

DATE: 31 DECEMBER 2025

Supervisory Benchmark No. 1/2025

Expectations of the Financial Market Supervision Department regarding the audit of an institution's governance system in the AML/CFT area

1. Relevant legislation

Auditing the governance system in the area of anti-money laundering and countering the financing of terrorism (hereinafter "AML/CFT") involves verifying the overall functioning and configuration of the institution's AML/CFT system, or parts thereof, against all applicable legal requirements and standards. The basic legal framework governing the area of AML/CFT relevant to financial institutions consists mainly of the following legal regulations:

- Act No. 253/2008 Coll., on Selected Measures against Legitimation of Proceeds of Crime and Financing of Terrorism, as amended (hereinafter the "AML Act")
- Act No. 69/2006 Coll., on the Implementation of International Sanctions, as amended (hereinafter "Act No. 69/2006 Coll.")
- Act No. 1/2023 Coll., on Restrictive Measures against Certain Serious Acts Committed in International Relations
- Government Regulation No. 210/2008 Coll., implementing special measures to combat terrorism, as amended by Government Regulation No. 88/2009 Coll.¹
- Decree No. 67/2018 Coll., on selected requirements for the system of internal rules, procedures and control measures against legitimisation of proceeds of crime and financing of terrorism, as amended (hereinafter the "AML Decree")
- Decree No. 163/2014 Coll., on the performance of activities of banks, credit unions and investment firms, as amended (hereinafter "Decree No. 163/2014 Coll.")
- 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 (hereinafter the "TFR")
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit institutions and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries (hereinafter "Commission Delegated Regulation 2019/758")
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

¹ EU sanctions are also governed by directly applicable EU legislation, in particular the relevant Council decisions and regulations (a list of which is available, for example, at <https://fau.gov.cz/informacni-zdroje>).

Additional relevant legislation includes:

- Act No. 21/1992 Coll., on Banks, as amended (hereinafter the “Act on Banks”)
- Act No. 87/1995 Coll., on Savings and Credit Unions, as amended (hereinafter the “Act on Savings and Credit Unions”)
- Act No. 277/2009 Coll., on Insurance, as amended (hereinafter the “Insurance Act”)
- Act No. 427/2011 Coll., on Supplementary Pension Savings, as amended (hereinafter “Act No. 427/2011 Coll.”)

The Czech National Bank (hereinafter the “CNB”) published an overview of recognised standards on its website in its Official Information of 26 May 2009 on certain requirements for the system of internal principles, procedures and control measures against the legitimisation of the proceeds of crime and financing of terrorism.²

These primarily include standards, recommendations and analyses of methods and trends reflecting developments in the AML/CFT area and similar documents (for example, guidance) intended to prevent ML/TF prepared by the intergovernmental Financial Action Task Force (hereinafter the “FATF”).³ Other relevant actors are also mentioned, in particular:

- the Basel Committee on Banking Supervision (BCBS)⁴
- the International Organisation of Securities Commissions (IOSCO)
- the International Association of Insurance Supervisors (IAIS).

Also essential are the general AML/CFT guidelines issued by the European Banking Authority⁵ (hereinafter also the “EBA”), which institutions must take into account in their internal regulations in accordance with Article 4(2) of the AML Decree.

Relevant EBA guidelines include, for example:

- Guidelines EBA/2021/02 under Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (“The ML/TF Risk Factors Guidelines”), repealing and replacing Guidelines JC/2017/37 (EBA/GL/2021/02);
- Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT compliance officer under Article 8 and Chapter VI of Directive (EU) 2015/849 (EBA/GL/2022/05);
- Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (“Travel Rule Guidelines”) (EBA/GL/2024/11);
- Guidelines on policies and controls for the effective management of money laundering and terrorist financing risks when providing access to financial services (EBA/GL/2023/04);
- Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of

² https://www.cnb.cz/export/sites/cnb/en/legislation/.galleries/provisions_and_official_information/v_2009_08_21109560_en.pdf.

³ The FATF is an intergovernmental organisation that issues *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, The FATF Recommendations* (updated November 2023, available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>).

⁴ For example: Basel Committee on Banking Supervision, *Sound management of risks related to money laundering and financing of terrorism (Guidelines)*, January 2014 (rev. July 2020).

⁵ <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countermeasures/anti-money-laundering-and-countermeasures>

- Directive (EU) 2015/849 (EBA/GL/2022/15);
- Guidelines on outsourcing arrangements (EBA/GL/2019/02).

In accordance with Article 4(3) and Article 5(1) of the AML Decree, institutions must also take into account other recognised standards that are current and proportionate to the nature of the specific institution. These include, in particular, methodological and interpretative materials and decisions of the CNB, the Financial Analytical Office (hereinafter the “FAU”) and other relevant national authorities.

The following materials fall within this category:

CNB supervisory benchmarks⁶ and FAQs, for example:

- Supervisory benchmark No 2/2023 – On client due diligence via the transaction monitoring system
- Supervisory benchmark No 4/2022 – On prudent approach of credit institutions to publicly available information with AML/CFT implications
- Supervisory benchmark No 2/2018 as amended on 22 July 2022 – On the requirements for selected procedures for the implementation of international sanctions
- Answers to FAQs published on the CNB’s website – on selected topics.⁷

FAU methodological instructions,⁸ in particular:

- Methodological Instruction No. 1 – On the implementation of international sanctions in the context of the financing of terrorism
- Methodological Instruction No. 3 – Determining the beneficial owner
- Methodological Instruction No. 4 – Submission of a suspicious transaction report otherwise than by the MoneyWeb tool
- Methodological Instruction No. 5 – Implementation of certain restrictive measures in respect of persons, entities and bodies subject to the decisions of the United Nations Security Council
- Methodological Instruction No. 7 – Measures against politically exposed persons + the national list of PEP functions
- Methodological Instruction No. 8 – Copying of identity cards for the purposes of the AML Act
- Methodological Instruction No. 9 – Customer due diligence for credit and financial institutions

FAU opinions,⁹ particularly those concerning customer identification, customer due diligence, politically exposed persons (PEPs) and other areas.

Relevant opinions and interpretative materials of other authorities, for example the *Handbook of the Ministry of Justice of the Czech Republic on the registration of beneficial owners*.¹⁰

⁶ Available on the CNB website: <https://www.cnb.cz/en/supervision-financial-market/legislation/money-laundering/methodological-and-interpretative-documents/>

⁷ CNB answers to FAQs – selected Q&As on the CNB website <https://www.cnb.cz/en/supervision-financial-market/legislation/cnb-opinions-on-financial-market-regulations/>

⁸ Available on the FAU website: <https://www.fau.gov.cz/en/site-map/international-and-legal-agenda/national-legislation-285>

⁹ Available on the FAU website: <https://fau.gov.cz/stanoviska-fau> (in Czech only).

¹⁰ Available at: <https://esm.justice.cz/ias/issm/prirucka> (in Czech only).

2. Introduction

Banks are required to establish an internal control system, the key components of which are an internal audit function and continuous monitoring of compliance with legal obligations and obligations arising from the institution's internal regulations (the compliance function). This requirement arises from Article 8b(1)(c) of the Act on Banks. The institution's risk management framework includes AML/CFT risk management. The statutory requirement is specified further in the EBA guidelines on internal governance (EBA/GL/2021/05),¹¹ particularly in Title V, points 141 et seq. These guidelines address the internal control framework, including the internal audit function and the compliance function. The assessments conducted by the internal audit function – the third line of defence – cover the AML/CFT area.

This document provides guidance for the internal audit function's approach to each component of the institution's AML/CFT risk management framework. It examines in detail the related statutory obligations of banks, the manner in which compliance should be reviewed, and the evidence that should be used for the audit.

The report assessing the bank's internal control system should always be adapted to the nature of the specific institution. This will be reflected primarily in the content and scope of the report, as well as in the internal audit procedures applied, particularly with regard to the formal requirements and structure of the report. All expectations set out below should therefore be applied proportionately and only where they are relevant.

The benchmark below sets out the CNB's expectations regarding the audit of the governance system specifically in the AML/CFT area. It can likewise be used as guide for other audits of the governance systems of banks which are subject to verification of compliance with AML/CFT obligations. Such audits include, in particular, the audit of the governance system, or part thereof, by an external auditor, which the CNB may order for a bank or branch of a foreign bank from a non-Member State pursuant to Article 22a of the Act on Banks, provided that the conditions set out in that provision are met. Article 22a(6) of the Act on Banks sets out the minimum requirements for the audit report.

This document is also applicable to internal or external audits conducted in other financial market entities. Under Article 8b(1)(c)(1) of the Act on Savings and Credit Unions, credit unions, too, must have an internal control system, including an internal audit function and a compliance function. Insurance undertakings and pension companies likewise have an obligation to establish and maintain an effective governance system, including an internal audit function (Article 7(1) et seq. of the Insurance Act and Article 50 of Act No 427/2011 Coll.).

This document may be used for external audits in these entities. Under Article 8b(1)(b) of the Act on Savings and Credit Unions, a credit union is required to have its governance system audited by an auditor once every three years; the CNB is authorised by law to waive the requirement to perform the audit or parts thereof. Under Article 81 of the Insurance Act, the CNB may order a domestic insurance or reinsurance company to have an auditor audit its governance system, or part thereof, where such an audit is warranted by deficiencies identified in its activities.

