PREPARATION OF RISK ASSESSMENT

for money laundering and terrorist financing

BEST PRACTICE REPORT

2022 | 1. Published April

The Central Bank of Iceland issues *best practice reports* in order to provide guidance to entities under its supervision, by sharing lessons learned from inspections conducted and data collected by the Bank's supervisory personnel.

With the entry into force of the new Act on Measures to Prevent Money Laundering and Terrorist Financing in 2019, a change was made in that obliged entities are now required to adopt risk-based measures to prevent their activities from being misused for the purpose of money laundering and terrorist financing. This entails, among other things, that all obliged entities are now required both to prepare their own risk assessments of their activities and business transactions in order to identify and assess the risk of money laundering and terrorist financing and to carry out regular monitoring of their customers on the basis of these assessments.

The purpose of this best practice report is to communicate the knowledge possessed by the Bank concerning requirements for and best practices in both the preparation of obliged entities' money laundering and terrorist financing (ML/TF) risk assessments and the regular monitoring of their customers. This report explains the requirements entailed in the Act on Measures to Prevent Money Laundering and Terrorist Financing and can therefore be useful to obliged entities' boards of directors, management, supervisory units, and front-line employees.

Issuer:
Central Bank of Iceland, Kalkofnsvegur 1, 101 Reykjavík, tel: +354 569 9600, sedlabanki@sedlabanki.is, www.sedlabanki.is

1. Published April 2022

Table of contents

I Introduction

1.1. With the passage of the Act on Measures to Prevent Money Laundering and Terrorist Financing, no. 140/2018, in 2018, the European Union's fourth anti-money laundering and terrorist financing Directive[1] and selected provisions from the fifth Directive[2] were incorporated into Icelandic law. With the implementation of the directives, a number of priorities were changed in connection with how obliged entities pursuant to Article 2 of Act no. 140/2018 (the Act) should approach their money laundering/terrorist financing (ML/TF) defences. One of the most pronounced changes was the requirement that all obliged entities prepare their own risk assessments of their activities and business transactions so as to assess the risk of money laundering and terrorist financing. Furthermore, obliged entities were required to carry out risk-based supervision of business relationships and occasional transactions on an ongoing basis.

1.2. Following the passage of the Act, the Central Bank's financial supervisors required that obliged entities under the Bank's supervision submit a copy of their risk assessments, pursuant to the authorisation found in Article 5, Paragraph 2 of the Act. The primary purpose of this requirement was to determine whether obliged entities had fulfilled their statutory obligation to prepare risk assessments rather than to examine the contents of the assessments.Í framhaldinu var ákveðið að fara í vettvangsathuganir (þemaathugun) hjá völdum tilkynningar- skyldum aðilum. Í þemaathuguninni var farið efnislega yfir áhættumat á starfsemi aðilanna, áhættumat á samningssamböndum og einstökum viðskiptum (áhættuflokkun viðskiptamanna), framkvæmd áreiðanleikakannana með hliðsjón af áhættumati og reglubundið áhættumiðað eftirlit.

1.3. Thereafter, it was decided to undertake on-site inspections (thematic checks) of selected obliged entities. In the thematic check, Bank staff reviewed the contents of the entities' business-wide risk assessments, their individual risk assessments of business relationships and occasional transactions (customer risk classification), and execution of due diligence checks, with reference to the risk assessments and ongoing risk-based supervision.

1.4. The Central Bank commenced the on-site inspections in question at the beginning of 2020. The reports prepared thereafter were comprehensive and detailed, and they took pains to explain the requirements made of obliged entities in the Act and the regulations adopted on the basis of it. Among other things, the reports outlined the flaws the Bank had identified in obliged entities' business-wide and individual risk assessments, in their methods to control or reduce risks, and in their ongoing monitoring.

1.5. The purpose of the present report is to share the knowledge possessed by the Central Bank with obliged entities, point out instances of good practice among obliged entities, and identify instances

1. Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
2. Directive 2018/843/EU of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849/EU.

where practice could have been improved. Furthermore, this report contains the Central Bank's interpretation of the meaning of certain terms and concepts not defined in the Act. This document wields no regulatory authority in and of itself but represents the Central Bank's attempt to facilitate obliged entities' attempts to handle their defences in a manner consistent with the Bank's expectations. Attempts have been made to avoid explicit statutory citations unless there is particular reason to include them. The discussion in this report is limited primarily to obliged entities' business-wide risk assessments and individual risk assessments.

1.6. It is appropriate to mention that although this report does not directly take account of perspectives and statutory requirements pertaining to personal data protection or other similar requirements, obliged entities are naturally required to consider such perspectives and other applicable statutory requirements.

1.7. This report is not intended to take the place of either the documents and source materials referred to in Article 6 of Regulation no. 545/2019 or other comparable instruments that must be considered during risk assessment preparation. Nor is it intended to take the place of guidelines or instructions from the Ministry of Justice steering group.

1.8. It is the Central Bank's hope that this report can be useful to obliged entities as they refine their practices so as to make their defences against money laundering and terrorist financing more effective.

II The concepts of risk assessment and risk classification

2.1. The term risk assessment is interpreted rather broadly in the Act and the regulations adopted on the basis of it. In the materials issued by the Ministry of Justice steering group on measures to combat money laundering and terrorist financing, *risk assessment* is defined as follows: "A written analysis that reviews all possible risk factors in an obliged entity's activities so as to identify where the key threats and weaknesses relating to money laundering and terrorist financing lie, and to assess where there is the risk that the activities will be misused."[3]

2.2. The Central Bank is of the view that the term *risk assessment* in the sense of the Act and related regulations is three-fold. First, it refers to a *business-wide risk assessment*, which covers risks throughout the obliged entity's activities. Second, it refers to *individual risk assessments*, which cover business relationships and occasional transactions and entail risk classification or customers or of business relationships and occasional transactions. Third, it refers in some instances to both business-wide and individual risk assessments.

2.3. In the Central Bank's opinion, the term *risk classification* in the sense of the Act and related regulations is used to describe two types of risk classification: the classification of risk factors in a business-wide risk assessment and the assignment of risk categories to business relationships and occasional transactions on the basis of an individual risk assessment.

2.4. The Act and related regulations contain examples where the terms *risk assessment, risk classification*, and even *classification* are used more or less interchangeably. Therefore, it could be unclear whether the terms refer to classification of risk factors in a business-wide risk assessment or an individual one. In most cases, the intended meaning is clear from the context in which it is used in the regulatory provision concerned. In instances when the meaning of the term is not as clear, the Bank takes the view that it refers to the risk classification for both business-wide risk assessments and individual risk assessments.

3. Risk assessment, informational material issued by the Ministry of Justice steering group, June 2019.

III Methodology for risk assessment preparation

General

3.1. In preparing risk assessments and organising other anti-money laundering and terrorist financing (AML/CFT) measures, obliged entities must satisfy the requirements laid down in the Act on Measures against Money Laundering and Terrorist Financing, no. 140/2018; the Regulation on Risk Assessments due to Money Laundering and Terrorist Financing, no. 545/2019; and the Regulation on Customer Due Diligence with Respect to Anti-Money Laundering and Terrorist Financing Measures, no. 745/2019. The two regulations are based on the authorisation contained in Act no. 140/2018. In addition, obliged entities must, as applicable, take into account the *EBA Guidelines on money laundering and terrorist financing risk factors*[4] (referred to hereinafter as the *ML/TF Risk Factors Guidelines*), as well as other generally accepted domestic and foreign instruments that provide information and explanations, as appropriate. In the appendix to this report is a list of various instruments and documents the Central Bank takes into account in this context. In spite of the foregoing, all obliged entities are given considerable latitude concerning how they structure their defences; furthermore, the risk assessment must take account of the size, nature, scope, and complexity of the obliged entity's activities.

