory reporting and supervisory audits.

EXECUTIVE SUMMARY

This fourth edition of the Recofise White Paper Series provides a comprehensive analysis of financial sanctions compliance requirements for financial institutions operating within the EU, particularly focusing on recent regulatory developments and their practical implications. Against the backdrop of increasing geopolitical risk and a rapidly evolving sanctions framework, including the AMLD6, AMLR and guidelines from the EBA, this White Paper equips financial institutions with the tools to mitigate risks and ensure compliance in a landscape increasingly dominated by the *weaponisation of finance*.

First, this White Paper covers the origin and scope of sanctions, encompassing those imposed by the UN, the EU, and the Netherlands. Financial institutions are presented as gatekeepers with an obligation to identify, assess, and report sanctioned entities or individuals qualifying as a 'relation'. The document emphasizes the importance of tailored sanctions policies, effective risk assessments, and robust screening methodologies.

Second, governance plays a pivotal role in implementing these requirements. This White Paper therefore highlights the roles of management bodies, supervisory boards, and sanctions compliance officers in ensuring accountability and operational effectiveness. This White Paper also focuses on the Sanctions Risk Assessment, pursuant to which financial institutions must assess the amount of sanctions risk they are exposed to. In this assessment, there is a particular emphasis on risk factors, such as geographic, customer, and product-based exposures, illustrating the intricate dynamics institutions must address when complying with sanctions.

Third, practical insights on policies, screening processes, data utilization, and the calibration of compliance tools are provided, seeking to provide a useful roadmap for financial institutions to address both general and ad hoc requirements. Furthermore, the importance of employee training and cautious outsourcing practices underlines the approach needed for complying with sanctions legislation.

TABLE OF CONTENTS

1.
INTRODUCTION

1. INTRODUCTION

In recent years, the European Union ("**EU**") has significantly increased the use of restrictive measures[1], commonly known as "sanctions", as a foreign policy tool. This trend has accelerated since the Russian invasion of Ukraine in 2022, with a surge in sanctions targeting both individuals and entities. This strategic use of financial systems as instruments of enforcement is often referred to as the *weaponisation of finance*[2] and has imposed new demands on financial institutions.

As gatekeepers of the financial system, financial institutions are expected to assess whether their *relations* involve a sanctioned entity or person. Upon identifying a sanctioned entity or person, financial institutions are required to notify the competent authority and take appropriate measures to prevent such relation from having access to the financial system. However, the absence of a harmonized and detailed supervisory framework at a European level has made compliance by financial institutions increasingly challenging, leading to operational and legal uncertainties.

In response, a string of new publications and initiatives were developed in the past year seeking to tackle: (i) the outdated legal framework, (ii) the lack of clear guidance, and (iii) the measures applied by financial institutions. Particularly in the Netherlands, this led to a consultation on the revision of the current Sanctions Act 1977 (*Sanctiewet 1977*, "**Sanctions Act**"), supervisory reports by the Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") and the Dutch Authority for Financial Markets (*Autoriteit Financiële Markten*, "**AFM**")[3], and a renewed supervisory focus on the enforcement of sanctions by financial institutions. At the EU level, new regulations have been adopted in the form of the sixth Anti-Money Laundering Directive ("**AMLD6**")[4], the Anti-Money Laundering Regulation ("**AMLR**")[5] and the Transfer of Funds Regulation ("**TFR**")[6].

1 Broadly defined as: 'Union sanctions, i.e. sanctions adopted by the Union on the basis of Article 29 TEU or Article 215 TFEU, and national sanctions adopted by Member States in compliance with their national legal order (to the extent that they apply to financial institutions).' See also: art. 2(1) of Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union sanctions.

2 DNB, Weerbaar in een gure wereld: Geopolitieke risico's en financiële instellingen, (2024), p. 4.

3 AFM, Leidraad Wwft en Sanctiewet Toelichting op de Wet ter voorkoming van witwassen en financieren van terrorisme en de Sanctiewet 1977, (2024), ("**AFM Guideline**").

4 Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

5 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

6 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

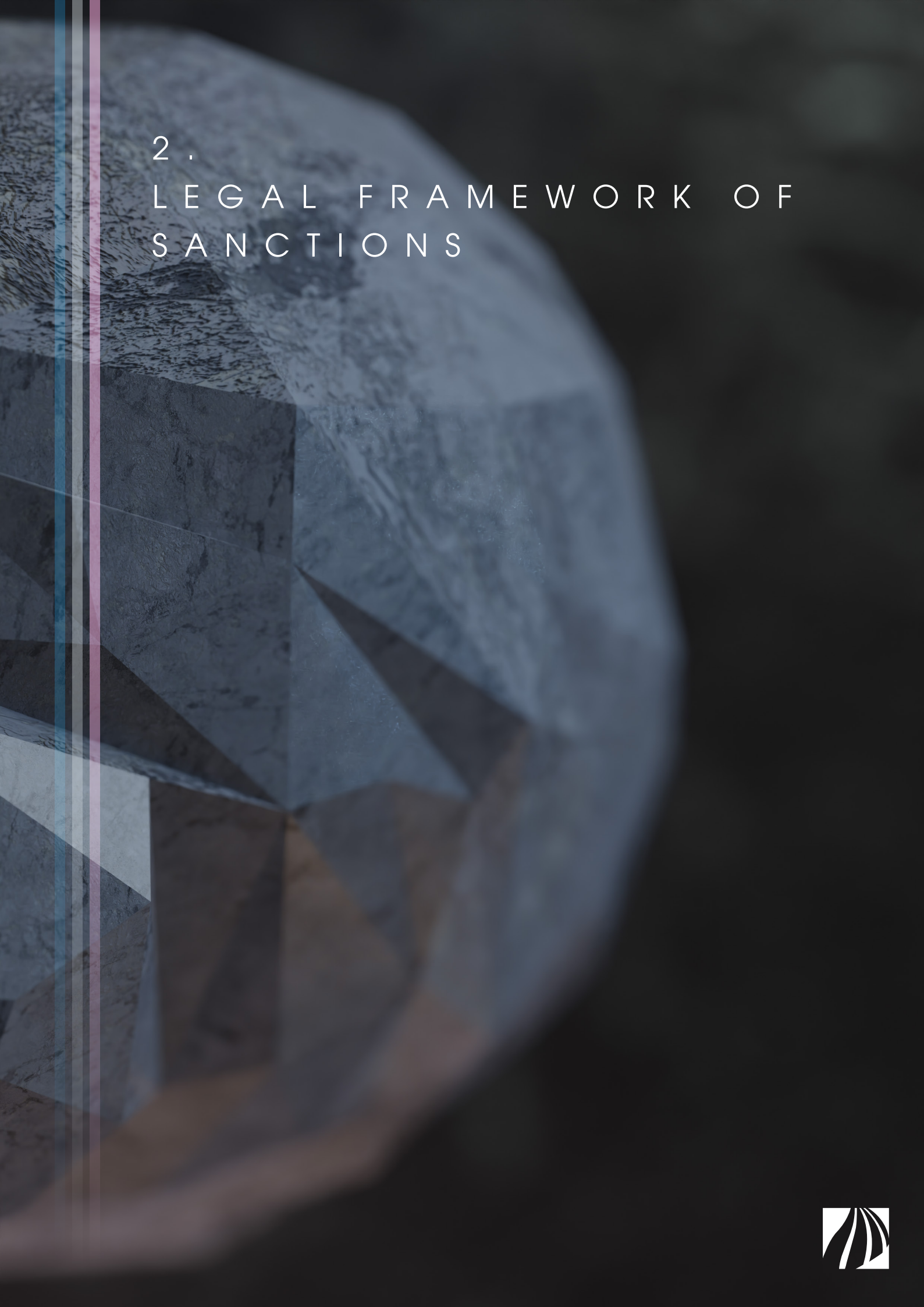
Additionally, the European Banking Authority ("**EBA**") published a set of new Guidelines on the policies and procedures in respect of sanctions to be maintained by financial institutions ("**EBA Sanctions Guidelines**")[7]. Furthermore, the European Council ("**Council**") provided its own guidance on the application of sanctions.[8]

Against this background, this White Paper provides a structured overview of the regulatory developments surrounding financial sanctions, with a particular focus on the impact on financial institutions operating in the Netherlands. Moreover, it offers a practical guide for drafting a sanctions policy, helping financial institutions navigate through these regulations.