This document is not intended to provide a complete list or a mandatory and fixed structure for a report resulting from an assessment under any of the above provisions. Its purpose – in respect of

¹¹ https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-05%20Guidelines%20on%20internal%20governance/translations/1021312/GL%20on%20internal%20governance%20under%20CRD_CS%20-%20updated.pdf

audits conducted pursuant to Article 22a of the Act on Banks, Article 8b of the Act on Savings and Credit Unions and Article 81 of the Insurance Act – is to provide guidance on the scope and content of auditors' reports in order to enhance their applicability and comparability.

3. CNB expectations

The CNB expects external and internal auditors (hereinafter collectively referred to as the “auditor”), to assess, through their investigation, the **overall functioning of the governance system** in the AML/CFT area across all lines of defence, where relevant,¹² or in the specific part of the AML/CFT area to which the audit was limited. In this context, they should focus in particular on evaluating the adequacy of the institution's organisational and technical arrangements, its system for identifying and assessing the risk of money laundering and the financing of terrorism (hereinafter “ML/FT”), the segregation of incompatible functions and decision-making powers, the internal regulatory framework, the sufficiency of the internal control mechanisms in place, and staffing and resourcing.¹³ In this context, it is essential to test whether the defined AML/CFT processes and measures are truly embedded in all of the institution's activities (use test), whether the institution applies a risk-based approach effectively to the management of its ML/FT risks, whether information and control mechanisms are configured vertically and horizontally within the institution, and whether the configuration and application of AML/CFT procedures is compliant with the legal requirements. Where relevant, these risk management rules should also be implemented and maintained by institutions with a governance system on a consolidated or sub-consolidated basis.

The method and depth of the audit of the governance system in the AML/CFT area should take into account the size, nature and scope of the specific institution's activities and the ML/FT risks to which it is exposed. In line with the risk-based approach, it is necessary to examine each area audited and assess it in terms of its relevance in the context of the institution concerned. The application of a risk-based approach by the auditor is particularly important when assessing the severity of the individual findings, as their impact and significance may differ fundamentally between institutions.¹⁴ The specific nature of the institution is also relevant when determining the level of detail applied to the individual areas audited. For some institutions it will be warranted to examine certain audited areas in greater depth than others.¹⁵ The approach taken should always be justified in the report, at least briefly, particularly with regard to the context of the institution concerned. **Where the scope of the audit of the governance system is limited to a specific part or parts of the AML/CFT area,¹⁶ the expectations set out above apply proportionately. In such cases, however, the CNB**

¹² The “three lines of defence” model is generally applied to governance systems. The first line of defence is responsible for owning and managing risks in day-to-day activities. The second line of defence is responsible for coordinating and overseeing the effectiveness and integrity of the risk management framework. The third line of defence – usually the internal audit function – provides objective assurance on the functionality and effectiveness of the risk management system. It regularly assesses the risk management process, compliance, and the effectiveness and timeliness of information flows, and identifies potential vulnerabilities in this process.

¹³ “Staffing and resourcing” refers to having a sufficient number of qualified and trustworthy employees.

¹⁴ For example, in the case of a credit institution that specialises in retail clients and has a limited number of corporate clients, the findings relating to the identification of beneficial owners may be less severe than for an institution with a different business model. However, this always depends on the overall impact assessment.

¹⁵ While for some institutions, correspondent banking may constitute a significant part of their business model – requiring very detailed examination of the effectiveness of related risk management measures – for other institutions, this area may be irrelevant/inapplicable.

¹⁶ Such a limitation may arise, for example, from the internal audit work plan or from the CNB's decision to impose such a limitation.

generally expects a greater level of detail in the audit of the relevant part, including broader testing of practical implementation (where relevant).

A mere review of the internal regulations by the auditor is not sufficient to assess the effectiveness of the institution's governance system; it is necessary to test their implementation in practice. The report should clearly indicate whether each statement (i.e. the identification of shortcomings or, conversely, confirmation of compliance with legal requirements) relates to an assessment of the internal regulations or of their actual implementation.¹⁷

The recommendations set out below form a basis that the CNB expects the auditor, in cooperation with the institution under assessment, to further elaborate, expand and adapt to the nature of the institution.

4. Recommended structure and content

The content of the report is stipulated in Article 22a(6) of the Act on Banks. For the report to meet these requirements, the CNB expects it to include, inter alia, the following:

- a definition of the standards governing the audit;
- a description of the institution undergoing the audit of its governance system in the AML/CFT area, and of the areas audited;
- an identification of the internal control mechanisms in place and an assessment of their functionality and effectiveness, in particular against the legal requirements;
- an overall evaluation of the areas audited, including the identification of any missing internal control mechanisms and an assessment of the severity of the individual findings.

4.1. Definition of standards and formal requirements

The regulations listed in section 1 of this document do not specify formal requirements for audits, and even in the case of audit reports, the legislation does not determine the level of assurance that the audit should provide.¹⁸ It is therefore for the contracting authority to determine the level of the audit and the formal requirements for the structure of the report, ensuring that the purpose of the audit is fulfilled and that its quality is assured.

4.2. Description of the institution whose governance system is under audit in the AML/CFT area, and of the areas audited

The CNB expects this section to include the following, where relevant:

- an overview of the institution's bodies, committees and other units involved in AML/CFT

¹⁷ The report should assess both the compliance of the internal regulations with the legislation and the compliance of actual practice with the internal regulations and, where applicable, the legislative requirements. This distinction is also necessary for formulating appropriate remedial measures.

¹⁸ Auditing standards distinguish between reasonable assurance engagements and limited assurance engagements.

activities by dint of their functions, powers and responsibilities, specifying the individuals heading these units or those responsible for AML/CFT activities, together with a description of the basic hierarchical relationships within these units, within the institution as a whole and, where applicable, within the group;

- staffing and resourcing for the performance of activities in individual AML/CFT areas;
- a description of the ML/FT risks to which the institution is exposed across its lines of business;
- a description of the roles, powers and approval and decision-making processes within the institution, with emphasis on AML/CFT risk management – for example, a basic description of the responsibilities (tasks) of individual bodies, committees, units or individuals in the AML/CFT area;
- an overview and description¹⁹ of the institution's internal regulations governing AML/CFT;
- a basic description of the institution's processes, measures and control measures in the AML/CFT area;
- a description of the information systems used by the institution for ML/FT risk management.

4.3. Identification of the internal control mechanisms in place and assessment of their functionality and effectiveness, in particular against the legal requirements and recognised standards

This section should include a risk management assessment relating to the specific areas of the institution's AML/CFT system under audit, either with regard to the AML/CFT system as a whole or to the individual parts defined by the CNB. The CNB expects the auditor to describe and evaluate the control mechanisms applied in the institution's activities listed below, or in specified categories of those activities.²⁰ The auditor should carry out this audit in accordance with the requirements laid down in the legislation and recognised standards, describe the procedures used and set out its findings.

The description of the assessment should always clearly distinguish between the institution's own statements, the content of its internal regulations, the procedures actually implemented in practice, and the auditor's conclusions. This part of the report should therefore be divided into a section describing the situation in the institution (distinguishing between the applicable internal regulatory framework and its practical implementation) and a section presenting the auditor's opinion, comparing these facts with the legal requirements and recognised standards. This opinion should state briefly but specifically where a deficiency has been identified and whether it affects only the internal regulatory framework, actual practice, or both. When describing the

¹⁹ A description means a summary of the content, the date of the last update, and the completeness of the regulations, including any annexes.

²⁰ Alternatively, the auditor should state that the area is not relevant to the institution.

procedures and the auditor's assessment, the scope and depth of the assessment should always be evident so that it is clear how the auditor examined and tested the procedures applied.²¹

We emphasise that, in this section, the auditor should describe the institution's internal procedures and their effectiveness as they actually work in practice. It is neither appropriate nor useful to include lengthy quotations from internal regulations or from interviews with employees or persons performing work for the institution other than under an employment relationship (hereinafter collectively "staff"). Such information should be summarised, with any specific quotations included in an appendix.

With regard to the classification of ML/FT risk management measures and their legislative framework, the main areas audited are summarised in six sections set out in the **appendix** to this benchmark. A suggested structure is provided, forming a basis that the auditor should further elaborate, expand and adapt to the nature of the institution as appropriate.

APPENDIX:

1. AML/CFT risk management framework and organisational arrangements	12
2. Staffing and technical arrangements	24
3. Customer identification and due diligence	29
4. Transaction monitoring and reporting of suspicious transactions	38
5. Implementation of sanctions measures	44
6. Other	47

4.4. Overall assessment of the areas audited, including identification of any missing internal control mechanisms and assessment of the severity of individual findings

As mentioned above, it is appropriate – for the sake of clarity – to briefly present the individual findings already in the description of the area under review.

The detailed description of each finding should always make it clear whether it involves a deficiency in the design of the internal regulations or a deficiency in the procedures implemented in practice. In this context, it is also necessary to examine the scope and underlying causes of each finding in order to determine whether it represents an isolated error or a systemic deficiency; this information should always be included in the report. This is particularly important where customer sample testing is used as a tool, as it is always important to assess whether an error relating to one or more customers resulted from a broader systemic issue (such as missing procedures, insufficient training or IT system errors). Conversely, some procedures may function effectively in practice despite being insufficiently documented, indicating that the cause of the deficiency lies elsewhere.