3.2. Risks in obliged entities' activities are determined by a variety of factors, including risk appetite, type of activities, and geopolitical factors. As a result, each and every obliged entity must prepare a risk assessment based on the risks that it faces. One entity's risk assessment could therefore differ from another's even if their activities are comparable: for instance, if there are significant differences in their customer base, product offerings, or distribution channels. By the same token, these entities' defences could differ as well.

3.3. Each obliged entity must formulate its own methodology for risk assessment preparation. Once it has done this, it prepares a business-wide risk assessment and individual risk assessments on the basis of that methodology. The obliged entity shall then use results of the risk assessments to formulate AML/CFT defences and controls. Obliged entities' risk assessments are therefore a fundamental part of AML/CFT defences, as the defences should be based on the results of the analysis contained in the risk assessments.

3.4. It is important that the methodology underlying the risk assessment be well grounded and supported. If the methodology is flawed or based on inappropriate or irrelevant premises, if it is unclear where and how the data are gathered, or if the approach to the risk assessment is poorly supported, the foundations of the risk assessment will be inadequate and it will be more likely that the assessment will not accurately reflect the existing risk. In such cases, the obliged entity may not maintain satisfactory risk-based supervision of products, services, transactions, and business relationships, and this will exacerbate the risk that the entity's activities will be used for money laundering and terrorist financing.

3.5. Article 5 of the Act (cf. Articles 4-7 of Regulation no. 545/2019) focuses on obliged entities' risk assessments and the methodology underlying them. In the Central Bank's opinion, these provisions

4. EBA Guidelines on money laundering and terrorist financing risk factors, EBA/GL/2021/02.

must be considered during documentation of methodologies for business-wide risk assessments and individual risk assessments, as applicable. The points below follow from these provisions on methodology:

a. *Risk assessments shall be prepared in accordance with accepted methodology and shall contain an analysis and assessment of the risk of money laundering and terrorist financing.*[5]

   The Central Bank interprets "accepted methodology" to mean clear, cogent, systematic, and reasoned methods of assessing risk. The methodology shall be based on relevant data used as a foundation for the analysis of all existing risk factors.

b. *It shall include a rationale for the approach the obliged entity chooses to apply for its risk assessment.*[6] *Because the legislation grants a certain flexibility in risk assessment preparation, the obliged entity must provide support for the approach it has selected. In general, this requirement should be considered satisfied if the methodology is clear, cogent, systematic, and reasoned.*

c. *Before the risk assessment is prepared, the obliged entity shall document the methodology that will be used to prepare it.*[7]

   The Central Bank interprets this provision to mean that the methodology must be able to stand alone as a separate document and is not interwoven into the obliged entity's risk assessment in an undefined and unfocused way. The methodology may be presented in a separate section on the risk assessment, however, or as an introduction to it.

d. *The methodology shall explain clearly how the assessment is carried out, including how risks are identified, where and how data are compiled, how risk classification is carried out, and what criteria are used for risk classification.*[8]

   In order to identify risks in the operations of an obliged entity, the documents listed in Article 6 of Regulation no. 545/2019 and other data that provide indications of risk factors shall be used as a reference.

   The Central Bank considers it important that it be stated how the documents in question will be used. This can be done in various ways; for instance, with footnotes inserted into the risk assessment or in some other clear manner.

   The Bank considers it important that it be stated how classification of risks in business-wide and individual assessments will be carried out, and what criteria are used for the risk categories; i.e., when risk moves from one category to another. Furthermore, the criteria must be defined so as to prevent the risk classification from being overly subjective.

e. *Insofar as is possible, the risk assessment shall be based on comprehensive, relevant data and broad information on known risks and risk factors, including information and data from governmental authorities, financial supervisors, law enforcement bodies, and other entities listed in Article 6 of Regulation no. 545/2019.*[9]

   If the requirements in Item (d) above have been satisfied, the requirements for this item should generally be considered satisfied as well.

   The risk assessment shall cover all possible risks relating to money laundering and terrorist financing.[10]

5. Article 4 of Regulation no. 545/2019 and exposition accompanying Act no. 140/2018.
6. Article 4 of Regulation no. 545/2019.
7. Article 4 of Regulation no. 545/2019. .
8. Article 4 of Regulation no. 545/2019.
9. Article 5, Paragraph 1 of Regulation no. 545/2019; cf. Article 6 of Regulation no. 545/2019.
10. Article 5, Paragraph 1 of Regulation no. 545/2019.

In this context, it is important to formulate the methodology based on all relevant internal and external data and documents; for instance, the EBA's ML/TF Risk Factors Guidelines.

f. The methodology shall be assessed regularly and updated if warranted.[11]
The reasons for an update could involve internal and external factors; for instance, when new products are being put on the market, when new technology is being brought into use (both new and existing products), and when there are changes in risk appetite and the regulatory framework.
Furthermore, the methodology for business-wide and individual risk assessments could change if it is revealed that the current methodology does not detect specific risk factors effectively enough, or if the obliged entity's customer base changes in a manner requiring consideration of new risk factors.

3.6. The Central Bank is of the view that it must be stated explicitly when a methodology is used as a basis for a business-wide risk assessment and when it is used as a basis for individual risk assessments. This can be achieved, for instance, by including in the methodology a separate section on the methodology for individual risk assessments.

Business-wide risk assessment methodology

3.7. In the Central Bank's thematic check, business-wide risk assessment methodologies were examined and a determination made of the extent to which they aligned with the criteria specified in the section above. This examination revealed that obliged entities' methodologies for business-wide risk assessments varied in terms of how well supported they were. In some instances, the methodology in place was very limited, or even virtually non-existent. In these cases, the risk assessments contained only general statements mentioning that certain domestic and foreign documents had been considered, and a review of the risk assessment did not reveal how the documents in question had been used. In order for a risk assessment to achieve its purpose, it is vital that the methodology be clear and well supported. The more detailed and explicit the rationale is, the greater the probability that it will be possible to identify the risk factors actually facing the obliged entity in question and respond to them appropriately.[12]

3.8. In some instances, obliged entities' methodology consisted of a short document with limited contents, yet in the Bank's on-site inspection it was noted that various documents were actually part of the methodology even though the methodology itself did not state this explicitly. In the Bank's opinion, the methodology must be clear and accessible, and it must be obvious upon reading it what is part of the methodology or an appendix to it. If it proves necessary at later stages, after the foundations for the methodology have been laid, to add appendices to it, this should be done in a clear manner. If the methodology needs major revision, however, it is best that this be done in a comprehensive way, and not with appendices and addenda.

3.9. Although the number of risk categories obliged entities defined in their methodologies varied greatly, there were commonly three to five categories. To a degree, obliged entities themselves are in charge of their risk classification methodology and the number of risk categories it contains. On the other hand, it is natural that the more complex an obliged entity's activities are, the broader the methodology and risk assessments must be. In the Bank's view, it is best that the risk classification methodology be as simple as possible while still achieving the set objective.

11. Article 4 of Regulation no. 545/2019. .
12. Articles 1.13-1.17 of the ML/TF Risk Factors Guidelines provide guidance on these points.

3.10. In some instances, risk assessments were not prepared on the basis of the existing methodology. For example, there were cases where classification of risk factors was based on risk categories defined in the methodology, while the risk assessment itself used other categories. Similarly, the risk classification methodology was sometimes opaque, so that it was not clear when a risk factor moved from one risk category to another.