This White Paper is structured as follows. First, we describe the legal framework of sanctions and the policies and procedures regarding sanctions. Thereafter we will discuss the governance surrounding sanctions and the sanctions risk assessment. Finally, we will go into the ongoing screening requirements and the outsourcing and training of employees.

7 EBA, Final Report: Two sets of Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national sanctions, (2024). Comprising the Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national sanctions (the "**EBA Sanctions Policy Guideline**"); and Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national sanctions under Regulation (EU) 2023/1113 (the "**EBA TFR Sanctions Guidelines**").

8 Council, Sanctions Guidelines – update (11618/24), (2024).



2. LEGAL FRAMEWORK OF SANCTIONS

2. LEGAL FRAMEWORK OF SANCTIONS

2.1 Where do sanctions come from?

Sanctions in the Netherlands can stem from the following three (3) distinct sources: (i) the United Nations ("**UN**"), (ii) the EU and (iii) the Dutch government.

The UN regularly adopt sanctions to support peaceful transitions, deter non-constitutional changes, combat terrorism, protect human rights, and promote non-proliferation of nuclear weapons. These measures are taken by the UN Security Council and are consolidated in the UN Sanctions List ("**UN List**"),[9] which is regularly updated. The UN List includes the names and relevant information of sanctioned (legal) persons to facilitate their reliable identification. However, the UN List, by itself, does not constitute binding law in the EU and is not directly enforceable on financial institutions. Nonetheless, as most (if not all) UN sanctions are adopted by the EU (see below), the UN List serves as an important tool for anticipating forthcoming sanctions before their adoption by the EU.[10]

The EU regularly adopts sanctions, either by incorporating sanctions issued by the UN or on its own initiative. The EU, specifically the Council, usually adopts sanctions independently: (i) when no consensus is reached on measures at the level of the UN (e.g., due to a veto by a permanent UN Security Council member) or (ii) to implement the EU's own foreign policy objectives. Once adopted, the European Commission ("**Commission**") is the EU institution primary responsible for overseeing the implementation of sanctions. As a result, sanctions are included in Council Regulations[11] and applied in conjunction with Commission guidance.

9 UN Security Council Consolidated List, (link) (last consulted: 19 November 2024).

10 Moreover, in the Netherlands, sanctions that have been adopted by the UN but which have not (yet) been adopted by the EU are legally binding, by means of the Sanctieregeling overbrugging tenuitvoerlegging sanctieresoluties van de Veiligheidsraad van de Verenigde Naties 2019; see also Dutch Minister of Finance, Leidraad Financiële Sanctieregelgeving, (2020), p. 5; Furthermore, following the implementation of the AMLR, obliged entities will also be required to retain records on assets and activities of persons included on the UN List but not yet on the EU List, see art. 27 and Recital (36) AMLR.

11 Council Regulation (EU) No 833/2014 of 31 July 2014 concerning sanctions in view of Russia's actions destabilising the situation in Ukraine; Council Regulation (EU) No 269/2014 of 17 March 2014 concerning sanctions in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (as amended).

Sanctions applicable within the EU are included in a consolidated list of individuals, groups and organisations subject to EU financial sanctions ("**EU List**"). Sanctions included in the EU List are directly applicable in the EU and must be directly observed by financial institutions. Additionally, the EU maintains the EU Sanctions Map, an interactive digital tool of all applicable sanctions ("**Sanctions Map**").[12] Notably, the Sanctions Map includes not only measures listed in the EU List but also sanctions such as service provision restrictions *vis-à-vis* a country (e.g., prohibitions on purchasing, importing or transferring gold from Russia).[13]

In the Netherlands, the primary legislative instrument in respect of sanctions is the Sanctions Act, supplemented by the Supervisory Regulation on the Sanctions Act (*Regeling toezicht Sanctiewet 1977*, "**Sanctions Act Regulation**"). The Sanctions Act serves as a framework regulation for the Dutch legislature to impose further sanctions than those adopted by the EU. In practice, this is predominantly applied to persons and entities designated as terrorists by the UN or the Dutch government, by including those on the national sanctions list terrorism (*Nationale Sanctielijst Terrorisme*, "**Dutch List**").[14] Furthermore, the Dutch Minister of Finance may issue regulations (*regelingen*) that support the implementation of EU sanctions. While technically directly applicable, these regulations serve to: (i) ensure the criminal nature of violations of EU measures within the Dutch criminal law framework, (ii) assign responsibility to the appropriate Dutch authority for overseeing the application of sanctions and (iii) implement Council decisions (as opposed to Council regulations) relating to sanctions.

Due to the extraterritorial scope of the Office of Foreign Assets Control ("**OFAC**") sanctions, Dutch financial institutions that are internationally active may also be required under U.S. federal law to adhere to these measures. Strictly speaking, however, sanctions issued by non-EU Member States (including OFAC sanctions) are not legally binding in the Netherlands.[15] In fact, adhering to some of these measures may even be prohibited under the EU Blocking Statute.[16] However, this only involves a limited amount of (American) sanctions, which do not cover all OFAC sanctions.

12 EU sanctions Map, (link) (last accessed: 19 November 2024).

13 Annex XXVI and XXVII of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning sanctions in view of Russia's actions destabilising the situation in Ukraine.

14 As created by the Sanctieregeling Terrorisme 2007-II; see for the Dutch List: (link).

15 See also Dutch MoF Guidance, (2020), p. 16; AFM Guidance, (2024), p. 51-52.

16 Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, (link).

Nevertheless, it may be prudent for financial institutions that wish (or are required to do so under a contractual obligation) to observe OFAC sanctions to check whether this is allowed by the EU Blocking Statute.

Furthermore, if a Dutch financial institution operates in another EU Member State, it may also be subject to sanctions imposed by the local legislature, i.e., the local equivalent of the Dutch List.[17] These are legally binding on the Dutch financial institution if they fall under the applicable national regulations.

2.2 What do financial sanctions comprise?

Financial sanctions typically require financial institutions to comply with the following three (3) obligations:[18]

I A freeze-of-funds requirement;

II A prohibition on directly or indirectly making financial means available to sanctioned (legal) persons; and

III A prohibition or restriction on the provision of certain financial services to the sanctioned (legal) persons.

These financial sanctions are usually applied simultaneously to a sanctioned person. Moreover, financial institutions are prohibited from knowingly and intentionally participating in activities of which the object or effect is to *circumvent* financial sanctions.[19] This requirement emphasizes the substance over form nature of the above prohibitions and imposes a result-oriented obligation to adhere to both the spirit and letter of the law. Consequently, financial institutions must assess, on a case-by-case basis, whether they effectively apply sanctions in specific situations. This includes evaluating the scope of relations under the Sanctions Act, such as identifying the representatives, owners or controllers of entities with which the financial institution engages.

17 Dutch MoF Guidance, (2020), p. 15.

18 See primarily, art. 2(2) of Council Regulation (EU) No 269/2014.

19 Art. 9(1) of Council Regulation (EU) No 269/2014; Commission, Opinion of 8.6.2021 on Article 2(2) of Council Regulation (EU) No 269/2014, (2021), p. 5-6.

2.3 What is a financial institution required to do under the sanctions?

Financial institutions must screen their *relations* when conducting business to identify any matches with (legal) persons included on the UN, EU or Dutch Lists.[20] Upon detecting a match, referred to as a 'hit', the financial institution must:

I Immediately (*onverwijld*) report the match to the competent authority (i.e., the AFM or DNB); and

II Refrain from making financial means available and/or providing the financial service in question and/or 'freeze' the funds, as applicable.

These obligations are rule-based, meaning these must be strictly followed, leaving no room for a risk-based approach.[21] However, as discussed further below, financial institutions may adopt a risk-based approach in *designing* the procedures for detecting persons subject to sanctions.[22]

20 Art. 1(b) Sanctions Act Regulation: 'relation: any person involved in a financial service or financial transaction.' This includes the customers of a financial institution, the beneficiaries of a transaction or product (e.g. addressees of benefits from a life insurance policy), the (ultimate) beneficial owner(s) or controllers of legal entities, partnerships, trusts and similar legal arrangements, correspondent relations and the counterparty to a financial transaction or product (e.g., in the case of a non-life insurance payment).

21 The Dutch Minister of Finance also considered that practically therefore, no real residual risk can exist in respect of sanction monitoring and application by financial institutions; see Dutch MoF, (2020), p. 10; see also Recital (8) AMLR: 'Measures should also be put in place to mitigate any (stress rec.) risk of non-implementation or evasion of targeted financial sanctions.'