²¹ For example, it should always be clear whether the auditor verified only the existence of a particular internal regulation, or also assessed compliance with its formal requirements, or also examined the effectiveness and quality of its content.

The severity of each finding must be inferred from an assessment of the above factors and, in particular, with regard to the actual and potential impact on the effectiveness of the institution’s risk management processes.²² Severity should be assessed in the context of AML/CFT risk management, so the assessment of the impact of the deficiency on the implementation and effectiveness of the required AML/CFT measures should take precedence over purely financial criteria. The context of the specific institution and the nature and scope of its activities is also relevant (as described in more detail above in relation to the application of the risk-based approach).

The CNB expects the auditor to assess the severity of its findings using the following severity scale:

Assessment of deficiency	Description of deficiency	Impact of deficiency on effectiveness of assessed AML/CFT measures
Low severity	Deficiencies predominantly of a non-systemic nature with low severity	No impact
Medium severity	Systemic and non-systemic deficiencies with medium severity	Minor negative impact
High severity	Deficiencies predominantly of a systemic nature with high severity	Major negative impact
Very high severity	Significant deficiencies of a systemic nature with very high severity	Effectiveness not ensured

5. Audit method

The above text for each area audited also lists recommended sources of information that may be used to verify both the compliance of the procedures in place with the legal requirements and their effectiveness in practice.

5.1. Internal regulatory framework

The basis for verifying the effectiveness, completeness and adequacy of an institution’s governance system in the AML/CFT area is an **assessment of its internal regulations and established procedures**.

The internal regulations are documented requirements for the design of internal procedures and processes. When evaluating internal regulations, the first step is to determine whether the required regulations exist and whether they contain all the formal and practical elements stipulated in Article 22a(6)(c) of the Act on Banks.

The internal regulations should include all the requirements stipulated by law and reflect the specific characteristics of the institution concerned. In particular, they should cover all relevant activities of the institution to the necessary extent, adequately define all the key attributes of the institution’s processes and procedures in the AML/CFT area, and thereby create the conditions for ensuring that the institution’s actual procedures and processes correspond to their prescribed formulation in the internal regulations, are reconstructable and auditable, and comply with the legal requirements.

²² One example is a finding that processes implemented in practice were not documented. Such a seemingly formal shortcoming may have significant implications in the event of staff turnover or even when the procedures applied are challenged, as the absence of documentation makes them unenforceable.

To meet these requirements, it is essential to ensure the practical applicability of the regulations. This requires clarity and specificity in determining who is responsible for fulfilling each obligation, as well as when and how it is to be met, and who is accountable for implementing the regulations.

5.2. Practical implementation

After assessing the internal regulations, it is also necessary to verify their practical implementation in the institution's processes, i.e. to assess how each process is actually implemented in practice and how effective it is. The method of verification will vary depending on the specific area audited. **The CNB expects the auditor, in line with the risk-based approach and taking into account the specific characteristics of the institution concerned, to use an appropriate combination of the following procedures and methods to a proportionate extent for the audit.**

A fundamental tool that is particularly relevant for verifying customer identification and due diligence, including the detection and reporting of suspicions, is **sample testing**. The sample selection method should always be consistent with the objective of the audit so that the sample is representative²³ and proportionate to the population under review (in terms of customer portfolio, generated alerts, etc.). The sampling approach should always be explained and justified in the audit. This tool involves testing, for example, a customer sample, a sample of alerts generated by the transaction monitoring or sanctions screening system, and a sample of suspicious transaction reports.

Summary data on customers and transactions can also be used for making broad checks in these areas. This enables verification of the general fulfilment of certain obligations (including whether all the necessary information is recorded in the system), as well as the identification of areas where closer examination is warranted (for example, the frequency of errors or missing information). This method also allows for a broad assessment of compliance with obligations in terms of their timing, for example in the case of periodic customer due diligence (and related updates of customer information), the handling of alerts generated through transaction monitoring, and sanctions screening (i.e. whether a backlog exists and how significant it is). This method is a useful complement to sample testing, particularly where the volumes and numbers of data items under review (customers, alerts, notifications) are high.

In the case of transaction monitoring and sanctions screening, it is appropriate to verify the general **configuration of the system used**, i.e. whether the system actually corresponds to the described configuration. This will primarily involve checking whether the required detections occur when the specified conditions are met and whether there are any hidden exceptions. The effectiveness of the audit of the system can also be enhanced by testing it in a dedicated test environment using a pre-prepared fictitious sample of inputs (transactions, customers).

For certain specific processes, it is also appropriate to review additional documentation (for example, mutual contractual arrangements), particularly in the context of correspondent banking or outsourcing. When examining outsourcing and the contracts on which it is based in the AML/CFT area, the primary focus is not on determining the materiality of the outsourcing, the transfer of all obligations or legal guarantees, but rather on taking a holistic view of the outsourcing arrangement,

²³ As an example, when verifying the quality of the approach to customer risk categorisation, the sample should not be created solely on the basis of customers assigned a high risk; on the contrary, it is appropriate to examine all types and categories of customers. This makes it possible, among other things, to verify whether all customers who should be in the higher-risk category are actually there.

the obliged entity's awareness of how the outsourced processes are structured, the extent of its influence over this structure, and its ability to verify the outputs.

To verify the functioning of the governance system as a whole, as well as any of its individual components, it is essential to review the relevant control mechanisms (**the frequency, scope and results of internal audits, the content of assessment reports or discussions by the institution's management, and the outcomes of internal assessments of the effectiveness of implemented processes**). Other appropriate tools include **interviews with relevant staff, verification of their job descriptions, training content and e-mail documentation, and verification of the reconstructability of processes, i.e. document retention and the logging of actions and information**.

The aim of verifying the effectiveness of individual AML/CFT measures is to ensure a more in-depth assessment that takes into account their practical implementation and actual effectiveness within the institution. The primary focus, however, is to assess the substantive functioning of the systems, and for this purpose it is not always necessary to review (i) the technical configuration of IT systems, (ii) the technical functioning of IT systems, (iii) the general access management rules or (iv) the financial aspects of IT systems (i.e. the IT budget and its adequacy).

Specific sources for verifying the effectiveness of individual areas are set out in detail in the relevant sections below.

Financial Market Supervision Department, 31 December 2025

APPENDIX:

1. AML/CFT risk management framework and organisational arrangements

1.1. Group-wide procedures and strategy

Legal requirements	
Consistency of the institution's group-wide strategies, procedures and risks with Czech law and with the institution's individual characteristics	Article 21(7) of the AML Act and Article 15(1) and (2) of the AML Decree
Application of group-wide procedures across the group, in particular within the institution's branches and subsidiaries	Article 21(7) and Article 24a of the AML Act and EBA/GL/2022/05
Procedures for information sharing within the group and for taking account of such information	Article 15(3) of the AML Decree
Effective management of risks associated with the group's activities in third-country jurisdictions	Commission Regulation 2019/758

Audit content²⁴

An institution that is part of a group:

- takes into account the group-wide AML/CFT strategies and procedures, as well as other factors associated with the institution's participation in the group, in its internal regulations and procedures;
- sets its internal regulations in accordance with Czech legislation and reflects the Czech environment, inter alia within its risk assessment;
- takes into account, within its internal regulations – in particular within its risk assessment – the risks and other factors associated with its participation in the group;
- takes into account, within its internal regulations – in particular within its risk assessment – its own individual characteristics and the risks associated with them.

An institution that has branches, establishments and subsidiaries:

- implements the group-wide AML/CFT procedures and strategies in a manner that ensures the effective management of ML/FT risks across the group (unless these are set at a higher level within the group), and coordinates the configuration of the internal regulations and procedures of the individual entities within the group;
- applies these group-wide strategies and procedures across all its branches, establishments and subsidiaries, and regularly assesses their effectiveness;
- configures in an appropriate manner an organisational structure and coordination and control mechanisms at group level that prevent conflicts of interest, set communication channels for

²⁴ The assessment in this area concerns primarily the quality and effectiveness of the configuration of the group-wide procedures, including the control mechanisms in place, rather than the assessment of compliance with AML/CFT regulations by entities other than the institution under review (although such an assessment may also be carried out).

adequate information exchange, define relevant decision-making powers at group level, and ensure compliance with AML/CFT obligations across the group;

- ensures the remediation of deficiencies identified in the AML/CFT area across the entities within the group.

An institution that has branches, establishments and subsidiaries operating in third-country jurisdictions:

- applies the group-wide AML/CFT procedures and strategies in its branches, establishments and subsidiaries in third-country jurisdictions in a manner that ensures that the measures implemented are at least equivalent to the requirements of European Union law in the AML/CFT area;
- informs the FAU where its branches, establishments or subsidiaries are located in third-country jurisdictions whose legal frameworks do not permit the application of the group-wide AML/CFT procedures and strategies to the extent described above, and implements additional measures to manage the associated risks.

Sharing of information within the group

- The institution implements procedures to ensure the appropriate consideration of, at a minimum, information on reported suspicious transactions, refusals to execute a transaction or to enter into or continue a business relationship with a customer, or the termination of an existing business relationship for reasons related to ML/FT risk, as well as the sharing of information affecting a customer's risk profile, including such risk-profile information obtained within the group, in its internal procedures, assessments, analyses and its approach towards specific customers.