3.11. In many cases, obliged entities' methodologies made little or no mention of how risk factors should be identified, other than to make reference to the National Police risk assessment, the ML/TF Risk Factors Guidelines, and other documents, while the risk assessment itself showed no signs of having actually been based on these documents. Furthermore, few obliged entities had conducted a targeted analysis of their business environment, including customer groups, in order to identify risks in their activities. As a result, the risk factors specified in the risk assessment were often poorly supported or based on weak premises.

3.12. Moreover, in some instances, the methodology was based on premises that should not be considered in preparation of ML/TF risk assessments. In these cases, the methodology was based on so-called operational risk perspectives; i.e., how the obliged entity's activities would be affected if they were used for money laundering or if its customers were involved in financing terrorism. In the Central Bank's assessment, the Act does not assume that such perspectives will be considered in ML/TF risk assessments.[13]

3.13. In some cases, the boundaries between the risk assessment and the methodology were very unclear, making it difficult to determine which document should play which role. For instance, in some cases, the risk factors themselves were specified in the methodology or other related documents (such as rules of procedure) and not in the risk assessment itself. Such a structure is likely to cause misunderstandings, both for the entities themselves and for supervisory bodies, and it is not conducive to achieving the set objective.

Individual risk assessment methodology

3.14. In the thematic check, the Central Bank examined methodologies for individual risk assessments; i.e. assessments of risk associated with business relationships and occasional transactions. This examination revealed that obliged entities' methodologies for individual risk assessments varied in terms of how well supported they were.

3.15. There was some variation in how obliged entities set up their methodologies for individual risk assessments. In the most effective presentations, the methodology for individual risk assessments was discussed separately instead of being included as an undefined part of the methodology for business-wide risk assessment. In some instances, individual risk assessments were not based on the obliged entity's existing business-wide risk assessment.

3.16. In order for ongoing monitoring to deliver targeted results, the methodology for individual risk assessments must be carefully prepared. In the documented methodology, the obliged entity must formulate its responses to all of the risk factors specified in Article 5 of Regulation no. 745/2019, as well as other risks that may exist. For instance, the methodology must specify, among other things, how reputational risk and risk associated with political exposure are identified.[14] In addition, the methodology must state how heavily each risk factor weighs in customer risk classification.[15]

13. Although the said perspectives do not apply to the methodology under consideration here, they do apply in other respects; cf., for instance, Item 143 in EBA/GL/2021/05.

14 For instance, the methodology could specify that an analysis of reputational risk should take into account media coverage, court judgments, charges filed for certain criminal violations, etc.

15. Articles 3.2-3.7 of the EBA's ML/TF Risk Factors Guidelines contain a more detailed list of points to consider in determining the weight of risk factors.

3.17. Furthermore, it is important that the methodology for individual risk assessments be formulated without consideration of external factors such as the number of employees tasked with conducting ongoing monitoring. In practice, it appears to the Central Bank that some obliged entities limit documented risk so as to ensure that monitoring it will be "manageable." In the Bank's opinion, such an approach is not conducive to achieving the set objective. The aim of those who prepare individual risk assessments must always be to identify existing risk. If it is revealed that risk is more extensive than the obliged entity's current system of defences can handle, the board and senior management must take appropriate action.

Good practice in formulating risk assessment methodology:

- A well-grounded, documented methodology that satisfies the requirements laid down in Article 4 and Article 7, Paragraph 1 of Regulation no. 545/2019 must be in place.
- The requirements in the Act and in Regulations no. 545/2019 and 745/2019 must be reviewed systematically.
- Consideration must be given to the documents and information specified in Article 6 of Regulation no. 545/2019 and, as applicable, other relevant sources, and it must be specified how the said documents/information are used in formulating the methodology and, as applicable, preparing the risk assessment.
- Individual risk assessments shall be based on Article 5 of Regulation no. 745/2019.
- Consideration must be given to which preparatory documents are needed for the risk assessment, such as an internal analysis of customer groups based on their activities.
- The methodology shall be based solely on premises relevant to the risk of money laundering and terrorist financing and not on operational considerations or other premises.
- There must be clear boundaries between the methodology and the risk assessment.
- It must be clear which methodology applies to business-wide risk assessments and which applies to individual risk assessments.

IV Risk assessment

General

4.1. In the thematic check, the Central Bank examined whether obliged entities' risk assessments and other measures were conducive to identifying risks facing the entities in question and building up systematic defences against money laundering and terrorist financing. In the Bank's opinion, both business-wide and individual risk assessments were inadequate in many cases. To an extent, these inadequacies can be attributed to the fact that the process is a new one.

4.2. In most instances, business-wide risk assessments were in place, while in many cases individual risk assessments were flawed. In other instances, individual risk assessments were in place, while business-wide risk assessments were very limited or even non-existent.

Business-wide risk assessment

General

4.3. The term *business-wide risk assessment* applies to an assessment of risks affecting most or all of an entity's operations. In the EBA's ML/TF Risk Factors Guidelines, a business-wide risk assessment is defined as an assessment of the ML/TF risk to which supervised entities are exposed, with consideration given to the nature and complexity of their activities.

4.4. Obliged entities' business-wide risk assessments are discussed in Article 5 of the Act and in Regulation no. 545/2019. To put it briefly, it can be said that the risk assessment should identify the risks (risk factors) associated with obliged entities' activities, without taking into consideration any controls or other methods used to reduce risk (referred to hereinafter as mitigating measures). This risk is referred to as inherent risk. The risk assessment shall then specify the ways in which mitigating measures are used to reduce inherent risk. When the mitigating measures have been assessed, the next task is to identify the risk that remains. This is usually referred to as residual risk. If the risk assessment is well prepared, the obliged entity will have a cogent description of where ML/TF risk is most pronounced in its activities, and it can therefore focus its ongoing monitoring more effectively on the most prominent risk factors.

4.5. Obliged entities set up their risk assessments using a wide variety of approaches. Some based their assessment on a numerical presentation of inherent risk, mitigating measures, and residual risk. In the Central Bank's opinion, such numerical analyses were generally quite clear and accessible, and they captured risks effectively. On the other hand, the Bank found that the rationale for these numerical analyses was often lacking. Others approached the risk assessment in a more subjective manner, and in those cases, the Bank often found it difficult to identify the premises upon which the risk assessment results were based.

Written comprehensive risk assessment

4.6. As is stated in Article 2 of Regulation no. 545/2019, obliged entities shall prepare a "written comprehensive risk assessment of their activities and business transactions." The question of exactly what these two terms – *written* and *comprehensive* – meant came up repeatedly during the thematic check.

4.7. In the Bank's opinion, the term "written risk assessment" means that obliged entities must have their risk assessment in written form. This does not imply a prohibition on presenting information in numerical form to some extent in order to identify and assess risk, but in the main, the assessment shall be written. Therefore, the Bank has not found fault with risk assessments presented in formats intended for numerical approaches – such as Excel documents or other spreadsheets – provided that they were presented in writing.[16] However, the Bank was of the view that in some instances, the risk assessments presented in spreadsheet form resembled preparatory documents in the sense of Article 11 of Regulation no. 545/2019 rather than comprehensive written risk assessments. On the other hand, the Bank was of the opinion that the documents in question were extremely good preparatory documents for the risk assessment.