22 See also, Recital (29) AMLR.

3. POLICIES AND PROCEDURES REGARDING SANCTIONS

3 POLICIES AND PROCEDURES REGARDING SANCTIONS

Pursuant to the Sanctions Act Regulation, a wide range of financial institutions must have policies and procedures in place that enable effective compliance with sanctions. These institutions include, amongst others, banks, investment firms, fund managers, insurance companies, payment institutions and electronic money institutions. Under the legislative proposal of the Dutch Act on international sanction measures (*Wet internationale sanctiemaatregelen*), for which a public consultation was launched between 7 June and 9 August 2024, this group of institutions will be expanded with, among others, attorneys-at-law, notaries and tax advisers. Similarly, under the AMLR, obliged entities must have in place internal policies, procedures and controls to ensure compliance with the Anti-Money Laundering and Counter Terrorism Financing ("**AML/CTF**") rules, and, in addition to the obligation to apply targeted financial sanctions, mitigate and manage the risks of non-implementation and evasion of targeted financial sanctions.

In practice, policies and procedures related to sanctions are often incorporated in an AML/CTF policy framework. While this approach may generally be effective (and straightforward), the growing emphasis of authorities regarding sanctions increasingly justifies the use of a stand-alone policy on sanctions ("**Sanctions Policy**"). This view is also supported by the EBA Sanctions Guidelines, which focus on having such separate policy.

Central to a Sanctions Policy is the exposure to *sanctions risk* and the methodology to address this risk. In our view, a working definition of "sanctions risk" could be the '*risk of failing to properly observe sanctions, either by directly transgressing such measures or by (knowingly) participating in their circumvention or indirectly providing financial services or funds or other financial means to sanctioned natural or legal persons.*'

Building on this definition and the EBA Sanctions Guidelines, this White Paper outlines the essential components of a Sanctions Policy.

EBA Sanctions Guidelines

The EBA Sanctions Guidelines can be categorised as own-initiative guidelines, meaning that they do not derive from a direct legal mandate for the EBA to develop them. These guidelines are primarily intended for banks, payment institutions, and electronic money institutions. However, given the EBA's authority and the universal obligation for most financial institutions in the EU to comply with sanctions, these guidelines are also highly relevant for other financial institutions.[23]

As set out above, in the Netherlands, nearly all regulated financial institutions are, to some extent, required to implement a Sanctions Policy, further evidencing the (indirect) relevance of the EBA Sanctions Guidelines for those financial institutions.

EBA TFR Sanctions Guidelines

The EBA TFR Sanctions Guidelines, in contrast, are based on a specific legal mandate under Article 23 TFR.[24] These guidelines apply explicitly to payment service providers ("**PSPs**") and crypto-asset service providers ("**CASPs**"). However, the TFR clarifies that this regime is temporary and will ultimately be replaced by provisions of the AMLR and AMLD6.[25]

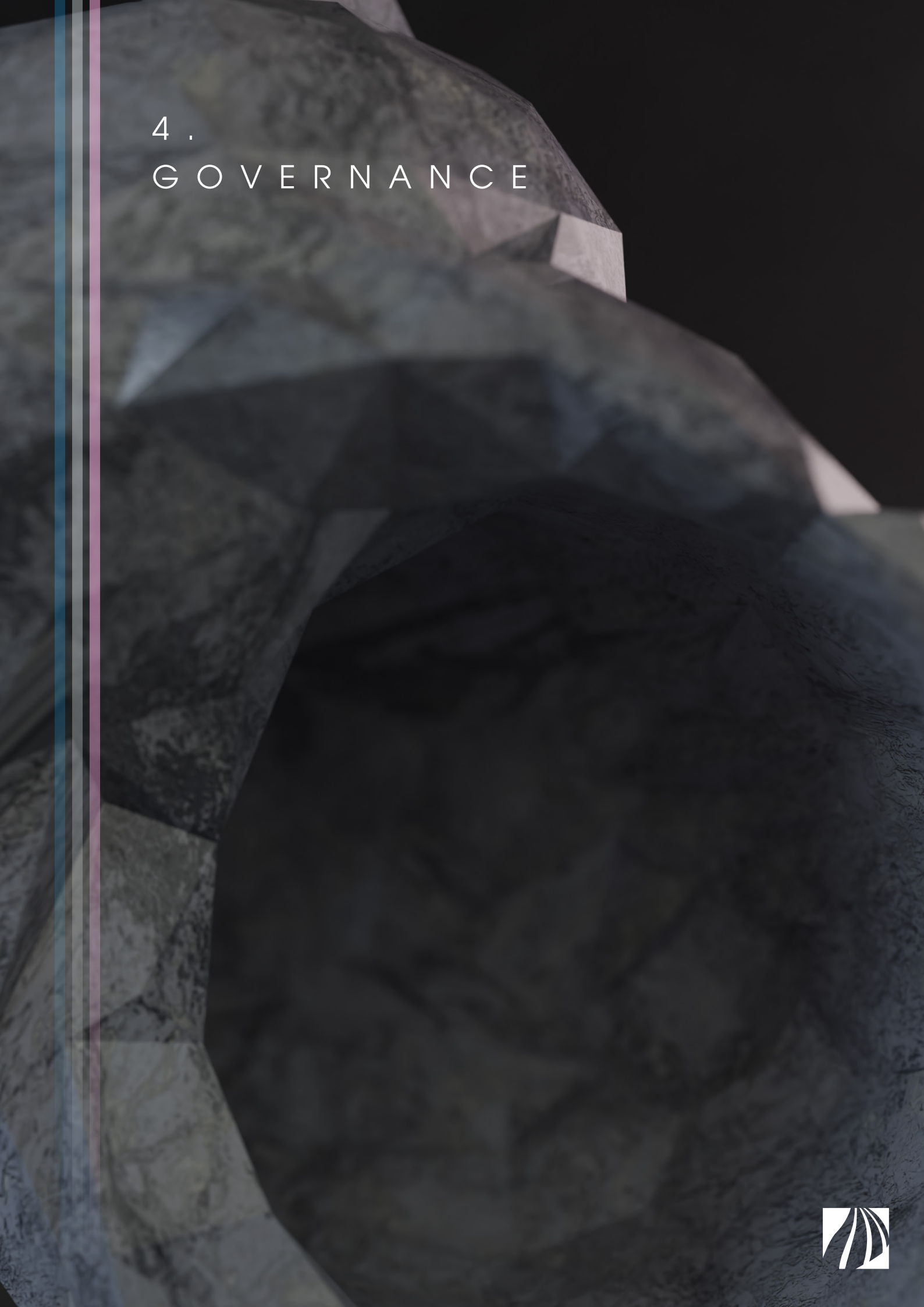
23 Thus, where we refer to financial institutions we refer to all financial undertakings that are subject to supervision by the AFM or DNB. Other non-financial undertakings do not necessarily have to take the considerations of this White Paper into account, though the conclusions may still be of relevance for those parties.

24 Art. 23 TFR: 'Payment service providers and crypto-asset service providers shall have in place internal policies, procedures and controls to ensure the implementation of Union and national sanctions when performing transfers of funds and crypto-assets under this Regulation.'

25 Recital (18) TFR.

It is important to note that some of the measures to be included in the Sanctions Policy may appear overly complex or burdensome for smaller financial institutions. There is, however, no *one-size-fits-all* for sanctions screening. Under the Sanctions Act (and the Sanctions Act Regulation), each financial institution retains the discretion to design a sanctions screening framework tailored to its specific operations, size and risk profile.