Links to other assessed areas

Risk assessment

- The institution's risk assessment takes into account both the factors arising from its participation in the group and the institution's individual characteristics, as well as those of the Czech Republic.

Outsourcing

- The institution always retains the key and strategic decision-making functions, including ensuring the necessary staffing and expertise to perform them;
- The configuration of outsourcing arrangements, including those within the group, is subject to all key obligations (contractual basis, definition of mutual obligations, performance of controls over outsourced activities, etc.).

Audit sources
<ul style="list-style-type: none"> • <i>Mandatory disclosures containing information on the composition of the group and its business activities (basic information about the institution and the group);</i> • <i>The organisational chart of the institution and the group, including governing and advisory bodies, the names of senior officers, and all mechanisms and units responsible for fulfilling AML/CFT obligations;</i> • <i>The organisational rules and job descriptions of the relevant units and senior officers of the institution and the group;</i> • <i>Relevant internal regulations of the institution and the group, including the risk assessment;</i>

- Minutes of meetings of the institution's and the group's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;
- The group-wide AML/CFT strategy;
- Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;
- A list of any meetings held between the group AML function (where established) and the individual institutions within the group, together with records of those meetings;
- The configuration of the technical tools used to ensure information sharing within the group;
- Outsourcing contracts;
- Interviews with relevant staff and senior officers;
- Reports from previous internal/external audits and compliance reports for the institution and the group, where available;
- The internal audit plan;
- The compliance monitoring plan;
- Reports on relevant supervisory investigations/inspections.

1.2. Internal regulations as the framework for ML/FT risk management

Legal requirements	
Scope and configuration of the institution's internal regulations for AML/CFT risk management, including coverage of the requirements laid down in legislation and all relevant business activities of the institution	Article 4(1) and (2) and Article 21 of the AML Act, Article 4(4) of the AML Decree and Article 8 et seq. of Decree No. 163/2014 Coll.
Consistency of the institution's internal procedures with its internal regulations, and the effectiveness of its internal AML/CFT regulations	Article 10 of Decree No. 163/2014 Coll. and EBA/GL/2022/05
Procedures for monitoring relevant changes and identifying the need to update internal regulations	Article 21(2) of the AML Act and Article 4 of the AML Decree

Audit content

The institution has established – and applies – procedures for the preparation and ongoing updating of its internal regulations, including:

- the clear allocation of responsibility for preparing and updating the internal regulations;
- the setting of minimum intervals for updating the internal regulations and the identification of ad hoc situations in which updates must be made;
- the establishment of control mechanisms to verify that the above updates have been carried out;
- the documentation of the process for preparing and updating the internal regulations.

The institution has a written system of internal principles, procedures and control measures, including a written risk assessment, which:

- covers and takes into account the relevant legal obligations and applicable guidelines and, where appropriate, interpretative materials. The institution's internal regulations reflect the EBA Guidelines and other recognised standards, or the institution provides a reconstructable explanation as to why certain aspects have not been taken into account;

- is approved by the statutory body;
- is up to date, and its up-to-dateness is regularly reviewed within the institution;
- covers all relevant activities of the institution, including all products offered, services provided, its entire customer portfolio and the distribution channels it uses;
- covers all relevant legal obligations and is in accordance with the legislation currently in force in the Czech Republic;
- clearly defines specific obligations within the institution’s organisational structure and the responsibilities for performing specific activities;
- has a duly documented process for preparation and updating.

Links to other assessed areas

- The configuration of the internal regulations is linked to all other assessed areas.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution, including the risk assessment;</i> • <i>The institution’s internal regulations and documentation governing the process for their adoption and approval;</i> • <i>A list of the materials, documents, information and AML/CFT standards taken into account in the internal regulations;</i> • <i>The catalogue of products and services offered;</i> • <i>Documents demonstrating the process of preparation of the internal regulations and their approval by the institution’s statutory body;</i> • <i>A list of changes and revisions to relevant internal regulations;</i> • <i>Interviews with relevant staff and senior officers;</i> • <i>Minutes of meetings of the institution’s governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

1.2.1. Institution’s risk assessment

Legal requirements	
Procedures for assessing all relevant risks and for updating that assessment, including mechanisms to identify new ML/FT risks	Article 21a(1) and (3) of the AML Act and Articles 4 and 5 of the AML Decree
The type and scope of information, and the sources of such information, that are taken into account in the risk assessment	Article 21a(1) and Annex No. 2 of the AML Act, Articles (2)–(4) and Article 5 of the AML Decree and Supervisory Benchmark No. 4/2022

Application of the risk-based approach to the fulfilment of AML/CFT obligations	Article 21(1) and (5)(d) of the AML Act, Article 6 of the AML Decree and EBA/GL/2021/02
Procedures for identifying risks and managing them with an individual approach to customers (procedures to prevent the blanket refusal of groups or categories of customers – de-risking)	EBA/GL/2023/04

Audit content

General

- The institution has established in its internal regulations – and applies – procedures for preparing, approving, amending, implementing and applying its risk assessment, including the allocation of the relevant responsibilities;
- The institution has established in its internal regulations – and applies – procedures for regularly updating the risk assessment, both at periodic intervals and on an ad hoc basis, at least:
 - where the information used for the risk assessment is no longer current, where there are changes to the institution’s business activities or strategy, or where there are changes to the legislation,
 - prior to the introduction of new products or the use of new technologies;
- The institution’s risk assessment is up to date and is regularly updated;
- The institution documents all changes to the risk assessment or, where relevant, the reasons why no changes were made following an evaluation of potential grounds for revision, together with justification and identification of the decision-making powers applied;
- The institution has established in its internal regulations – and applies – procedures under which it regularly and continuously monitors publicly available information and analyses it at both the strategic and individual level in order to assess how, and to what extent, such information is relevant to its activities and the risks to which it is exposed;
- The institution has established in its internal regulations – and applies – procedures to ensure that the conclusions of the risk assessment are appropriately reflected in its internal regulations, and that the institution’s procedures are amended, where necessary, to ensure that they correspond to the results of the risk assessment;
- The institution has established in its internal regulations – and applies – procedures for the appropriate management of the risks to which it is exposed, including procedures ensuring an individual approach to customers and preventing the blanket refusal of groups or categories of customers (de-risking).

Content of the risk assessment

- The institution’s risk assessment ensures the identification of all relevant risks and provides a sufficient basis for defining the related procedures for managing them;
- In its risk assessment, the institution takes into account:
 - all relevant sources of information on ML/FT risks to which it is exposed, including at a minimum the national risk assessment, the EU supranational risk assessment, methodological and interpretative materials and decisions of the CNB and the FAU, and other information from the FAU, law enforcement authorities and other reliable sources,

- factors indicating potentially higher or lower risk (in relation to customers, products, services, transactions, distribution channels and geographical risk factors),
 - all products and services it offers or provides, including the ways in which they may be misused for ML/FT purposes,
 - information obtained in the course of customer identification and due diligence;
 - the technologies and distribution channels it uses,
 - reliable publicly available information, which it uses both for the identification of risks in respect of individual customers and for understanding generalised risks;
- The scope of information and the types of sources used in the risk assessment correspond to the nature, scale and complexity of the institution’s activities.

Links to other assessed areas

An institution that is part of a group:

- takes into account its participation in the group, the characteristics of the group and its business activities in the risk assessment;
- takes into account its own individual characteristics in the risk assessment.

Internal regulations and system of internal principles

- The institution has established in its internal regulations – and applies – procedures that ensure the management of ML/FT risks identified, thereby ensuring that the findings of the risk assessment and the measures applied are appropriately linked.

Customer risk assessment and application of preventive measures in relation to identified risks (customer identification and due diligence, risk categorisation, transaction monitoring, etc.)

- The institution has established in its internal regulations – and applies – AML/CFT measures towards customers in a manner proportionate to the risks they present, thereby ensuring that the findings of the risk assessment and the measures applied are appropriately linked;
- The institution regularly and continuously monitors publicly available information for the purpose of identifying risks relevant to its activities and takes this information into account both at the level of the institution’s risk assessment and in respect of individual relevant customers.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations, in particular the institution’s risk assessment;</i> • <i>A list of the changes made to the risk assessment and the documentation relating to those changes, or the justification where no change was made;</i> • <i>Documents demonstrating the approval of the risk assessment by the statutory body and the related discussions;</i> • <i>A list of the information sources used, including the procedure for verifying them;</i> • <i>The catalogue of products and services offered;</i> • <i>A list of high-risk countries, including the methodology for its preparation;</i> • <i>A list of high-risk activities, including the methodology for its preparation;</i> • <i>A list of the risk levels of legal forms, including the methodology for its preparation;</i>

- *Analyses of the risks of specific situations (e.g. the impact of a published case or geopolitical developments on the institution) and strategic risk analyses (e.g. the use of a particular product) prepared by the institution;*
- *Interviews with relevant staff and senior officers;*
- *Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

1.2.2. Information retention

Legal requirements	
Information retention – duration, scope and manner; retention of information in relation to all areas referred to in this benchmark	Article 11(5), Article 12(1), Article 16 and Article 17 of the AML Act
Ability to reconstruct the institution’s procedures and processes ex post, in particular approval and decision-making processes, including the documentation of refused and terminated business relationships with customers	Articles 17 and 18 of the AML Decree and EBA/GL/2023/04