4.8. As regards a "comprehensive risk assessment," the Central Bank considers that term to entail the following, at a minimum:

a. The risk assessment is a discrete unit, either a single document or a document with clearly defined appendices.

b. The risk assessment takes into consideration all risk factors facing the obliged entity in question, and each and every risk factor is assessed in terms of inherent and residual risk.

c. The measures used to mitigate the risk factors in question are specified in the risk assessment, and a reasoned assessment has been made of their efficacy.

d. The risk assessment gives an in-depth view of the risk associated with the risk factors listed in Article 5 of the Act, as well as other existing risk factors; i.e., what the obliged entity's inherent and residual risks are in connection with: i) customers; ii) trading partner countries and regions; iii) products; iv) services; v) business transactions;[17] vi) distribution channels; and vii) technology. However, in those instances when some of the above-mentioned risk factors have been assessed together because of the nature of the obliged entity's operations and business transactions, it should be sufficient to make a comprehensive assessment of that risk factor based on those premises.

Risk factors

4.9. Article 5, Paragraph 1 of the Act and Article 5 of Regulation no. 545/2019 state that obliged entities must prepare a risk assessment of their operations and business transactions. The assessment must contain the following:

a. A written analysis and assessment of the risk of money laundering and terrorist financing, which shall, among other things, take into account risk factors associated with customers, business partner countries or regions, products, services, transactions, technology, and distribution channels.

b. In preparing the risk assessment, obliged entities must use the National Commissioner of the Icelandic Police's risk assessment as a reference.

c. The risk assessment shall take into account the size, nature, scope, and complexity of the obliged entity's activities.

d. The assessment shall also cover all aspects of the obliged entity's operations, it shall be based on comprehensive, satisfactory, and relevant data and information, and it shall cover all possible ML/TF risk factors.

e. The term "risk factor" is not defined in either the Act or Regulation no. 545/2019. In the EBA's ML/TF Risk Factors Guidelines,[18] it is defined as follows: "Risk factors" means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction. In the materials issued by the Ministry of Justice steering group on measures to combat money laundering and terrorist financing, risk factor is defined as follows:

16. Article 8, Paragraph 2 of Directive 2015/849 states that the risk assessment shall be "documented." It can therefore be said that Icelandic law goes further than the Directive in specifying that the risk assessment must be written.

17. In this context, the term transactions refers to individual transactions.

18. See page 17 of the ML/TF Risk Factors Guidelines.

"The term risk factors refers to the aspects of the supervised entity's activities that could be exposed to money laundering or terrorist financing."[19]

4.10. Most obliged entities divided their risk assessments into several sections focusing on risk factors relating to: (1) customers; (2) trading partner countries and regions; (3) products, services, and transactions; (4) technology; and (5) distribution channels, as is specified in Article 5 of the Act. Some obliged entities combined several of the above factors into a single risk factor; i.e., customers and products. These efforts produced varying results, but in the Bank's opinion, the outcome was best when each risk factor was covered in a separate section.

4.11. It is the task of each obliged entity to identify and assess the risk factors falling under each category. Similarly, it is assumed that the categories listed in Article 5 of the Act are minimum risk factors and that others should be identified and assessed if circumstances warrant it. Here, as elsewhere, it is important that the analysis and rationale be presented clearly. Once this work is complete, it should be established whether the risk factor in question is present and what the inherent risk is in the activities of the obliged entity in question.

4.12. Actually, few entities utilised the available reference documents, such as the EBA's ML/TF Risk Factors Guidelines and materials from the Central Bank (and Financial Supervisory Authority) to analyse risk factors in their operations, even though these documents contain cogent guidance on known risk factors in obliged entities' activities. Instead, most obliged entities either relied on their employees' experience in assessing which risk factors existed or used other opaque or unfocused methods. In those cases where available sources were used, however, the analysis of the risk factors identified was sometimes insufficiently based on the obliged entity's actual activities.

4.13. In the Central Bank's opinion, it is best that obliged entities consider all relevant sources when analysing the risk factors that apply to their activities. The risk factors that are specified in the sources then need to be mapped onto the activities of the obliged entity in question in order to determine whether they apply or not. If the risk factor exists, the obliged entity's inherent risk must then be determined, as is discussed more fully in the section below.

Inherent risk

4.14. As is noted above, inherent risk is the risk that exists in the obliged entity's activities before account is given to mitigating measures designed to reduce that risk. When risk factors have been identified, the obliged entity must assess how much inherent risk is entailed in the risk factor in question. This assessment should be made using methods described in the obliged entity's methodology.

4.15. But how shall the entity determine whether the risk level is high, medium, or low? In this context, consideration must be given to various documents and information listed in Article 6 of Regulation no. 545/2019, including the National Police risk assessment, foreign guidance documents, and internal analyses. Furthermore, there must be grounds for the identification of inherent risk. In the Central Bank's view, it is not sufficient merely to refer to employee experience as a rationale for this assessment.

4.16. In this context, some obliged entities misunderstood at times how to use the information and documents to prepare their risk assessments. For example, some of them assumed that because the National Police risk assessment indicated limited risk in Iceland, this automatically meant that all obliged entities' activities were low-risk as well. The Central Bank wishes to point out that the conclusions drawn by the National Police are based on a comprehensive assessment of the ML/TF

19. See page 3 of Risk Assessment, informational material issued by the Ministry of Justice steering group, June 2019.

risk that is considered to exist based on market conditions in Iceland. Even if the risk assessment for Iceland suggests limited risk associated with, for instance, sales of ships, this does not necessarily mean that individual obliged entities' risk is limited if ship vendors are prominent among their customers.

4.17. In assessing inherent risk, it is necessary to consider the nature and scope of the risk factor and the probability of ML/TF activity in connection with it. For example, certain products could be of such a nature that a certain type of abuse is likely – i.e., through a large number of small transactions (probability) – while on the other hand, few customers use the product in question (scope). By the same token, there may be a strong probability of money laundering in connection with transactions with certain countries or jurisdictions, yet the scope of business relationships associated with such jurisdictions may be very limited. The analysis of nature, scope and probability was very frequently not heeded in obliged entities' risk assessments.

4.18. In essence, obliged entities used two methods to assess inherent risk. The first method relied on a numerical scale, so that a risk score of less than 30 points was classified as low risk, a score of 31-70 indicated medium risk, and a score above 70 indicated high risk. When such a method is used, there must be a well-grounded methodology detailing how the point system is structured. A colour-coding system was often used to distinguish between risk levels, with green indicating low risk, yellow indicating medium risk, and red indicating high risk. In some instances, a subjective measure of risk was used, although it may have been based on certain objective criteria; for instance, notifications filed with the Financial Intelligence Unit in recent years.

The assessment of inherent risk was most transparent when:

- A well-grounded numerical risk metric was used.
- An assessment was made of the nature, scope, and probability for each risk factor.
- A clear, reasoned, objective assessment was made of inherent risk.

Policies, controls, and procedures and other methods of reducing risk

General

4.19. Article 5, Paragraph 4 of the Act stipulates that obliged entities shall have documented policies, controls, and procedures to mitigate and manage the risks associated with money laundering and terrorist financing. As is noted above, the present report includes a discussion of such mitigating measures.

4.20. Even though the Act provides for policies, controls, and procedures to mitigate risk, these terms are actually intended to capture all measures that reduce risk, no matter what the obliged entity concerned may call them.

4.21. On the whole, most entities had mitigating measures in place, but the measures were often insufficiently clear and detailed or were inadequately followed up in practice.