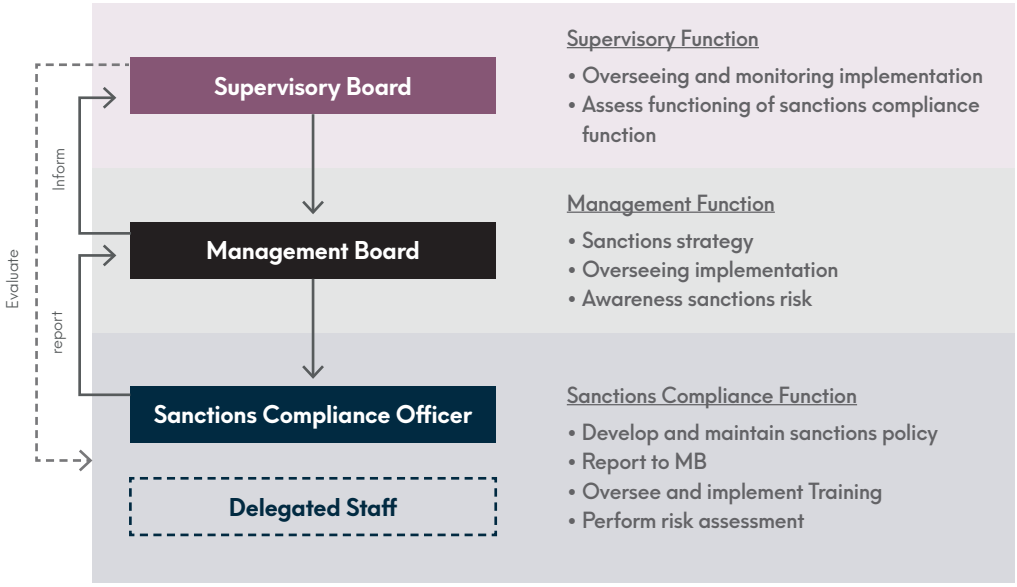
The measures described here, however, are intended as best practices or guidance for drafting a comprehensive and clear Sanctions Policy. Nevertheless, the measures described and guidance given can be seen as a *best practice* or as a guiderail for drafting a clear policy document in light of the ambiguous legal framework.



4.
GOVERNANCE

4. GOVERNANCE

The financial institution's governance structure is critical to ensuring its effective oversight and application of sanctions. The diagram below outlines the recommended governance framework, emphasizing the hierarchy of roles and responsibilities. While this structure can be adapted to the size and complexity of the institution, maintaining the hierarchy of roles is essential for clarity and accountability.



4.1 Management body

The management body is ultimately responsible for approving the strategy regarding sanctions and ensuring its effective implementation. All members of the management body must be aware of the institution's prevailing sanction risk, requiring periodic updating of the management body on the status of such risk.[26] In group structures, the parent entity's management body must ensure subsidiaries have the necessary information and resources to comply with the Sanctions Policy. However, the management bodies of the subsidiary retain primary responsibility for adherence to sanctions at their respective levels.[27]

26 Moreover, we expect that sanctions may become one of the topics the knowledge of which is by management body members is assessed in the fit and proper assessment.

27 EBA Sanctions Policy Guideline, (2024), par. 3-7.

4.1.1 Management board

The management board, or the management body in its executive function, must remain up-to-date with the sanction risk assessment(s) and ensure that the outcome thereof is proportionally translated into the Sanctions Policy, both in terms of the granularity of the Sanctions Policy itself and the procedures applied in the implementation thereof.[28] Moreover, the management board is responsible for ensuring that the functions tasked with executing the Sanctions Policy are sufficiently staffed, structured and equipped to ensure that the sanctions are complied with.[29]

4.1.2 Supervisory Board

The supervisory board, or the management body in its supervisory function, should monitor and oversee the application of the Sanctions Policy. To fulfil this requirement, the supervisory board must be: (i) informed about the outcome of the risk assessment (discussed in paragraph 5.1), (ii) take appropriate action when it detects any deficiencies in the application of the Sanctions Policy and (iii) at least annually review the effectiveness of the Sanctions Policy and its implementation (see paragraph 6.3).[30] In group structures, the supervisory board of the parent entity oversees compliance on a group level, while supervisory boards of subsidiaries retain responsibility for their respective entities.

4.2 Sanctions Compliance Officer

Financial institutions must appoint a senior staff member responsible for the operational oversight of the Sanctions Policy's application ("**Sanctions Officer**"). This role can be combined with other functions (e.g., AML/CTF Compliance Officer or Chief Compliance Officer) as long as the combination does not compromise the independence or effectiveness of the Sanctions Officer.[31] For institutions with substantial sanctions risk, separation of the Sanctions Officer role from other functions may be more appropriate.

28 Where the term proportionality must still be understood within the principle-based frame of the Sanctions Act, i.e. the proportionate measures must still be adequate in ensuring that the sanctions are observed.

29 EBA Sanctions Policy Guideline, (2024), par. 11-12.

30 EBA Sanctions Policy Guideline, (2024), par. 8-10.

31 Compare also art. 11(2) AMLR.

The Sanctions Officer must be able to liaise directly with other control functions and should have direct reporting lines to the management body, though it may sub-delegate some of its responsibilities to its subordinates. Ultimately, the Sanctions Officer remains responsible for the tasks attributed to it, regardless of any delegation. We recommend that financial institutions include clear mandates for Sanctions Officers, specifying what tasks may and which may not be delegated to lower level employees.[32]

The main duties of the Sanctions Officer are to apply the Sanctions Policy effectively and to report to the management body on specific data points (see below). We can imagine that the Sanctions Officer personally sees to the effective application of the Sanctions Policy and reporting to the management board, but that the operational procedures and gathering of the (to be reported) information is left to lower level employees. What seems to be an essential task of the Sanctions Officer that logically is not delegated, is reporting to the AFM or DNB in case of positive screening hits. The Sanctions Officer should be the main liaison between the financial institution and the competent authority.

32 EBA Sanctions Policy Guideline, (2024), par. 15-17.

The information that the Sanctions Officer must report to the management body can be best comprised in the *periodic* reporting of the AML/CTF officer (where this function has been combined with the Sanctions Officer) to the management body or should be set up as a separate periodic report. Given the frequent alterations to sanctions, this report should be submitted at least annually and, probably, at least quarterly.

The report should contain the following information:[33]

I. Changes to the sanction risk to which the financial institution is exposed;

II. The outcome of the sanctions exposure assessment;

III. Changes to sanctions regimes and their impact;

IV. Statistics and information relating to:

   a. the number of alerts generated;

   b. the number of alerts awaiting analysis;

   c. the number of reports submitted to the competent authority;

   d. the average time between the true positive match and the report submitted to the competent authority;

   e. the value of frozen funds, frozen economic resources and the nature of those assets, held at the financial institution;

V. Information on human and technical resources and the adequacy of those resources in light of the financial institution's sanctions risk;

VI. Deficiencies or shortcomings identified in relation to the financial institution's Sanctions Policy, including observations provided by the competent authority;

VII. Cases of violation and circumvention of sanctions and the reasons for those;

VIII. Proposals on how to address any changes in regulatory requirements or in sanctions risk, or any deficiencies or shortcomings in the Sanctions Policy that have been identified and cases of violation and circumvention of sanctions that have been identified.

33 EBA Sanctions Policy Guideline, (2024), par. 19.

5. SANCTIONS RISK ASSESSMENT

5. SANCTIONS RISK ASSESSMENT

Financial institutions must assess the amount of sanctions risk they are exposed to ("**Sanctions Risk Assessment**"). This obligation, as formulated by the EBA, aligns with existing practices, such as the general risk assessment (GRA) or the systematic integrity risk assessment (SIRA).[34] However, the Sanctions Risk Assessment must be enshrined in its own governance, or at least governance meeting the requirements of the EBA Sanctions Policy Guideline.[35]

This own governance must: (i) include the methodology used for the Sanctions Risk Assessment, (ii) specify the applicable periodic and ad hoc reassessment moments and (iii) be provided to the competent authority, along with the risk assessment itself.[36]

In group structures, each subsidiary is responsible for its own Sanctions Risk Assessment, while the parent undertaking performs a group-wide assessment.

5.1 Outputs of the Sanctions Risk Assessment

The Sanctions Risk Assessment must consider a set of risk factors,[37] based on a certain set of information[38] and their effect on the following outputs:

I Identification of applicable sanctions regimes;
II Likelihood of non-implementation of sanctions;
III Likelihood of sanctions circumvention; and
IV Impact of potential sanctions breaches.

34 See DNB, The section on the Sanctions Act in the former DNB Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act (DNB Leidraad Wwft en Sw) Version December 2020, (2024) (the "**DNB Guideline**"), p. 3; and see DNB Consultation, DNB SIRA Good Practices, (2024) (the "**(draft) DNB SIRA Good Practices**"); AFM Guideline (2024), p. 50; Art. 10(1) AMLR.