Audit content

Internal regulations and procedures applied

- The institution has established in its internal regulations – and applies – procedures, in particular for retaining all relevant information on customers, relevant documents and records, records of the steps taken in the course of customer identification and due diligence and of any difficulties encountered in that process, and records of the procedure for assessing, determining or updating the customer’s risk profile, individual investigations of transactions within the business relationship, the application of mitigating measures and sanctions screening;
- The institution has established in its internal regulations – and applies – retention periods for information, ensuring that such information is retained for 10 years from the execution of a transaction outside a business relationship and from the termination of a business relationship with the customer;
- The institution has established in its internal regulations – and applies – procedures to ensure that decision-making and control processes are documented, including the approval of strategic materials, the performance of control activities, decisions on measures against customers, the investigation of alerts and the reporting of suspicious transactions, in a manner that makes these processes reconstructable;
- The institution has established in its internal regulations – and applies – procedures for retaining information where reliance is placed on customer identification carried out by another obliged entity, ensuring that the institution retains the required information, including copies of the documents related to customer identification and to the purpose and nature of the transaction;
- The institution has established in its internal regulations – and applies – procedures to ensure that the necessary information and copies of documents are obtained from another institution

where more than one institution is involved in a transaction and the information is retained only by one of them.

Information retention and reconstructability in practice

- Information relating to customer identification and due diligence and to the business relationship is:
 - available to the persons who assess suspicious transactions,
 - available in a form that enables effective processing,
 - available in a timely manner;
- The way in which information is processed ensures access to it and enables its subsequent processing and analysis;
- Information retrieval is ensured through an automated solution (appropriate to the size, scope and nature of the institution's activities) that enables timely work with relevant information.

Links to other assessed areas

Information retention is linked to all other areas assessed.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations, including regulations governing data archiving;</i> • <i>An overview of changes made to internal regulations, including their justification and approval;</i> • <i>An aggregated overview of the customer portfolio stating basic information;</i> • <i>A sample of customer files reflecting the different types of customers, including:</i> <ul style="list-style-type: none"> ○ <i>transactions executed outside a business relationship,</i> ○ <i>ongoing business relationships,</i> ○ <i>business relationships terminated less than 10 years ago,</i> ○ <i>business relationships established with reliance on customer identification and other remote identification methods under Article 11 of the AML Act;</i> • <i>A sample of agreements with third parties governing the reliance on customer identification and other remote identification methods (for example, the provision of information and copies of documents);</i> • <i>A sample of alerts from the transaction monitoring system, the way they were investigated and closed, and any documents requested/related to them;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system, including the configuration of access rights and the retention of information on changes made;</i> • <i>The content of training for relevant staff;</i> • <i>Interviews with relevant staff and senior officers;</i> • <i>Access rights relating to information on customer identification and due diligence and the business relationship;</i> • <i>Minutes of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections</i>

1.2.3. AML/CFT outsourcing (external provision of services or activities)

Legal requirements	
Configuration of outsourcing in accordance with the applicable legislation; completeness and effectiveness of governance	Article 12 of Decree No. 163/2014 Coll., EBA/GL/2019/02 and EBA/GL/2022/05
Definition and documentation of mutual obligations and responsibilities relating to the outsourcing of AML/CFT activities	Articles 11(3–6), 10 and 54(6) of the AML Act, Article 12(3) of Decree No. 163/2014 Coll., EBA/GL/2019/02 and EBA/GL/2022/05
Rules on controls at the outsourcing provider	Article 21(6) of the AML Act, Article 12 of Decree No. 163/2014 Coll., EBA/GL/2019/02 and EBA/GL/2022/05

Audit content²⁵

- The institution has defined, within the risk management strategy, its approach to outsourcing risk and has in place procedures for managing the risks associated with outsourcing;
- The institution has established in its internal regulations – and applies – procedures:
 - to determine whether an arrangement with a third party meets the definition of outsourcing,
 - to ensure that outsourcing does not result in the transfer of the responsibilities of the management body or of the institution’s accountability, and in particular that the institution remains able at all times to take strategic and key decisions,
 - for deciding whether to use outsourcing, including conducting an outsourcing risk assessment, selecting the outsourcing provider and carrying out due diligence on the provider,
 - to ensure that the outsourcing provider is authorised to perform the relevant activity, is reliable, professionally competent and experienced in carrying out the activity, and has a comparable risk management framework and internal control system,
 - to ensure that outsourcing is governed by a written contract and that contracts with outsourcing providers contain all required elements, in particular a specification of the subject matter and scope of the outsourced activities, a definition of the roles, powers and relationships between the contracting parties (the institution and the outsourcing provider), information security conditions, the provider’s obligation to supply information to the institution, procedures for

²⁵ All assessments in this subsection relate solely to outsourcing in the AML/CFT area, and only to the extent that it is relevant to the institution concerned. As the institution relies on a third party in these cases, while remaining responsible for carrying out the relevant measures as if it had performed them itself, it is essential to assess the control mechanisms by which the institution ensures the quality of implementation of those measures in respect of activities performed on its behalf by a third party.

terminating the contract, and the manner in which compliance with the contract is monitored,

- for monitoring and controlling the performance of activities carried out by the outsourcing provider, including practical testing of the performance of those activities;
- The institution has the professional capacity and powers needed to maintain control over the outsourced activity (inter alia, the institution has access to all relevant documents, understands the configuration of the IS/IT system provided and related procedures, and is able to influence the outputs);
- The institution has concluded outsourcing contracts in a manner that ensures controllability, enforceability and retainability;
- The institution’s internal regulations cover the activities of persons who perform customer identification and due diligence on its behalf and for its account, and the institution ensures that they receive training (in particular in relation to reliance on customer identification under Article 11(5) of the AML Act);
- Information, including copies of documents (obtained from customer identification and information on the intended transaction or business relationship, on the customer’s ownership and management structure and on the identity of the beneficial owner), is retained by the institution even where the identification was carried out by a person acting on behalf of the institution and who is bound by its internal regulations, and the institution remains responsible for these activities as if it had carried them out itself (in particular in relation to reliance on customer identification under Article 11(5) of the AML Act);
- The institution has agreed with the outsourcing provider on procedures for remedial measures and sanctions in the event of breaches or non-fulfilment of contractual conditions or failures on the part of the provider;
- The institution has a business continuity plan and, where relevant, an exit strategy.

Links to other assessed areas

- The assessment of outsourcing is linked to all audited areas in which the institution makes use of outsourcing.

Internal audit

- The activities of the internal audit function include an independent review of externally provided activities.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations;</i> • <i>Contracts with outsourcing providers used by the institution;</i> • <i>A risk analysis for outsourced activities;</i> • <i>Documents evidencing the selection and approval of the outsourcing arrangements used;</i> • <i>Documents relating to the exit strategy and business continuity plans;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system, including the configuration of access rights;</i> • <i>Interviews with relevant staff;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i>

- Documents evidencing controls carried out on the outsourcing provider and the outsourced activities;
- Reports from previous internal/external audits and compliance reports for the institution and the group, where available;
- The internal audit plan;
- The compliance monitoring plan;
- Reports on relevant supervisory investigations/inspections.

1.2.4. Internal control mechanisms

Legal requirements	
Control functions, mechanisms and procedures for control activities at all management and organisational levels, including ensuring that the relevant bodies and persons are informed	Articles 23, 46 and 48 of Decree No. 163/2014 Coll. and EBA/GL/2022/05
Internal mechanisms for ex-ante and ex-post assessment of the functioning and effectiveness of systems and procedures in the AML/CFT area, including the preparation, discussion and approval of the assessment report within the timeframe and scope laid down in legislation	Article 21(6) of the AML Act, Articles 19–21 of the AML Decree, Article 47(3) of Decree No. 163/2014 Coll. and EBA/GL/2022/05
Internal audit in the AML/CFT area, including internal IS/IT audit – scope, time limits, method of planning and focus	Article 49 of Decree No. 163/2014 Coll.
Implementation of, and follow-up to, the findings, recommendations and remedial measures arising from the CNB’s supervisory activities, and from internal and external audits and assessment reports	Article 19(4) of the AML Decree and Article 51 of Decree No. 163/2014 Coll.
Role and obligations of the management body and senior officers, and of the designated person; allocation of responsibilities relating to AML/CFT policies and procedures	Article 22a of the AML Act and EBA/GL/2022/05

Audit content

General governance and control mechanisms

- The institution has established in its internal regulations – and applies – internal control and communication procedures and strategies in the AML/CFT area, including mechanisms for assessing the effectiveness of those procedures and strategies;
- The institution has established in its internal regulations – and applies – procedures:
 - for monitoring compliance with legislation and the institution’s internal regulations, covering all of the institution’s activities in a comprehensive and interconnected manner,
 - for identifying and managing conflicts of interest and the associated risks,
 - for controlling the measures applied, in particular to prevent human error (four-eyes controls),
 - to ensure that the relevant bodies of the institution, their members and other staff and units have access to information for their decision-making that is up-to-date, reliable and comprehensive;

- The governing, control and advisory bodies are regularly informed of key and strategic matters in the AML/CFT area, in particular on the results of the risk assessment, the effectiveness of AML/CFT measures and compliance with AML/CFT legislation;
- The designated person²⁶ ensures that the management body is regularly informed about AML/CFT matters, that the management body is informed of all significant issues and breaches in this area, and that the AML/CFT compliance officer²⁷ has sufficient human and other resources at their disposal;
- The AML/CFT compliance officer ensures, in particular, that risk assessments are conducted, that the internal regulations are set appropriately and that compliance with them is monitored, that regular and complete reporting to the management body takes place, that suspicious transaction reports are submitted, and that training is provided;
- The key performance indicators (KPIs) of all staff with AML/CFT responsibilities correspond to their obligations in this area and ensure compliance with those obligations (including staff in business units responsible for customer identification and due diligence, the AML/CFT compliance officer and the designated person).