Policies

4.22. Obliged entities are required to formulate policies for defences against money laundering and terrorist financing. In general, it is the board of directors' role to formulate policy, but according to Article 5, Paragraph 6, cf. Article 3, Item 19 of the Act, it is sufficient if parties other than the board set policies for ML/TF defences. In accordance with the above, there were instances where the policy in question had been approved not by the board but by the responsible person (often

referred to as money laundering reporting officer (MLRO)).[20] Notwithstanding the above-cited statutory provision, the Central Bank considers it preferable that the obliged entity's policy be approved by its board of directors.

4.23. It is preferable that the obliged entity's policy present a broad outline of the entity's position on ML/TF defences. In this sense, the policy lays the foundation for the company culture that the board expects the entity to have in place in its activities. It is also preferable that the policy specify which activities and customer conduct fall outside the obliged entity's risk appetite.[21]

4.24. Furthermore, it is best that the policy be structured in a conventional way, although no explicit requirements are made concerning the contents of the policy in either the Act or the associated regulations, apart from those laid down in Article 5, Paragraphs 4 and 5 of the Act, which state as follows:

a. Obliged entities shall have documented policies, controls, and procedures to mitigate and manage the risks associated with money laundering and terrorist financing.

b. Policies, controls, and procedures shall include the following, at a minimum:

1. provisions on the development and updating of policies, controls, and procedures, including risk mitigation methods, due diligence checks, notifications of suspicious transactions, internal controls, and the designation of a money laundering reporting officer, with consideration given to the size and nature of the company, and checks on employee eligibility; and

2. as applicable, and with consideration given to the size and nature of the activities, the requirement that an independent auditing department or independent appraiser be tasked with appraising and testing policies, controls, and procedures.

4.25. It can be seen from the foregoing that no clear distinction is made concerning what falls under policies, what falls under controls, and what falls under procedures. In the Central Bank's assessment, it is necessary to have general and specific information available for reference as regards what should fall under the company's policies in individual cases; cf., among other things, the EBA Guidelines on internal governance.[22]

4.26. The policy contains documented instructions from the board to the managers and employees who carry out day-to-day activities. It is a separate document approved by the board, and it lays down objectives and purposes, roles and responsibilities, and monitoring and auditing, among other things. Rules, controls, and procedures are based on the contents of the policy; therefore, it is important that the presentation be clear and designed to ensure that management and employees understand and become familiar with the contents. In the case of some entities included in the Central Bank's thematic check, the policy did not exist as a separate document; instead, it was specified in internal rules or elsewhere, sometimes in a disjointed manner, what the entity's policy was.

Controls and procedures

4.27. Where the policy leaves off, controls and procedures take over as regards measures to mitigate inherent risk. Mitigating measures were called by various names in obliged entities' procedures, but it is most important that such mitigating measures be effective, explicit, and conducive to achieving the set objective.

20. Article 3, Item 19 of Act no. 140/2018 defines a senior manager as follows: "A person with satisfactory knowledge of an obliged entity's risks regarding money laundering and terrorist financing who is of sufficiently high standing to take decisions regarding such risk. The person in question need not in all cases be a member of the board of the obliged entity."

21. See, for instance, Article 4.7, Item (g) in the ML/TF Risk Factors Guidelines.

22. EBA Guidelines on internal governance, EBA/GL/2021/05.

4.28. In general, the following should be borne in mind in connection with formulation of procedures:

a. Procedures serve as a further orchestration of the provisions laid down in the policy.
b. Procedures are prepared by management and employees who carry out day-to-day activities.
c. Procedures must specify who is responsible for ensuring that they are followed and updated.

4.29. The Central Bank's thematic check revealed significant weaknesses in four aspects of obliged entities' mitigating measures:

a. In many cases, it was unclear which mitigating measures were in place to address specified risk factors. In order for mitigating measures to achieve the set objective in an effective and transparent way, the risk assessment must specify which mitigating measures apply to which risk factors.

b. Reasoned assessments of the mitigating measures, which should reveal how effectively the measures would have mitigated inherent risk, were severely lacking. In this area, it was relatively common that obliged entities made only a subjective, unsupported assessment of the measures. The Bank is of the view that this approach often caused the entities in question to over- or underestimate the efficacy of their mitigating measures.

c. Furthermore, it was common that the risk assessment did not specify the frequency with which individual risk factors should be monitored.[23]

d. Finally, the procedures were sometimes lacking in content, clarity, or focus, or they were not followed up in practice.

In the Central Bank's assessment, the following are the mitigating measures most frequently used by obliged entities:

- Due diligence checks and enhanced due diligence checks.
- Internal procedures, controls, and rules.
- Systems that flag unusual transactions as defined using predetermined, well-grounded criteria.
- Screening for political exposure.
- Screening against targeted sanctions lists.
- Updates of information on customers.

Residual risk

4.30. When risk factors have been identified, inherent risk assessed, and mitigating measures specified and assessed, it should be relatively simple, all else being equal, to identify residual risk. If inherent risk and efficacy of mitigating measures are scored on a numerical scale, the residual risk associated with a given risk factor can be calculated quickly: for example, if the inherent risk score is 80 (high risk) and the mitigating measures receive a score of 30, the residual risk score is 50. If risk classification has been defined in the methodology, so that a score of 0-30 points indicates low risk, 31-70 indicates medium risk, and 71-100 is high risk, then, in the example above, the mitigating measures have "converted" a high level of inherent risk into a medium level of residual risk. If no numerical measures of risk and mitigating measures have been defined, it can be more difficult to determine the level of residual risk, which will then require clearer and more detailed reasoning.

4.31. Obliged entities varied greatly in how effectively they determined residual risk levels. In some cases, entities considered their residual risk to be the same as their inherent risk even though they considered their mitigating measures sound and effective. In such instances, it was often unclear whether the mitigating measures would have affected the risk, as the risk assessment contained no evaluation of their efficacy. Here, as elsewhere, it is most important that the methodology be clear and that it be adhered to when the risk assessment is carried out.

23. This applies, for instance, to how often customers' political exposure is checked; i.e., whether it is done daily, weekly, monthly, etc.

Residual risk – good practice:

- The risk assessment identifies residual risk for each risk factor.
- The risk assessment provides rationale for the determination of residual risk.
- The rationale for residual risk was clearest in cases where numerical scores were used for risk and mitigating measures.

Residual risk – unsatisfactory practice:

- Subjective assessment of residual risk.
- Residual risk is the same for risk factors bearing different levels of inherent risk, even in the presence of comparable mitigating measures.

Update of business-wide risk assessment

4.32. Article 5, Paragraph 2 of the Act states that the risk assessment shall be updated every two years, or more often if warranted. Furthermore, a risk assessment shall always be carried out before new products or services are put on the market, and when new distribution channels or new technologies are brought into use.

4.33. As is noted above, risk assessment preparation is a relatively new approach to ML/TF defences, and it is natural that it should take time for obliged entities to adapt to the practice. While they are adjusting to the risk assessment requirement, it is certainly appropriate for obliged entities to update their risk assessment well within the maximum timeframe provided for by law.

4.34. The Bank's thematic check revealed that only in a very few cases had the time come for an update to meet the statutory deadline. In many instances, however, obliged entities had not updated their risk assessments even though there was every reason to do so; i.e., they had made changes to the approach/practices in their activities or had put new products on the market. In a few cases, entities had not updated their risk assessments even though new regulations (such as Regulations no. 545/2019 and 745/2019) had taken effect, which must surely be considered good reason in the sense of Article 5, Paragraph 2 of the Act.

4.35. In the Central Bank's view, it would be sensible for obliged entities to include in their methodology a list of occasions or events that should prompt an update of the risk assessment; furthermore, it could be useful to specify in the risk assessment itself when it is appropriate to begin an update in order to meet the deadline provided for in the Act or in internal rules.