35 EBA Sanctions Policy Guideline, (2024), p. 23: '[The Sanctions Risk Assessment] is different from the AML/CTF risk assessment described in the EBA's Risk Factors Guidelines as the same elements can carry different risks from an AML/CTF and sanctions perspective, although some synergies exist. For example, a jurisdiction may be associated with high levels of corruption and thus increased ML risk, but it may present very few risks from a sanctions perspective.'

36 EBA Sanctions Policy Guideline, (2024), par. 27.

37 Being (a) geographic risk; (b) customer risk; (c) products and services risk; and (d) delivery channels risk.

38 Being a sufficiently diverse range of information sources, including at least the following (a) information obtained as part of the application of the financial institution's customer due diligence measures, (b) information from international bodies, government, national competent authorities including AML/CTF supervisors, financial intelligence units and law enforcement authorities, such as up-to-date typologies on the circumvention of sanctions, (c) information from credible and reliable open sources, such as reports in reputable newspapers and other reputable media outlets, (d) information from credible and reliable commercial organisations, such as risk reports and (e) where this is available, an analysis of previous sanctions alerts concerning true positive and false positive matches in order to identify situations where true positive matches are most likely to occur.

The assessment's outcome typically includes a gross risk figure adjusted with mitigating measures, resulting in a net risk figure. If the net risk is within the financial institution's risk appetite and sanctions strategy, the institution may accept the outcome of the Sanctions Risk Assessment. Mitigating measures must be implemented in the Sanctions Policy and the institution's operational procedures. An example of such mitigating measures could be, where a financial institution has a high exposure to geographic risk, the use of *geolocation tools* in the screening process (see paragraph 6.2).[39] Other examples of mitigating measures could include:

I. Upon establishing (business) relations, acquiring detailed information about the customer's type of business and countries where the customer is conducting business;

II. Requesting additional information from the customer, such as a description of dual-use goods or any goods subject to sectoral sanctions, information about the appropriate licence for dealing with the dual-use goods, country of origin of the goods, information about the end user of the goods;

III. Requesting more detailed information from the customer about the purpose of a transfer of funds or crypto-assets;

IV. Using the following data: shipping registers, real estate records and other publicly available datasets (where available) for screening purposes.

5.2 Risk factors

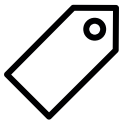
The Sanctions Risk Assessment should include the following risk factors: geographic risk, customer risk, products and services risk, and delivery channels risk.[40]

Geographic risk includes the risk: (i) where the financial institution conducts its business and performs transactions, i.e., the jurisdictions and territories in which the financial institution is established or operates, (ii) the extent to which those jurisdictions and territories are exposed to restrictive measures or are known to be used to circumvent restrictive measures, and (iii) the origin and destination of transactions. The relevant jurisdictions could then be assessed for their exposure to sanctions or whether they are known for circumventing sanctions.

39 I.e. tools that could detect the use of proxy services to identify and prevent IP addresses that originate from a country for which sanctions apply, affecting the ability of this country to access the PSP's and CASP's website and services for an activity that is prohibited under sanctions.

40 EBA Sanctions Policy Guideline, (2024), par. 23; Recital (30) AMLR.

Customer risk includes the risk related to the links of customers and their (ultimate) beneficial owners and controlling shareholders, to countries for which sanctions are in place due to a situation affecting this country, or known to be used to circumvent sanctions. Furthermore, customer risk is affected by the number of customers, the type of customers, and the complexity of those customers, such as the issues with identification of the beneficial owner. Moreover, customer risk is affected by the (transaction) activity of the customer base and complexity of the activity, including any links to industries or sectors that may be subject to economic or any other restrictive measures, as well as frequency and types of transactions.[41]



Products and services risk includes: (i) the risk related to the nature of the financial institution's products and service offering, and (ii) the extent to which providing these products and services exposes the financial institution to the risk of breaches of sanctions and circumvention of sanctions.

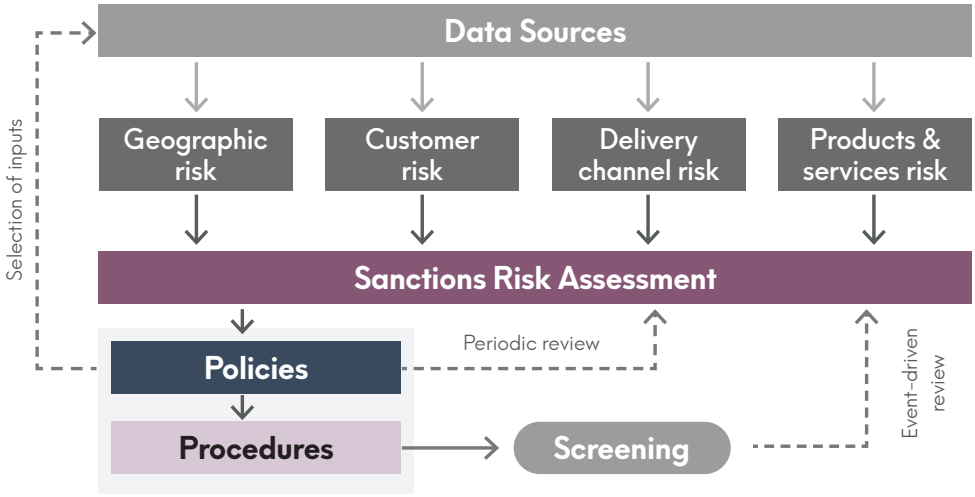
Delivery channels risk, including whether the use of intermediaries, agents, third parties, correspondent banking relationships or other delivery channels creates vulnerabilities to sanctions, is particularly prevalent where the financial institution has limited visibility on the parties involved, making the financial institution dependent on the screening processes of third parties. Moreover, this risk increases the financial institution's exposure to geographic risks where delivery channels are operating or based in countries for which sanctions are in place or in countries known to be used to circumvent sanctions.

5.3 Review of Sanctions Risk Assessment

The Sanctions Risk Assessment must be **periodically** reviewed, at least once per year. This ensures that financial institutions reassess their exposure to sanction risks and confirm whether their Sanctions Policy and procedures remain proportionate and effective. If the review determines that the framework remains appropriate, no changes are required. If any changed risks (or shortcomings)[42] are identified, the financial institution must recalibrate its Sanctions Policy and procedures to address them.

41 Including any links to industries or sectors that may be subject to economic or any other sanctions.

42 In which case, there might be cause for the financial institution to rescreen its customer database for relations that match any of the UN, EU or Dutch Lists; see EBA Sanctions Policy Guideline, (2024), par. 25.



Moreover, there may be cause for an **ad hoc** review of the Sanctions Risk Assessment when certain events occur.[43] Generally speaking, these events comprise *significant changes* to either the sanctions framework or to the business activities of the financial institution.[44] Such events include:

I Adoption of new sanctions and significant changes to existing sanctions;

II Before providing new products, offering new product delivery channels, servicing new client groups, entering new geographical areas;

III Significant changes to the institution's activity profile, customer base, organisational structure or business model;

IV Identification of non-implementation of sanctions and circumvention of sanctions, which reveals the inappropriateness of the sanctions exposure assessment; or

V Deficiencies in existing sanctions exposure assessment as identified by the financial institution or the competent authority.

We note in respect of point: (i) that a full reappraisal of the Sanctions Risk Assessment may not be feasible with every new sanction, as these may occur frequently. Instead, financial institutions could conduct a quick-scan for immediate assessment of whether the new sanctions have a relevant impact on the Sanctions Risk Assessment. If relevant, a full ad hoc review may be warranted; if not, the new sanctions could be incorporated in the next periodic review.

43 EBA Sanctions Policy Guideline, (2024), par. 26; see for an example: (draft) DNB SIRA Good Practices (2024), p. 30.

44 Consequently, a part of the Sanctions Risk Assessment will have to be reviewed, but probably not the entire Sanctions Risk Assessment. Ad hoc reviews generally limit themselves to the affected areas.

We stress, however, that the sanctions themselves have to be applied immediately. We recall that financial institutions must always ensure the effective application of the sanctions (i.e., the principle-based nature of sanctions).