Assessment report

- When preparing the assessment report, the institution fulfils all formal requirements, in particular:
 - the institution prepares an assessment report at least once every 12 months, and that report is approved by the designated person,
 - the assessment report is prepared by the AML/CFT compliance officer, or it at least includes their opinion on its completeness and accuracy,
 - the assessment report is discussed by both the management and the supervisory bodies no later than by the end of the fourth calendar month following the end of the period to which it relates, and the relevant body responds thoroughly to the deficiencies and proposals identified in the report;
- The assessment report contains all required elements, in particular an assessment of whether the AML/CFT procedures and measures are sufficiently effective, whether any deficiencies have been identified in the institution's system of internal principles and what risks these deficiencies may pose for the institution, proposals for remedial measures, and statistical data and other key information relating to the AML/CFT area within the institution;
- The institution sets out in its internal regulations procedures for preparing and discussing the assessment report.

Internal audit

- The internal audit function regularly assesses the AML/CFT area or its components so that the area is covered in its entirety on a regular basis;
- The internal audit function assesses the effectiveness of AML/CFT systems and procedures, including the effectiveness of IS/IT systems and data quality;
- Internal audit staff have appropriate AML/CFT knowledge and receive training in this area;
- The institution's management body responds in an adequate manner to internal audit findings.

²⁶ The designated person under Article 22a of the AML Act.

²⁷ The AML/CFT compliance officer pursuant to Article 16(2) of the AML Decree.

Remediation of identified deficiencies

- The institution has established in its internal regulations – and applies – procedures requiring that any identified deficiencies and non-compliance are communicated appropriately to the relevant bodies, including ongoing information on the implementation of remedial measures.

Audit sources
<ul style="list-style-type: none"> <i>The institution's organisational rules;</i> <i>Relevant internal regulations of the institution;</i> <i>A list of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed;</i> <i>Minutes of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;</i> <i>The KPIs of relevant staff;</i> <i>Interviews with relevant staff, including internal audit staff;</i> <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> <i>Reports on compliance department reviews;</i> <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> <i>The internal audit plan;</i> <i>The compliance monitoring plan;</i> <i>Reports on relevant supervisory investigations/inspections;</i> <i>An overview of the implementation of all remedial measures adopted in response to supervisory, internal audit and external audit findings or other findings.</i>

2. Staffing and technical arrangements

2.1. Staffing

Legal requirements	
Selection and allocation of the duties and powers of the management body and the designated person in line with legislative requirements, including requirements for suitability and the segregation of incompatible functions	Article 22a of the AML Act, Article 16 of the AML Decree and EBA/GL/2022/05
Selection and allocation of the duties and powers of the AML/CFT compliance officer and the contact person in line with legislative requirements, including requirements for suitability and the segregation of incompatible functions	Article 22 of the AML Act and Articles 16 and 17 of the AML Decree
Staffing of the AML/CFT area – adequacy in relation to the nature, scale and complexity of the institution's activities, and processes for identifying, selecting and vetting staff involved in the institution's AML/CFT framework	Article 16(2) of the AML Decree and Article 17(3) and (4) of Decree No. 163/2014 Coll.

Audit content

- The institution has established in its internal regulations – and applies – procedures to ensure staffing resources that are adequate in relation to the nature, scale and complexity of the institution's activities;

- The institution regularly maps the scope and complexity of its activities in the AML/CFT area and assesses the staffing resources required;
- Where justified by the scope and nature of its activities, the institution has set up an independent AML/CFT unit reporting directly to the management body;
- The institution has established in its internal regulations – and applies – procedures for identifying incompatible functions and conflicts of interest and for managing the associated risks.
- The institution has defined the group of staff involved in AML/CFT activities;
- The institution has established in its internal regulations – and applies – procedures for selecting staff involved in AML/CFT activities, including the AML/CFT compliance officer and the designated person. These procedures in particular set out the requirements regarding the knowledge and experience needed in light of their job descriptions and positions, as well as the integrity and reliability required of relevant staff;²⁸
- The institution has formally appointed a member of the management body to ensure the fulfilment of AML/CFT obligations (the designated person); this person:
 - has sufficient AML/CFT knowledge and experience,
 - has sufficient time to perform this function,
 - is not responsible for other incompatible areas;
- The institution has appointed a specific staff member as the AML/CFT compliance officer; this person:
 - has sufficient AML/CFT knowledge and experience,
 - has sufficient time to perform this function,
 - is not responsible for other incompatible areas;
- The institution has appointed a specific staff member as the contact person responsible for ongoing communication with the FAU and has notified the FAU accordingly;
- The staff member responsible for assessing suspicious transactions has access to all necessary information and to the institution's information system;
- The KPIs of all staff and other persons with AML/CFT responsibilities correspond to their obligations in this area and ensure compliance with those obligations (including staff in business units responsible for customer identification and due diligence, the AML/CFT compliance officer and the designated person).

Links to other assessed areas

Internal control mechanisms

- The institution has established in its internal regulations – and applies – procedures to ensure the suitability of staffing in key AML/CFT functions, including the designated person, and for managing potential conflicts of interest;
- The designated person ensures that the AML function has sufficient staffing resources.

²⁸ EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT compliance officer under Article 8 and Chapter VI of Directive (EU) 2015/849 (EBA/GL/2022/05).

Training

- All relevant staff involved in AML/CFT activities, including the AML/CFT compliance officer and the designated person, are adequately trained.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>The institution's organisational structure (organisational chart) and the organisational placement of units and staff responsible for the AML/CFT risk-management framework;</i> • <i>The current organisational rules (including the responsibilities of individual units);</i> • <i>Job descriptions of staff involved in the AML/CFT system (role profiles), and of senior officers;</i> • <i>The KPIs of relevant staff;</i> • <i>The number of staff in the AML/CFT area and its development over time;</i> • <i>Minutes of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

2.2. Training

Legal requirements	
AML/CFT training – frequency, set of staff to be trained; scope and linkage to the institution's activities	Article 23 of the AML Act, Article 16(2)(c) of the AML Decree, EBA/GL/2022/05 and EBA/GL/2021/02
Training of third parties entrusted with carrying out AML/CFT activities	Article 23(2) of the AML Act

Audit content

- The institution has established in its internal regulations – and applies – procedures to ensure that AML/CFT training for relevant persons is:
 - always provided before a staff member is assigned to the relevant position, and
 - carried out regularly, at least once every 12 months;
- The institution has established in its internal regulations – and applies – procedures for identifying the relevant persons who must receive AML/CFT training, including at least:
 - all staff who may encounter suspicious transactions in the course of their duties,

- all staff involved in performing certain AML/CFT obligations (customer identification and due diligence, branch work, etc.),
 - all staff with control functions relevant to the AML/CFT area (e.g. internal audit staff);
 - all persons responsible for taking strategic and other key decisions in the AML/CFT area (in particular members of the management and supervisory bodies),
 - persons who are not in a standard employment relationship but who are involved in the institution's activities and may encounter suspicious transactions in the course of their work;
- The institution maintains records of attendance and the content of training, and retains them for at least five years after the training has taken place;
 - The scope and content of training cover all AML/CFT aspects relevant to the staff concerned (the institution ensures that staff receive specific training on all activities and risks relevant to the institution, such as international sanctions, trade finance, investment banking and cash operations) and staff are trained in all aspects relevant to the performance of their duties;
 - The content of training includes at least typologies and indicators of suspicious transactions, requirements for carrying out customer identification and due diligence, and procedures for identifying customer risk factors and suspicious transactions;
 - The content of training is up to date;
 - The AML/CFT assessment report includes a description of completed AML/CFT training and the training plan for the following year.

Links to other assessed areas

Internal control mechanisms

- All relevant staff involved in AML/CFT activities, including the AML/CFT compliance officer and the designated person, are adequately trained and therefore have the knowledge necessary to perform their function.