Individual risk assessments

General

4.36. In order for obliged entities to be able to satisfy the requirement that they conduct risk-based supervision of business relationships and occasional transactions, as is provided for in the final sentence of Article 5, Paragraph 1 of the Act, individual risk assessments must naturally be in place. It follows from the EBA's ML/TF Risk Factors Guidelines that individual risk assessment refers to *an assessment of the ML/TF risks to which obliged entities are exposed as a result of business relationships or occasional transactions*.[24]

4.37. An important factor in systematic risk-based ML/TF defences is the assessment of which customers are considered higher-risk and which are lower-risk. In order to make such an assessment possible, customer due diligence checks are carried out, and this information is then used to assign customers to risk categories in accordance with the methodology in place. In day-to-day speech, this assessment is often called *customer risk classification*, even though it refers to the risk classification of all

24. See Item 1.21 of the ML/TF Risk Factors Guidelines.

business relationships and occasional transactions. Such risk classification does not entail a judgment of the customer's character, as the customer may simply be engaged in activities generally associated with a high level of ML/TF risk, do business in jurisdictions generally considered high-risk, or be classified as a politically exposed person.

On the other hand, a higher customer risk classification brings with it certain obligations, including enhanced due diligence and enhanced ongoing monitoring.

4.38. Individual risk assessments must take the business-wide risk assessment into account. This means that the obliged entity's business-wide risk assessment should affect individual risk assessments and customer risk classification.

4.39. There seems to be an overriding reluctance to inconvenience customers by requesting increased information disclosures from them. As a result, obliged entities tend to proceed very cautiously in classifying customers as high-risk even when there appears to be every reason to do so. In the Central Bank's opinion, this perspective is dangerous, in addition to being based on the misconception that the risk classification implies an indictment of the customer's character.

Risk factors

4.40. Article 5 of the Act specifies that account must be taken of risk factors relating to customers, trading partner countries or regions, products, services, business transactions, technology, and distribution channels. Article 5 of Regulation no. 745/2019 specifies that account shall be given to the following factors, among others, in connection with customer risk classification:

a. the activities,[25] reputation,[26] and political connections of the customer and the beneficial owner;
   - *Examples of activities generally considered risky include gambling, contracting, pharmaceuticals manufacturing, and trade in weapons.*
   - *As regards reputational risk, consideration must also be given to media coverage, information possessed by the obliged entity, court judgments, etc.*

b. which countries or regions are related to the business relationship;
   - *The home country of the customer, the home country or domicile of the beneficial owner, jurisdictions with which the above parties are connected, the place where the business activities take place, the customer's market areas, etc.*
   - *In this context, it is not sufficient solely to consider high-risk and uncooperative countries according to Article 6 of the Act; consideration must also be given to other metrics, such as the BASEL AML Index, the Corruption Index, etc.*

c. risk factors associated with the product, service, or transaction[27] being sought out;
   - *In this case, consideration must be given to the risk assessment for the said products, services, and transactions in the obliged entity's activities.*

d. which distribution channels are used;
   - *Do the transactions take place at the obliged entity's place of business, in electronic form, through a third party, etc.?*

e. whether the customer uses intermediaries as representatives;

f. whether the customer is a legal entity with a complex ownership or management structure;
   - *Is there a long or complex chain of ownership behind the customer? What is the purpose of this ownership chain, etc.? [I assume this refers to a chain of ownership, not a chain of assets.]*

25. Articles 2.3-2.4 of the EBA's ML/TF Risk Factors Guidelines contain a more detailed list of business-wide risk factors.
26. Article 2.5 of the EBA's ML/TF Risk Factors Guidelines contains a more detailed list of risk factors pertaining to reputational risk.
27. Articles 2.16-2.18 of the EBA's ML/TF Risk Factors Guidelines contains a more detailed list of risk factors relating to products, services, and business transactions.

g. whether the customer is a trust or comparable entity; and
h. whether the customer mainly conducts cash transactions.

4.41. When preparing individual risk assessments, it is important to consider all of the above-listed points, as well as the obliged entity's business-wide risk assessment. It should also be noted that the points above represent the minimum and that other factors must also be considered, as applicable based on the assessment and experience of the obliged entity in question. As such, there may be factors identified in the business-wide risk assessment that are considered high-risk, and if so, the obliged entity must respond to them in its individual risk assessments.

4.42. Various methods for customer risk classification

4.43. No explicit formal requirements are made in the Act or associated regulations concerning how risk classification should be handled. The Act and Regulation no. 745/2019 do state, however, that there must be at least two risk categories. In the Central Bank's opinion, customer risk classification was most effective when three or four risk categories were specified.

4.44. Obliged entities structured their risk classification systems using a wide variety of approaches. In some instances, all parties started out in the lowest risk category, but in the presence of specific risk factors they would move up by one or more categories.

4.45. In some cases, obliged entities had assigned their customers to differing risk categories depending on risk factor; i.e., the same customer could be classified as highly risky in connection with one product but low-risk in connection with another, and so forth. In the Bank's view, such risk classification is inconsistent with the objectives laid down in the Act. Instead, obliged entities must prepare a comprehensive assessment of the risks associated with the customer on the basis of all risk factors.

4.46. In some instances, customer risk classification was based on third-party software systems. In these cases, the obliged entity must have a thorough understanding of how the system works and must ensure that the system assesses the risk factors used for customer risk classification, in accordance with the obliged entity's business-wide risk assessment.

4.47. In the Central Bank's opinion, the most effective customer risk classifications were those in which specific risk factors – particularly those listed in Article 5 of Regulation no. 745/2019 and in the obliged entity's business-wide risk assessment – were scored according to a points-based system and each customer was assigned a risk category based on its total score. In this context, however, it must be borne in mind that risk factors can carry different weights, and if a customer is considered high-risk based on two or more factors – geographical region and business activities, for instance – it could be that overall risk does not merely double but increases many times over. For example, a customer from a high-risk jurisdiction who is also a politically exposed person is many times riskier than one who is from a high-risk jurisdiction but has no political exposure.

Transferring customers between risk categories

4.48. When a new customer starts a business relationship with an obliged entity, the entity must assess the risk associated with that customer and assign the customer to the appropriate risk category so that it can carry out satisfactory customer due diligence and ongoing monitoring. On the other hand, if there are changes in the customer's conduct, organisational structure, or other factors, the original risk classification may no longer be accurate. For instance, a customer who carried out very little cash-based business at the beginning of the business relationship could find that business premises have changed and cash business has increased, or a customer may end up conducting frequent business with counterparties in high-risk jurisdictions even though such a business pattern did not exist at the

beginning of the business relationship, and so forth. Similarly, it is not a given that the information provided by a customer at the outset gives realistic or accurate portrayal of that customer. Obliged entities must respond to such changes in premises. In this context, the interplay between ongoing monitoring and the individual risk assessment is put to the test, as has been discussed previously.

Unsatisfactory practice:

- Only some of the defined risk categories have been used.
- All or nearly all customers are in the same risk category.

V Ongoing monitoring

General

5.1. Ongoing monitoring actually refers to all monitoring of AML/CFT measures. In order to achieve the set objective, ongoing monitoring must be risk-sensitive, and based on risks associated with money laundering and terrorist financing. This entails, among other things, that customer risk classification must be conducive to capturing risky business relationships and occasional transactions, and that higher-risk customers must be monitored both more frequently and more thoroughly than lower-risk customers.