Ultimately, the review of the Sanctions Risk Assessment must ensure that it remains up-to-date and relevant and that its outcome is properly reflected in the Sanctions Policy.[45] The procedure that ensures this, i.e., detailing when and how periodic or ad hoc assessments are performed, should be properly detailed in the Sanctions Policy.[46]

45 EBA Sanctions Policy Guideline, (2024), par. 30(d).
46 EBA Sanctions Policy Guideline, (2024), par. 30(c).

6.
ONGOING SCREENING

6. ONGOING SCREENING

Using the outcome of the Sanctions Risk Assessment and the applicable governance framework, the Sanctions Policy must describe the financial institution's control framework for effective implementation of sanctions, starting from the moment they are issued. As any delays in implementing sanctions could expose the institution to significant legal, reputational and financial risks, it is of the utmost importance to have a robust Sanctions Policy. We emphasize that the obligation to observe the sanctions is rule-based and must be executed effectively.[47]

A quintessential element of the Sanctions Policy is the establishment of robust procedures for **ongoing screening**. This refers to the continuous operational process that ensures none of the financial institution's relations are listed on the UN, EU or Dutch Lists.[48]

To achieve effective ongoing screening, the following three (3) core elements must be incorporated:

I Up-to-date information sources on:
   - **a.** sanctions; and
   - **b.** relations;

II Robust screening processes that effectively match (a) with (b) above, within due time; and

III An adequate review process that ensures continuous functionality of (I) and (II) as necessary.

47 DNB Guideline (2024), p. 3: '[The reporting] requirement cannot be fulfilled on a risk basis, so the institution cannot opt to not comply with the sanctions regulations and dispense with the continuous screening of customers.'; Recital (33) AMLR: 'The risk-sensitive nature of AML/CTF measures related to targeted financial sanctions does not remove the rule-based obligation incumbent upon all natural or legal persons in the Union to freeze and not make funds or other assets available, directly or indirectly, to designated persons or entities.'

48 See art. 26(4) AMLR: '[O]bliged entities shall regularly verify whether the [screening of customers for sanctions, are met]. The frequency of that verification shall be commensurate with the exposure of the obliged entity and the business relationship to risks of non-implementation and evasion of targeted financial sanctions.

6.1 Information sources for screening

To conduct effective screening, the financial institution must use accurate and up-to-date information. First, the financial institution must implement a process that ensures access to newly issues or amended sanctions on a **real-time basis**.[49] Second, the financial institution must have a reliable database of its *relations*.

Third-party data service providers often offer combined solutions for sanctions-related and AML/CTF data services. In this context, we note that the range of 'relations' under the Sanctions Act is broader than the concept of 'business relations' under the AML/CTF framework and that, as a result, financial institutions must ensure that the databases of its own customers are sufficiently comprehensive.[50] The process adopted by the financial institution to ensure up-to-date information on the applicable sanctions as soon as they are published, should be clearly described in the Sanctions Policy.

6.2 The screening process

The Sanctions Policy must clearly define the screening process for identifying matches between the sanctioned entities and the financial institution's relations. Screening should occur at two (2) key points in time:[51]

I **Periodically**: For all relations, with a frequency aligned to the outcomes of the Sanctions Risk Assessment and immediately upon updates of the UN, EU or Dutch Lists.[52]

II **Incidentally**: Prior to executing transactions, including screening counterparties to those transactions, during the onboarding of new customers[53] or when significant changes occur in customer relationships, including termination.[54]

49 Compare also EBA TFR Sanctions Guideline (2024), par. 8-9.

50 For instance, a depot bank of a customer is not in scope of the AML/CTF screening, though it is in scope of the sanctions screening; AFM Guideline (2024), p. 50.

51 Dutch MoF Guidance, (2020), p. 10; DNB Guideline (2024), p. 3-4; EBA TFR Sanctions Guideline (2024), par. 14-16; AFM Guideline (2024), p. 51.

52 This needs to be frequent. A single annual periodic screening is most probably not enough, unless the Sanctions Risk Assessment points towards a very low sanction risk.

53 Art. 20(1)(d) AMLR.

54 Again, see also art. 26(4) second sub-paragraph AMLR.

At these points, financial institutions must compare their relations' data against the UN, EU or Dutch lists. Given the complexity and scale of this task, it is typically feasible only with automated systems, potentially supported by artificial intelligence ("**AI**"). These systems must be calibrated to ensure the institution can consistently identify whether its relations or transactions are subject to sanctions.[55]

6.2.1 Sanction screening during transactions

All parties involved in transactions must be screened against the UN, EU and Dutch Lists, including third parties that are involved **prior to the effectuation of those transactions**.[56] This obligation extends to crypto-asset transfers facilitated by CASPs.[57]

For transactions with third-parties, financial institutions may rely on the third party's sanctions screening, provided that the agreement between the parties explicitly requires both to conduct screening in compliance with the Sanctions Act and includes provisions requiring the parties to inform each other of transactions that will be or are frozen and the screening against all applicable lists, including the Dutch list.[58]

> An exception to this requirement is provided by the Instant Payments Regulation ("**IPR**")[59]. During the execution of an ***instant credit transfer***,[60] the PSP of the payer and the PSP of the payee involved in the execution of that instant credit transfer are not required to perform incidental sanction screening of the opposing party to the instant credit transfer.[61] However, PSPs involved in the execution of such transfers must conduct periodic screening, at least daily, to verify that none of their customers are subject to sanctions.[62]

55 DNB Guideline (2024), p. 3.

56 DNB Guideline (2024), p. 6.

57 EBA TFR Sanctions Guideline (2024), par. 19.

58 DNB Guideline (2024), p. 6-7.

59 Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.

60 Means a national or cross-border payment from or to a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer which is executed immediately, i.e. within ten (10) seconds, 24 hours a day and on any calendar day.

61 Art. 5d(2) IPR.

62 Art. 5d(1) IPR; The obligation of PSPs to periodically verify their customers is related only to persons or entities subject to targeted financial sanctions.

6.2.2 Data used for screening

An advantage for financial institutions is that the data used for sanctions screening does not have to be verified, unlike data used in the AML/CTF screening processes. Furthermore, processing personal data for sanctions screening is permissible under data protection regulation.[63] Institutions have flexibility in determining what data to use, provided the approach is such is an effective risk-based process (to achieve the principle-based goal) and in line with the Sanctions Risk Assessment.

While a basic screening process might only utilize the name of a (legal) person, this approach risks generating numerous false positives. To reduce false positives and improve accuracy, financial institutions are advised to incorporate as many relevant data points as possible in their screening process:

For natural persons

I First name(s);
II Last name;
III Date of birth;
IV Place of birth; and
V Place of residence.

For legal persons

I Name of incorporation;
II Place of incorporation;
III Beneficial owners; and
IV (Purportedly) Authorised persons.

63 See, for instance, Recital (32) IPR.

For transactions[64]

i Information on the originator/payer and beneficiary/payee;
ii The description and/or purpose of the transaction;
iii Involved jurisdiction(s);
iv Financial intermediaries involved in the transaction; and
v (Wallet addresses for crypto-asset transfers).[65]

The EBA TFR Sanctions Guidelines require PSPs and CASPs to at least screen against:

i First name or name of incorporation;
ii Last name (both in original form and transliteration); and
iii Date of birth.

Incorporating multiple data points may initially increase the effort required to gather data, but it ultimately reduces compliance burdens by lowering false positives and improving the detection of sanctioned (legal) persons.

Data quality is critical to effective sanctions screening. Precise data reduces false positives and enhances the identification of sanctioned persons. Moreover, the amount of datapoints used in the screening may also be calibrated to the outcome of the Sanctions Risk Assessment (see paragraph 5.1).[66]

64 EBA TFR Sanctions Guideline (2024), par. 21.

65 Where such addresses are included in the UN, EU or Dutch Lists. Where CASPs process large amounts or volumes of crypto-transfers, they should- according to the EBA – consider incorporating blockchain analysis in their screening process. The EBA does not provide any further guidance on this, leaving it unclear what is a large amount or volume and what the blockchain analysis would add; EBA TFR Sanctions Guideline (2024), par. 21(f) and 23.

66 EBA TFR Sanctions Guideline (2024), par. 10.

A crucial role of data quality for the purposes of sanctions screening is to combat **financial exclusion (discrimination)**. Due to the geographic concentration of sanctions in certain countries, persons that trace their names from these areas might quickly be identified as potential hits with persons included on the UN, EU or Dutch Lists. As a result, such persons are frequently faced with a refusal to be onboarded or lengthy transaction/onboarding processes. Automated decision-making, especially when AI is involved, can exacerbate these issues without adequate data.[67]

To address this, institutions should utilize comprehensive datasets, including, but not limited to, the detailed data points outlined above, ensuring a balanced and non-discriminatory approach to sanctions compliance.