Staffing

- All relevant staff involved in AML/CFT activities, including the AML/CFT compliance officer and the designated person, are adequately trained.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>Training documentation (training content, presentations, tests);</i> • <i>The training plan;</i> • <i>A list of training sessions held, including attendance records;</i> • <i>An overview of all staff and other relevant persons indicating the training they have attended and the dates of their attendance, including:</i> <ul style="list-style-type: none"> ○ <i>new staff,</i> ○ <i>existing staff,</i> ○ <i>staff subject to training on specific areas,</i> ○ <i>members of governing bodies,</i> ○ <i>persons involved in the activities of the obliged entity on the basis of arrangements other than an employment contract;</i> • <i>Interviews with relevant staff;</i>

- *Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

2.3. Technical arrangements and data quality

Legal requirements	
Technical arrangements for the AML/CFT area – adequacy in relation to the nature, scale and complexity of the institution’s activities	Articles 17 and 17b of the AML Decree

Audit content

- The institution has established in its internal regulations – and applies – procedures to ensure technical arrangements that are adequate in relation to the nature, scale and complexity of the institution’s activities;
- The institution regularly maps the scope and complexity of its activities in the AML/CFT area and assesses the technical arrangements required;
- Access to information relevant for identifying and assessing ML/FT suspicions is ensured by automated means, unless this would not be proportionate;
- The institution has the professional capacity and powers needed to maintain control over the IS/IT systems it uses (inter alia, the institution has access to all relevant documentation, understands the configuration of the IS/IT system provided and related procedures, and is able to influence the outputs);
- The institution has established in its internal regulations – and applies – procedures to ensure data integrity and data quality, including the implementation of appropriate control mechanisms (such as four-eyes controls) and the allocation of responsibilities and obligations to the relevant staff;
- The institution has established in its internal regulations – and applies – procedures to ensure that relevant data enter all relevant IS/IT systems and that data integrity is not compromised during their transmission.

Links to other assessed areas

- The quality and adequacy of the technical arrangements are linked with the fulfilment of obligations in all AML/CFT areas.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>An assessment of the adequacy of the IS/IT systems used;</i> • <i>Interviews with relevant staff;</i> • <i>Job descriptions of relevant staff;</i> • <i>The KPIs of relevant staff;</i>

- The budget for IS/IT equipment in the AML/CFT area;
- Documentation on, and the actual configuration of, the relevant IS/IT systems;
- Data quality control statistics;
- Minutes of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;
- Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;
- Reports from previous internal/external audits and compliance reports for the institution and the group, including IS/IT audits of AML systems, where available;
- The internal audit plan;
- The compliance monitoring plan;
- Reports on relevant supervisory investigations/inspections.

3. Customer identification and due diligence

3.1. Customer identification and due diligence for a transaction or at the start of a business relationship

Legal requirements	
Initial customer identification – the types of identification used and exemptions; the set of information collected; identification of other relevant persons; verification of identity, etc.	Articles 4(1)–(4), 5, 7–8a, 9a–13a and 21(5) of the AML Act, Article 14 of the AML Decree, EBA/GL/2023/04, EBA/GL/2021/02, FAU Methodological Instruction No. 9 and FAU Methodological Instruction No. 8
Customer due diligence, including verification from reliable sources – determination of the purpose and intended nature of the business relationship; the origin of funds and assets; the ownership and management structure, including the beneficial owner, etc.	Articles 4(4) and 9 of the AML Act, Articles 8 and 11 of the AML Decree, EBA/GL/2023/04, EBA/GL/2022/15, EBA/GL/2021/02, FAU Methodological Instruction No. 9 and FAU Methodological Instruction No. 3
Procedures for accepting and rejecting transactions/business relationships	Article 15 of the AML Act, Article 8(2) of the AML Decree and EBA/GL/2023/04

Audit content

Customer identification for a one-off transaction or at the start of a business relationship

- The institution has established in its internal regulations – and applies – procedures specifying in which situations and for which persons customer identification is carried out, in accordance with legislative requirements;
- The institution has established in its internal regulations the methods of identification it uses, and procedures ensuring that the statutory requirements for using these methods are fulfilled, in particular when using mediated identification, reliance on identification, remote identification, etc. The institution applies these procedures in practice;

- Where the institution relies on identification by means of a first payment, it has prepared a risk assessment of this approach and a risk assessment of the countries from which such identification is accepted;
- The institution has established in its internal regulations the content of customer identification (the set of identification data), in accordance with legislative requirements;
- The institution has established in its internal regulations – and applies – procedures governing the individual steps taken during customer identification, including detailed allocation of the duties and responsibilities of specific staff, in accordance with legislative requirements;
- The institution has established in its internal regulations – and applies – procedures for identifying connected transactions for the purpose of determining situations requiring customer identification and due diligence;
- The institution has established in its internal regulations – and applies – procedures for managing ML/FT risks in a manner that is non-discriminatory and does not assume a refusal to establish business relationships with, or a blanket rejection of, entire groups of customers.

Customer due diligence for a one-off transaction or at the start of a business relationship

- The institution has established in its internal regulations – and applies – procedures specifying in which situations and for which persons customer due diligence is carried out, in accordance with legislative requirements;
- The institution has established in its internal regulations the content of customer due diligence, in accordance with legislative requirements (in particular the set of information obtained on the purpose and nature of the transaction or business relationship, the nature of the customer's business and the consistency of the customer's transactions with that information, and information on the beneficial owner, the ownership and management structure, and the source of funds or assets);
- The definition of the beneficial owner and the method for determining the beneficial owner correspond to legislative requirements and related interpretative materials;
- The institution has established in its internal regulations the documents it obtains during customer due diligence to evidence the relevant facts, including assessments of their reliability.

Exemptions from customer identification and due diligence

- The institution has established in its internal regulations the situations in which it is not required to perform customer identification and due diligence (exemptions from this obligation), in accordance with legislative requirements.

General

- The institution has established in its internal regulations – and applies – procedures for not executing a transaction and not establishing a business relationship, and for terminating a business relationship with a customer.

Procedures in practice

- The institution performs customer identification and due diligence in accordance with its internal regulations and legislation, in particular:
 - it holds the necessary set of information,
 - it verifies information from reliable sources,

- it has implemented measures to ensure best efforts are made to obtain all relevant information (e.g. all countries of origin and all business activities),
- when conducting customer due diligence, it consistently obtains and assesses information on the purpose and intended nature of the transaction/business relationship and on the source of funds;
- Customer information is recorded in the institution’s relevant systems;
- The institution records which staff member carried out the customer identification and due diligence, including the manner in which it was performed;
- The institution’s system enables the ex-post reconstructability of approval and decision-making processes and of control activities;
- The institution has in place control mechanisms verifying that all key fields in the IT system are completed with accurate and complete information;
- The institution has defined responsibility for the quality, completeness and timeliness of customer identification and due diligence data, including the relevant enforcement mechanisms (e.g. the KPIs of relevant staff).

Links to other assessed areas

Information retention

- The institution has established in its internal regulations – and applies – procedures for retaining information obtained from customer identification and due diligence in a manner that enables the reconstructability of the process carried out, including specifying the method of identification used and the responsible person.

Internal control mechanisms

- The institution has implemented control mechanisms for the quality of customer identification and due diligence (e.g. random compliance checks and automated controls with corresponding reports).

Training

- The relevant staff of the institution responsible for carrying out customer identification and due diligence are adequately trained in the AML/CFT area.

Risk-based approach to identification and due diligence

- The institution has established in its internal regulations – and applies – procedures to ensure that the manner in which customer identification and due diligence are carried out corresponds to the identified risk.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>The risk assessment, including an analysis of the risks associated with the identification methods used;</i> • <i>An aggregated overview of the customer portfolio;</i> • <i>A sample of customer files according to the different identification methods used;</i> • <i>A sample of customer files for which an exemption from customer identification was applied;</i> • <i>A sample of customer files relating to one-off transactions (e.g. cash transactions);</i>

- Interviews with the responsible staff carrying out or responsible for carrying out customer identification and due diligence, and the control thereof (front office, account managers, compliance, etc.);
- An overview of refused transactions/business relationships;
- The IT systems used to maintain customer data and customer profiles;
- An overview of the control mechanisms in place;
- An overview of the results of checks performed (e.g. reports generated);
- The KPIs of relevant staff;
- The content of training sessions for relevant staff;
- Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;
- Reports from previous internal/external audits and compliance reports for the institution and the group, where available;
- The internal audit plan;
- The compliance monitoring plan;
- Reports on relevant supervisory investigations/inspections.