5.2. Even though the discussion below focuses on transaction monitoring systems and updates of information, it can also be used as a reference when such systems are not in place. If systems are not used to analyse customers' behaviour – for instance, in cases involving smaller obliged entities – it is possible to analyse such behaviour manually. In those instances, the entity must have in place well-grounded procedures that are designed to identify deviations and suspicious transactions, among other things.

Transaction monitoring systems

General

5.3. In order for monitoring to deliver the intended results, it may be necessary to use a special transaction monitoring system; however, in some cases manual monitoring will suffice. The more complex and broad-based the obliged entity's operations are, the greater the need for an transaction monitoring system to support monitoring. But it is not enough merely to have such a system in place; it must be configured so as to capture the conduct it is intended to capture. Such configuration is painstaking work that to some extent is continuously evolving. Furthermore, subjective assessments always play some role in monitoring.

5.4. Most of the entities included in the thematic check had some sort of electronic transaction monitoring system in place to identify unusual and suspicious transactions or unusual conduct. These systems varied in terms of how effective they were for the monitoring in question, and some of them were actually designed for purposes other than ML/TF monitoring.

5.5. In general, such systems "flag" potentially unusual or suspicious transactions or conduct. If the monitoring system flags a transaction, the obliged entity must examine the flag, determine whether the conduct in question should be investigated further, and decide whether the flag in question represents what is called a "true hit."

5.6. Most systems were set up so that the entity itself had to specify the criteria to be monitored; however, the criteria themselves were often derived from core data furnished by the service provider. Minor modifications to the systems' furnished criteria – for instance, reference amounts or thresholds – could cause the number of flags to surge or plummet. In view of this, it is crucial that the underlying rules and criteria on which the systems rely be designed to capture unusual or suspicious transactions or conduct. If the systems issue too many flags, the result could be that investigations of flags will be cursory or perhaps not carried out at all. On the other hand, if the systems issue too few flags, all sorts of unusual or suspicious transactions or conduct could be overlooked and not investigated as they should be.

5.7. In the random samples examined by the Bank, the number of flags issued differed greatly from one obliged entity to another. For some entities, there were large numbers of flags, while for others there were few, if any. In the case of most entities, the Bank pointed out specific transactions that were not flagged – such as large amounts of money that were inconsistent with the customer's other transactions; transactions by a private limited company owned by a party from a high-risk jurisdiction; transactions involving cash deposited to the customer's account and then transferred directly to the beneficial owner; and so forth.

5.8. If risk assessments and customer risk classification have been prepared in a systematic way, they should give a clear view of where the key risks facing the obliged entity lie. Therefore, rules governing the transaction monitoring system should be designed on the basis of the business-wide and individual risk assessments; yet in practice, the obliged entity's risk assessments often appear to have limited bearing on system rules and criteria.

5.9. In order for ongoing monitoring to achieve the intended objectives, the rules and criteria for the transaction monitoring system must be adapted to the various customer risk categories. As such, higher-risk customers and transactions must be monitored more closely than those carrying lower risk. This can be done, for instance, by setting different amount thresholds for different risk categories, or by setting additional rules for higher-risk customers. In most cases, however, there was little or no difference in ongoing monitoring of the various customer risk categories.

Flagging and investigating unusual or suspicious transactions or conduct

5.10. The determination of what should be considered unusual or suspicious transactions or conduct should be based on general and specific perspectives concerning the conduct of the customer in question and on the obliged entity's information about that customer. This includes information disclosed by the customer during the due diligence process – turnover, source of funds, etc, – and the obliged entity's acquired experience concerning the customer's typical conduct, as well as the conduct of other customers engaged in comparable activities.

5.11. In general, a large share of flags are false positives, but experts in flag review are usually quick to identify them as such. In this context, it should be noted that there are reasonable explanations for most flags, but assessing this will often require explanations from the customer relations manager or, as applicable, from the customer in question. As regards flags requiring more thorough investigation, there were great differences in the amount of work invested in such investigations, whether an explanation of the conduct was requested, etc. In the Central Bank's opinion, there appears to be a certain reluctance to request explanations for transactions, but it must be deemed preferable that obliged entities work systematically towards changing this culture.

5.12. In general, 1-3 staff members were tasked with investigating flagged transactions. In order to reduce the volume of work involved, some obliged entities configured their systems to align the number of flags with the number of available staff members. In the Bank's view, such an approach is highly dubious. Obliged entities must align their staffing with the number of flags or, if this is not possible, set up their defences differently.

5.13. Once investigation of flags was complete, the quality of the explanations for the flags varied significantly. In some instances, flags had been marked resolved without any investigation at all. In the Bank's opinion, it is best if rules of procedure specify clearly the circumstances under which flags should be investigated, how the investigation should be handled, and how they should be resolved and the case closed. Such work habits facilitate all traceability in the case of investigations by the Financial Intelligence Unit and supervisory bodies.

5.14. Obliged entities' response time to flags varied significantly. In the Central Bank's opinion, it is important that flag review be risk-based; i.e., that reviews take into account, among other things, the risk category of the customers concerned. Investigation of flags shall commence as soon as possible – preferably on the same day or within a few days after the flag comes up, in the highest-risk cases.

5.15. In some cases, it was not possible to look flags up by national ID number, whether they were resolved or not. Furthermore, in a few instances there were technological glitches that made it difficult to examine resolved flags. The Central Bank is of the view that it can be important to examine older flags when investigating new cases, and furthermore, supervisory bodies and the Financial Intelligence Unit need to have easy access to such data.

Monitoring of information

5.16. As is provided for in the Act, information that obliged entities possess concerning their customers must be updated on a regular basis. Such updates must take place in a predefined and risk-based way, in accordance with the methodology in place. This statutory requirement is generally satisfied by updating customer information in a regular and risk-sensitive manner, so that the highest-risk customers are subject to more frequent due diligence updates than those who represent lower risk. In the Central Bank's opinion, however, such updates only satisfy minimum statutory requirements. In addition to these, obliged entities must have some sort of system or procedure that prescribes the action to be taken if predefined changes in risk factors should take place.[28] For example, media coverage or a court judgment could shed new light on a customer's reputation, or changes could take place in the customer's board, management, ownership structure, etc., which could affect the risk associated with the customer.

5.17. In the Bank's assessment, each and every obliged entity is responsible for keeping abreast of or having access to the best possible information about its customers. On the other hand, whether the entity should purchase access to a data utility or can maintain its access to information in another way depends on the entity's activities and scope of operations. In any event, obliged entities must have a clear, cogent plan outlining how they fulfil their obligation to know their customers, and their internal rules must specify who is responsible for enforcing it.

5.18. As is mentioned above, obliged entities varied greatly in how well set up they were to reassess their customers' risk category. In some instances, entities relied entirely on the most recent due diligence checks and had no systematic methods of detecting changes in the customer's circumstances. In these cases, it was sometimes said that the customer bore responsibility for notifying the entity of such changes, but in the Central Bank's view, this does not suffice. In other cases, it was assumed that the obliged entity's system would "learn" the customer's behaviour pattern and then flag activity that deviated from that pattern. Then, if the deviation warranted a change in the customer's risk classification, such a change would be made.

5.19. Many entities had contracted with data vendors to receive new information on their customers (from media monitoring companies or enterprise registers). Furthermore, in some instances, front-line employees were tasked with being on the watch for changes in the customer's conduct or information, and the employee in question was then responsible for responding to changes and, for instance, notifying the responsible person.

5.20. Several entities compared information from data vendors with their own information on a regular basis. The flaw in this method, however, was that the obliged entities did not respond systematically to new information by requesting documentation or explanations when appropriate or, if applica-

28. See, among other things, Items 1.6-1.10 of the ML/TF Risk Factors Guidelines.

ble, by conducting a new due diligence check. Nevertheless, this method was the most effective the Bank saw in this regard.