6.2.3 Screening methodology

The Sanctions Policy should include a clear and detailed description of the operational methodology used for sanction screening, aligned with the Sanctions Risk Assessment. A critical component is the calibration of the screening tool, as highlighted by the EBA:

> **'Calibration should be neither too sensitive, causing a high number of false positive matches, nor insufficiently sensitive, leading to designated persons, entities and bodies not being detected or free format information not used for other sanctions.'**[68]

Calibration must be documented in the Sanctions Policy *prior* to the screening and reviewed periodically and incidentally whenever updates to the Sanctions Risk Assessment or other triggering events occur.[69]

67 See (draft) DNB SIRA Good Practices (2024), p. 15; DNB, Tegengaan van discriminatie door banken bij de naleving van de Wwft, (2024); AFM Guideline (2024), p. 54.

68 EBA TFR Sanctions Guideline (2024), par. 24(a).

69 See for PSPs and CASPs: EBA TFR Sanctions Guideline (2024), par. 25. Though other financial institutions do not necessarily have to apply algorithmic techniques and thus do not necessarily incur the complexity of describing the governance of such models, we believe that the description of the screening tool should be robust. Eventually, this governance will be the key element under review in instances where a financial institution failed to observe a sanction.

For example, a screening tool based solely on first and last names may detect sanctioned individuals but is likely to generate an excessive number of false-positives. Introducing middle names as an additional parameter can significantly reduce false positives. For instance, while there may be numerous "John Smiths", there are far fewer "John Archibald Smiths", and even fewer with a specific birthdate, such as 29 February 2000. The inclusion of additional parameters is, therefore, essential to achieving a balance between detection and efficiency.

Algorithmic and AI screening

Automated detection systems must allow for some margin of imprecision to function effectively.[70] For instance, a model could be calibrated to produce hits for all 80%+ matches, rather than only 100% ones. This approach ties into the concept of **fuzzy matching techniques**, which, as required by EBA, must be employed by PSPs and CASPs.

Fuzzy matching is technology utilizing AI and machine learning to identify similar but not identical elements in datasets. Properly implemented, it enables the screening of names or phrases even when spelling, patterns or phonetics differ slightly from sanctioned entities.

Where a financial institution uses an **AI-based tool for sanctions screening**, it must explain: (i) how the parameters of the tool are calibrated, (ii) what they screen for (high-level), (iii) the verification of the accuracy of the methodology used, (iv) the expected behaviour of the model and (v) the expected output of the model.[71]

70 For example, the use of diacritics in names may not always be reflected in the names used by the screening tool. As such, a certain margin needs to be incorporated in order not to accidentally exclude persons based on such technicalities.

71 See also the EBA TFR Sanctions Guidelines (2024), par. 4-7 and 43.

White-listing

To reduce repetitive false positives, financial institutions may use a white-list to exclude specific (legal) persons that have been assessed as not subject to sanctions. Such white-list includes those persons that should not trigger a hit. The Sanctions Policy must establish robust processes for managing white-lists, including: (i) periodic reviews of the white-list, particularly after new sanctions are issued and (ii) documenting individual decisions to place entities on the white-list.[72]

Circumvention risk: Typologies and trends

Financial institutions must account for **typologies and trends** related to sanctions *circumvention* to prevent their involvement in such activities.[73] Relevant typologies and trends are frequently published and updated by public authorities, including:

I The Commission (e.g.,: link);
II DNB and/or the AFM;
III Financial Intelligence Unit Netherlands ("**FIU Netherlands**") (link);
IV Relevant public-private initiatives; or
V Other European authorities (e.g., EBA or the future AMLA).

72 EBA TFR Sanctions Guideline (2024), par. 13.

73 This as it is prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent sanctions, see art. 12 of Council Regulation (EU) No 833/2014; EBA TFR Sanctions Guidelines (2024), par. 44-46.

These typologies should be assessed in the Sanctions Risk Assessment as part of the risk factors (see paragraph 5.2),[74] but should also be part of the screening methodology (and subsequent investigations). The Sanctions Policy should describe the manner in which the financial institution continuously incorporates the typologies within its policy and procedure framework (and when),[75] ensuring that attempts to circumvent sanctions are effectively prevented. If correctly implemented, the screening methodology (and the due diligence process) should enable the financial institution to identify red-flags for circumvention risk, such as attempts to:

I Omit, delete or alter information in payment messages;

II Channel transfers through persons connected with a sanctioned person;

III Structure transfers to conceal the involvement of a sanctioned person;

IV Conceal the beneficial ownership or control of assets; and/or

V Use counterfeited or fraudulent background documentation for transfers.

6.2.4 Hits with the UN, EU or Dutch List: Due diligence

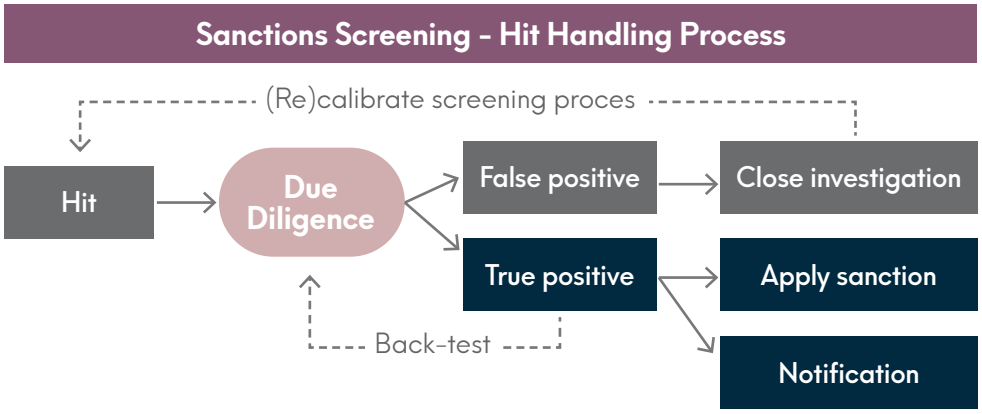
When the screening process produces a (partial) match with the UN, EU or Dutch Lists, financial institutions must investigate ***without delay***. The Sanctions Policy should describe: (i) which persons/functions are responsible for these investigations, (ii) what the applicable timelines are and (iii) how the outcome of the investigations is followed-up.[76] Particularly, the Sanctions Policy should describe the process of differentiating initial hits into **false positives**[77] and **true positive hits**. Such **due diligence** process must be clearly outlined.

74 In the Sanctions Risk Assessment, financial institutions should: (i) identify threats and vulnerabilities to circumvention risk, (ii) assess the risk and (iii) design of mitigating measures; see Commission, Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention, (2023), p. 4-5.

75 Where we suggest including circumvention risk in the periodic and/or incidental reassessment/review if necessary.

76 EBA TFR Sanctions Guideline (2024), par. 31.

77 False-positives are not reported to the competent authorities, as are undifferentiated hits.



A due diligence process should include at least the following elements[78]:

I Rules that prescribe the **timely investigation** of all hits generated;

II Rules on the **record-keeping** of the documentation produced during the due diligence process;

III Rules on the **actual investigation procedure** itself, including:

- **a.** The experience and training of employees involved in the investigations;
- **b.** Use of additional data to verify the trueness of a hit;[79]
- **c.** The assessment of the outcome of the investigation, i.e., whether the hit is a:
  - I True positive;
  - II False-positive, in which case the investigation is closed; or
  - III Inconclusive, in which case contact should be sought with the competent authority.

IV **Reporting lines** and control mechanisms with different levels of review, including the applicable reporting lines and *four-eyes principle* for final decisions.

78 EBA TFR Sanctions Guideline (2024), par. 36-38.

79 I.e. using further data such as (a) other identification data of persons that was not used at the screening stage, (b) information on the residence of natural persons and information on seat or registered address of legal persons not used at the screening stage, (c) information on nationalities, citizenships of natural persons not used at the screening stage, (d) representative, management and organisational structure of legal persons not used at the screening stage; and (e) contact details not used at the screening stage.

6.2.5 Outcome of the due diligence process: True positive match

When an investigation identifies a true positive match with a person subject to sanctions, the Sanctions Policy must clearly outline the follow-up actions required to ensure compliance with applicable sanctions. These actions include:

1 Immediate rejection or suspension of the person as a customer or of the transaction[80]

The Sanctions Policy should describe procedures for rejecting prospective customers, suspending existing client relationships, or halting specific transactions.[81] Where the financial institution expects that this may happen more than once, pre-drafted communications can facilitate swift action.

2 Immediate (*onverwijld*) freeze of the assets

The Sanctions Policy should define the process to ensure that funds are immediately held in a suspense account and are not made available to the sanctioned person. This should describe: (i) the moment where this obligation arises and desists (i.e., if no message to the contrary is received from the competent authorities after notification), (ii) the manner in which the freeze is executed and the duration thereof and (iii) the applicable reporting lines.[82] Moreover, the Sanctions Policy should describe the process after the freezing of funds, such as a review of past transactions.[83]

3 Reporting to competent authorities within the specified timelines and in accordance with the applicable reporting formats

80 I.e. contrary to the AML/CTF framework, a true positive (ex ante) hit leads to the blocking of a transaction, not the mere reporting of it; EBA TFR Sanctions Guideline (2024), par. 47-49.

81 No existing client relations may be terminated due to a true positive hit, see DNB Guideline (2024), p. 4.

82 Dutch MoF Guidance (2020), p. 11.

83 DNB Guideline (2024), p. 8.

The Sanctions Policy should describe the concrete procedure for notifying a true positive hit. Amongst others, this includes a description of: (i) the data that must be gathered for the reports, (ii) whom these must be submitted to and (iii) the timeline. The AFM and DNB use standardised forms for this purpose, describing the necessary information. In addition to the notification to AFM or DNB, a financial institution must also report a true positive hit to the FIU.[84] Such reports generally require the following information to be included:

- Identity information (of the respective persons involved in the hit);[85]
- Amount of the frozen assets or nature of measures taken;
- Account number;
- Information on the applicable sanction;
- Information of the investigation undertaken and measures applied;
- Nature of the relation; and
- Name and address if the contact person within the financial institution, presumably the Sanctions Officer.

> The average timeline for a notification is as soon as possible, but in no case later than two (2) days after the initial (unverified) hit was detected by the financial institution. This tight window underlines the importance of data quality in the first instance.

6.2.6 Data retention related to sanctions

All data related to accounts and transactions involving true positive hits must be retained for up to five (5) years after the relevant sanction is lifted or the underlying sanction framework is dissolved.[86] This data may be requested by the competent authorities.

84 Pursuant to the Besluit melding transacties financiering terrorisme, (link).

85 As included in art. 33(2) Wwft.

86 Art. 4 Sanctions Act Regulation; DNB Guideline (2024), p. 8; AFM Guideline (2024), p. 53.

6.2.7 Applications for derogations and the lifting of sanctions

Sanctioned individuals may request a derogation and subsequent access to frozen funds. In the Netherlands, it is up to the Minister of Finance to grant such derogations. Upon receiving a derogation request, the financial institution submit a request setting out the relevant information to the Minister of Finance,[87] who will assess it on its individual merits.[88] This process should be described in the Sanctions Policy, including the communication protocol with the sanctioned individual.[89]

Once sanctions are lifted, the frozen funds and suspended relations must/may be reinstated to the relevant persons. While this may seem straightforward, financial institutions must develop a process that deals with the aftermath of lifting sanctions. We imagine that such process describes: (i) the moment from which sanctions are considered lifted, (ii) the verification measures and (iii) the communication towards the respective person(s) and competent authorities.[90]

For institutions with minimal risk of freezing assets, we believe that a high-level description of these processes may suffice.

87 Addressed to: sancties@minfin.nl; or by mail to: Ministerie van Financiën, Directie Financiële Markten, Team Sancties, Postbox 20201, 2500 EE The Hague, the Netherlands.

88 Dutch MoF Guidance, (2020), p. 12; DNB Guideline (2024), p. 7-8.

89 Which communication should at least comprise a description of the sanctioned person's rights in the derogation request procedure.

90 EBA TFR Sanctions Guidelines (2024), par. 53.

6.3 Review of the effectiveness of the Sanctions Policy

The Sanctions Policy must regularly be assessed to ensure its continued adequacy and proportionality. In principle, the process applicable to the reassessment of the Sanctions Policy is not very different from that of the Sanctions Risk Assessment. Relevant review moments are:

I On a **periodic basis**, at least once per year.

II On an **ad hoc** basis, including in situations where:

- **a.** The Sanctions Risk Assessment was adjusted and requires adjustments to the Sanctions Policy;
- **b.** Where shortcomings in the Sanctions Policy were identified;
- **c.** Where substantial changes to the business of the financial institution or the applicable sanctions occur; or
- **d.** Following the reporting of a true positive hit.

As such, the Sanctions Policy should clearly describe the scope and depth of periodic and ad hoc reviews.[91] In our view, the primary responsibility for reviewing the Sanctions Policy should be allocated to the Sanctions Officer.

For smaller financial institutions, or those without prior true positive hits, annual testing of notification processes and systems is recommended to ensure readiness and effectiveness.

91 E.g., comprising the following elements (a) a test the calibration of the screening tool, (b) an assessment of the accuracy of the list management with the use of applicable and up-to-date sanctions, (c) and assessment whether all customers and transactions are being screened when required, (d) an assessment of the adequacy and relevance of the information fields used in the screening system, (e) an evaluation of the timeliness of the automatic suspension customer relations in light of true positive hits and (f) an assessment whether the processes and resources available for the investigation of alerts makes prompt reporting of true positive matches possible; EBA TFR Sanctions Guideline (2024), par. 54-57.

7.
OUTSOURCING AND TRAINING OF EMPLOYEES

7. OUTSOURCING AND TRAINING OF EMPLOYEES

7.1 Outsourcing

The outsourcing of the sanctions screening processes has become increasingly common among financial institutions. If a financial institution decides to outsource (part of) its sanctions screening, the Sanctions Policy must clearly delineate the roles and responsibilities of the institution and the third-party service provider to which the process is outsourced. At a minimum, the Sanctions Policy should:[92]

I Stipulate that the ultimate responsibility for compliance with sanctions, whether or not specific functions are outsourced, remains with the financial institution;

II Ensure that the rights and obligations of the financial institution and of the service provider are clearly allocated and set out in a written contract;

III Affirm that the financial institutions remain accountable for monitoring and overseeing the quality of the screening service provided by the service provider.

The Sanctions Policy must also describe the measures implemented to mitigate the additional risks associated with outsourcing sanctions screening. These risks should be evaluated and addressed within the Sanctions Risk Assessment.

For PSPs and CASPs, specific service agreements must minimize the risk of sanctions breaches. These agreements should: (i) include provisions ensuring service providers maintain up-to-date data on individuals, entities, and organizations subject to sanctions and (ii) be regularly reviewed to assess performance and, where necessary, introduce mitigating measures or amend contractual terms.

92 EBA TFR Sanctions Guidelines (2024), par. 26-30; AFM Guideline (2024), p. 52.

Given the likely involvement of ICT services in outsourced screening processes, the Digital Operational Resilience Act ("**DORA**")[93] provisions on third-party ICT-Services apply. This is relevant even when outsourcing occurs within a group entity. If DORA is not applicable, the standard outsourcing rules, such as those outlined in the EBA guidelines on outsourcing[94], will apply.

7.2 Training of employees

Financial institutions must provide regular training for employees on sanctions and their practical application, including in cases where financial institutions outsource (part of) their sanctions screening. This training is overseen by the Sanctions Officer and must be organised on a regular basis. The objective of the training is to ensure that employees are aware of:[95]

I Applicable sanctions;

II The development of relevant patterns, trends and typologies related to the circumvention of sanctions;

III The outcome of the Sanctions Risk Assessment;

IV The Sanctions Policy and related procedures.

The training process described in the Sanctions Policy must be proportional to the specific roles and experience of the employees. Moreover, the training should be timely and adequate to enable the financial institution to effectively comply with sanctions.

The training plan adopted in line with the Sanctions Policy should also be documented in a manner that permits the financial institution to demonstrate to the competent authorities that their training is adequate and effective.

93 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

94 EBA, Final Report on EBA Guidelines on outsourcing arrangements, (2019).

95 EBA Sanctions Policy Guideline, (2024), par. 31-33.

REGULATORY COUNSEL FINANCIAL SERVICES

Address: A.J. Ernststraat 595-F, 1082 LD Amsterdam, The Netherlands
Website: www.recofise.eu
E-Mail: info@recofise.eu
Tel: +31 (20) 520 68 54