Good practice:

- Rules and criteria in monitoring systems are based, among other things, on the obliged entity's risk assessments.
- Flags from monitoring systems give a reliable indication of risks, and the number of flags is not restricted in order to save labour.
- Customers in different risk categories are subjected to different levels/types of monitoring.
- Flags are reviewed in a risk-oriented manner as soon as possible.
- Employees who review flags have a good understanding of the rules and criteria that have been defined to monitor customer conduct.
- When there is uncertainty about a given transaction, explanations and/or documents about it are requested.
- The obliged entity's systems indicate how the investigation of flags was conducted and how the results of the investigation were obtained.
- Obliged entities are proactive in their approach instead of relying reactively on existing information from due diligence checks.

VI Points for consideration

Lines of defence

6.1. According to the EBA Guidelines on internal governance,[29] internal controls are split into three lines of defence. The first line of defence generally comprises front-line employees and management, the second line of defence extends to compliance and risk management staff, and the third line of defence is the internal auditor, who works for and is authorised by the board of directors. In its thematic check, the Central Bank did not assess whether defences were handled by the appropriate line of defence; instead, it focused primarily on whether the defences were in place and were adequate. As a result, the Bank did not find fault with defences that were in the "wrong" line of defence if they were indeed in place.

6.2. In formulating internal controls and risk management measures, it is important to ensure that the unit that generates the risk is responsible for it, and that monitoring measures are in place to ensure that internal and external requirements are met. Obliged entities must therefore define and describe the roles and responsibilities of each line of defence, as it was common that the first line of defence relied excessively on the second, which was generally sparsely staffed. Furthermore, there were examples where the first line of defence was relied upon more heavily than was practicable. In the cases where substantial responsibility was assigned tothe first line of defence, there was usually a significant lack of adequate handling of defences.

6.3. It is important that each line of defence play the role intended for it and that a distinction be made between first-line monitoring, on the one hand, and second-line monitoring by compliance and risk management, on the other. The third line of defence then conducts appraisals in order to determine the efficacy and quality of first- and second-line monitoring.

Employee expertise

6.4. The results of the Central Bank's thematic check reflect the need to bolster knowledge of ML/TF defences among obliged entities' employees. In this context, it is important that front-line staff and supervisory unit staff have full support from management and board members in carrying out tasks relating to ML/TF defences. Furthermore, it is necessary to foster a positive attitude among employees concerning customer due diligence and make it clear to employees that conducting due diligence checks serves an important purpose, both for the obliged entity and in the public interest.

6.5. There are various ways to increase staff awareness, but the Central Bank is of the view that the most important tool for changing the company culture in this respect is the steadfast involvement of board members and management. This entails, among other things, responding to comments in reports from compliance officers/money laundering reporting officers when they point out deficiencies in ML/TF defences, and providing scope for employee training.

29. EBA Guidelines on internal governance, EBA/GL/2021/05.

What can be learned from others' mistakes?

6.6. Increased emphasis has been placed on ML/TF defences worldwide in the recent term. As a result, obliged entities that have not paid due attention to this area have been subjected to heavy fines and have suffered reputational damage. It is important that Icelandic obliged entities acquaint themselves thoroughly with cases that have precedent value for them and learn from others' mistakes.[30]

References to regulatory instruments and other documents

Domestic regulatory instruments and guidance documents

- Act on Measures to Combat Money Laundering and Terrorist Financing, no. 140/2018
- Regulation on Customer Due Diligence with Respect to Anti-Money Laundering and Terrorist Financing Measures, no. 745/2019
- Regulation on Risk Assessments due to Money Laundering and Terrorist Financing, no. 545/2019
- Act on the Freezing of Funds and Designation of Entities on Sanctions lists in Relation to Terrorism Financing and Proliferation of Weapons of Mass Destruction, no. 64/2019
- Regulation on Information Accompanying Transfers of Funds in Connection with Measures to Combat Money Laundering and Terrorist Financing, no. 70/2019
- National Commissioner of the Icelandic Police Risk Assessment, issued March 2021
- Váþættir á bankamarkaði [Red Flag Indicators in the Banking Market; in Icelandic], issued by the Central Bank of Iceland, March 2021
- Áhættusöm ríki [High-Risk Jurisdictions; in Icelandic], issued by the Ministry of Justice steering group, May 2019
- Rannsóknar- og tilkynningarskylda [Obligation to Investigate and Notify; in Icelandic], issued by the Ministry of Justice steering group, May 2019
- Þjálfun starfsmanna [Employee Training; in Icelandic], issued by the Ministry of Justice steering group, May 2019
- Ábyrgðarmaður [Money Laundering Reporting Officer; in Icelandic], issued by the Ministry of Justice steering group, May 2019
- Áhættuþættir á líftryggingamarkaði [Risk Factors in the Life Insurance Market; in Icelandic], issued by the Financial Supervisory Authority, March 2019
- Áhættuþættir á verðbréfa- og sjóðamarkaði [Risk Factors in the Securities and Funds Markets; in Icelandic], issued by the Central Bank of Iceland, August 2022
- Áhættuþættir tengdir peningasendingum [Risk Factors Associated with Money Transfers; in Icelandic], issued by the Central Bank of Iceland, September 2022 [NOTE: There is a new version of his doc, issued in 2022.]
- Áhættuþættir vegna útgáfu og meðferðar rafeyris [Risk Factors Associated with Issuance and Treatment of Electronic Money; in Icelandic], issued by the Financial Supervisory Authority, June 2019
- Áhættumat [Risk Assessment; in Icelandic], issued by the Ministry of Justice steering group, June 2019.
- Áreiðanleikakönnun [Due Diligence; in Icelandic], issued by the Ministry of Justice steering group, June 2019.
- Alþjóðlegar þvingunaraðgerðir [International Sanctions; in Icelandic], issued by the Ministry of Justice steering group, July 2019
- Leiðbeiningar um eftirlit með viðskiptamönnum á listum yfir þvingunaraðgerðir [Guidelines for Monitoring of Customers on Targeted Sanctions Lists; in Icelandic], issued by the Financial Supervisory Authority, November 2019

30. See, for example, AML Bank Fines Report 2020 and AML Bank Fines Report 2021.

Foreign guidance documents

- EBA Guidelines on ML/TF Risk Factors, EBA/GL/2021/02, issued 1 March 2021
- FATF Recommendation, issued February 2012, updated June 2021
- Materials issued by the Joint Money Laundering Steering Group (JMLSG) in the UK
- Guidance for a Risk-Based Approach: for The Banking Sector, Life Insurance Sector, and Virtual Assets and Virtual Asset Service Providers, issued by FATF.
- FATF Guidance: Transparency and Beneficial Ownership, issued by FATF
- Best Practices on Beneficial Ownership for Legal Persons, issued by FATF
- FATF Guidance: Correspondent Banking Services, issued by FATF
- FATF Report: Professional Money Laundering, issued by FATF
- FATF Report: Virtual Assets – Red Flag Indicators, issued by FATF

Useful websites

- https://www.fme.is/eftirlit/eftirlit-med-adgerdum-gegn-peningathvaetti-og-fjarmognun-hrydju-verka/
- https://www.fatf-gafi.org/
- https://www.wolfsberg-principles.com/
- https://www.acams.org/en
- https://baselgovernance.org/
- https://www.handbook.fca.org.uk/handbook/FCG.pdf
- https://jmlsg.org.uk/