3.2. Risk-based approach to customer identification and due diligence

Legal requirements	
Rules and procedures according to which, at the start and during the course of a business relationship, the institution determines and updates the customer's risk profile – effectiveness and consideration of legislative requirements and the risks to which the institution is exposed	Articles 9a and 21a of the AML Act, Article 3(1)(b) and (c) and Articles 6–9 of the AML Decree, EBA/GL/2023/04, EBA/GL/2021/02 and Supervisory Benchmark No. 4/2022
Approach to customers in line with the identified risk, including procedures for enhanced customer identification and due diligence	Articles 9(3) and 9a of the AML Act and Articles 6(b), 8 and 9 of the AML Decree

Audit content

Determination of the risk category

- The institution has established in its internal regulations – and applies – procedures according to which, at the start and during the course of a business relationship, it determines and updates the customer's risk profile. These rules and procedures:
 - correspond to the risks that may arise within the institution's activities, as identified in the institution's risk assessment,
 - take into account the results of the national risk assessment of the Czech Republic, the EU supranational risk assessment, factors indicating potentially higher risk, and other available information,
 - take into account all relevant risk factors required by legislation,
 - take into account all relevant information available about the customer, including the type, legal form and country of origin of the customer, the purpose, regularity and duration of the business relationship or transaction outside a business relationship, the type of product or service used, the value and method of execution of the

transaction, the riskiness of the countries or geographical areas to which the transactions or persons connected with the business relationship relate, and negative information about the customer,

- ensure that the method for calculating the risk profile genuinely reflects the identified risks, in particular that higher risk is assigned where higher risk is required by legislation (in customer categorisation, the weighting of factors does not lead to an unjustified predominance of one factor or, conversely, to dilution and thus, for example, insufficient consideration of mandatory higher-risk factors);
- The institution has established in its internal regulations – and applies – procedures to ensure that transactions/business relationships involving higher-risk factors under legislation (e.g. a high-risk country of origin or a sanctions element) are always assigned to a higher-risk category;
- The institution has established in its internal regulations – and applies – procedures for analysing publicly available information on its customers, for appropriately assessing the relevant risks, and for reflecting those risks in the measures applied to the customer;
- The institution has established in its internal regulations the situations requiring a review and, where necessary, an update of the risk category, and acts accordingly; at a minimum, changes in the risk level of individual factors are taken into account;
- The institution has established in its internal regulations – and applies – sufficiently specific and instructive procedures for determining risk to ensure that the staff member applying them can clearly determine how to proceed, in particular for factors that are assessed manually (e.g. negative information and the reliability of documents);
- The institution applies procedures from the technical point of view in a manner that is proportionate to its size and activities; where proportionate, updates to the risk profile thus take place automatically;
- Where the risk category is adjusted manually, the action is recorded in a reconstructable manner, including justification, identifying at a minimum who made the change, how and why;
- Where the institution uses an automated system to assess customer risk, it has the ability, in justified cases, to override the automated risk assessment.

Approach to customers in line with the identified risk

- The institution has established in its internal regulations – and applies – procedures that ensure that, in line with the risks identified, the measures applied manage the specific risks identified;
- The institution has established in its internal regulations – and applies – procedures to ensure that, for transactions/business relationships where legislation requires enhanced customer due diligence (e.g. high-risk country of the transaction or high-risk business activity), additional measures are always applied, at least those measures required by legislation;
- The institution has established in its internal regulations – and applies – procedures for carrying out enhanced customer identification and due diligence in cases of higher risk, including:
 - specific additional measures going beyond standard identification and due diligence are defined, and these measures differ for individual risk categories;
- The institution has established in its internal regulations the situations in which simplified customer identification and due diligence are applied, and these situations are duly supported by a risk analysis and are in accordance with legislation;

- The institution has established in its internal regulations – and applies – procedures for managing risk which are sufficiently specific and instructive to ensure that the staff member applying them can clearly determine how to proceed.

Links to other assessed areas

Risk assessment

- The institution has identified and assessed the ML/FT risks that may arise in its activities, including geographical risk and the risk relating to the customer’s business activity, and these risks are reflected in the procedures for the risk-based approach towards customers; the institution regularly and continuously monitors publicly available information for the purpose of identifying risks relevant to its activities and takes them into account both at the level of the institution’s risk assessment and for individual relevant customers.

Control mechanisms

- The institution has implemented controls over the correctness of the risk assessment and controls over manual inputs.

Training

- The staff responsible for carrying out customer risk categorisation and for applying the follow-up measures are adequately trained.

PEP

- The PEP risk factor is taken into account and appropriate follow-up measures are applied;

Ongoing customer identification and due diligence

- The procedures for the risk-based approach towards customers are applied on an ongoing basis throughout the business relationship.

Audit sources
<ul style="list-style-type: none"> • <i>Internal regulations, including methodologies for calculating the risk category and for making changes to the risk category;</i> • <i>The risk assessment;</i> • <i>A list of countries with assigned risk levels, including the methodology for its preparation;</i> • <i>A list of business activities with assigned risk levels, including the methodology for its preparation;</i> • <i>A list of legal forms with assigned risk levels, including the methodology for its preparation;</i> • <i>Documentation of the preparation of the risk assessment, including lists, updates thereto and the allocation of responsibilities in the process;</i> • <i>An aggregated overview of the customer portfolio indicating the risk factors and the risk category;</i> • <i>A sample of customer files reflecting the different risk categories and individual risk factors, including at least:</i> <ul style="list-style-type: none"> ○ <i>cases where enhanced customer identification and due diligence were applied,</i> ○ <i>cases where simplified customer identification and due diligence were applied,</i> ○ <i>customers flagged as PEPs, with a high-risk business activity, or with a high-risk country of origin;</i> • <i>An aggregated overview of all changes to risk factors and to the risk category;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i> • <i>The content of training sessions for relevant staff;</i>

- *Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

3.3. Ongoing customer identification and due diligence

Legal requirements	
Ongoing customer due diligence – carrying out updates of customer identification and due diligence, and reassessing the customer’s risk profile; time limits and method	Article 8(9) of the AML Act, Articles 7(3) and 10(2) of the AML Decree, EBA/GL/2023/04, EBA/GL/2022/15, EBA/GL/2021/02 and Supervisory Benchmark No. 4/2022

Audit content

- The institution has established in its internal regulations – and applies – procedures for carrying out ongoing customer identification and due diligence, specifically
 - maximum regular intervals are set for updating the customer’s risk profile, and these rules apply to every customer,
 - rules and procedures are in place for verifying the validity and completeness of information held and obtained during the business relationship and during other transactions,
 - the scope and content of ongoing customer identification and due diligence is defined in a manner that includes all components required by legislation (including information beyond identification data, in particular information on the purpose and intended nature of the business relationship and information on the source of funds),
 - the scope and content of ongoing customer identification and due diligence takes into account the related risks.
- The institution has established in its internal regulations – and applies – procedures for verifying the justification for simplified customer due diligence and for exemptions from customer identification and due diligence;
- The institution has established in its internal regulations – and applies – procedures to ensure that, when there is a change in AML/CFT legislation, it verifies whether the information held on customers still meets the requirements of the new legislation and, where necessary, ensures remediation;
- Any automated execution of ongoing customer due diligence or parts thereof is supported by justification explaining how the ongoing customer due diligence process as a whole ensures the complete fulfilment of the content, meaning and purpose of ongoing identification and due diligence (in particular how truthful and complete updates of all relevant information, not only identification data, are ensured);

- The institution has established in its internal regulations responsibility for carrying out ongoing customer identification and due diligence and for ensuring the correct status thereof, including the relevant enforcement mechanisms (e.g. the KPIs of relevant staff);
- The institution has established in its internal regulations – and applies – procedures ensuring that the established time limits are met in a timely manner, in particular through timely alerts and successive escalation steps;
- The institution has established in its internal regulations – and applies – control mechanisms regarding compliance with established time limits and procedures for carrying out ongoing customer due diligence;
- The institution reviews the customer’s risk profile in a manner that enables the reconstructability of the assessments performed, including justification;
- The institution has established in its internal regulations – and applies – procedures for situations where it is not possible to carry out ongoing customer identification and due diligence, in particular with regard to blocking the customer’s ability to dispose of funds or potential off-boarding.

Links to other assessed areas

Information retention

- Ongoing customer due diligence is carried out in a reconstructable manner and all justifications are duly retained.

Customer identification and due diligence

- The institution ensures that all information is available and up to date to the extent required by legislation.

Risk-based approach to the customer

- The frequency, content and scope of ongoing customer due diligence correspond to the identified risks.

Transaction monitoring

- The institution reflects risk factors and categories in the configuration of transaction monitoring scenarios.

Audit sources
<ul style="list-style-type: none"> • <i>The internal regulations of the institution;</i> • <i>An aggregated overview of customers indicating the date of the customer’s risk category and the date of the last customer due-diligence review;</i> • <i>A sample of customer files reflecting the different risk categories;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system, including the configuration of access rights and the retention of information on changes made;</i> • <i>An overview of the control mechanisms in place;</i> • <i>An overview of the results of the controls applied (e.g. reports generated, reports for the institution’s management);</i> • <i>The KPIs of relevant staff;</i> • <i>The content of training sessions for relevant staff;</i> • <i>Interviews with relevant staff;</i>

- Reports from previous internal/external audits and compliance reports for the institution and the group, where available;
- The internal audit plan;
- The compliance monitoring plan;
- Reports on relevant supervisory investigations/inspections.

3.4. Politically exposed persons

Legal requirements	
Procedures for identifying politically exposed persons (PEPs) when conducting a transaction, when establishing a business relationship and during its course	Articles 4(5), 8(8) and 54(8) of the AML Act
Specific measures applicable to PEPs, including determining the PEP's assets, commensurate with risk	Articles 9, 9a and 15 of the AML Act, Article 9 of the AML Decree, EBA/GL/2021/02 and FAU Methodological Instruction No. 7

Audit content

- The institution applies measures to PEPs in line with the risk-based approach;
- The institution has established in its internal regulations – and applies – a definition of a PEP that is in accordance with legislative requirements;
- The institution has established in its internal regulations – and applies – procedures for identifying PEPs as customers and as beneficial owners of customers (together “PEPs”) in accordance with legislative requirements, including:
 - the use of appropriate tools for identifying PEPs (proportionate to the size of the institution and the scope of its activities),
 - the application of procedures for identifying PEPs before establishing a business relationship or executing a one-off transaction,
 - the setting of appropriate time intervals for the ongoing review of PEP status in existing business relationships;
- The institution has established in its internal regulations – and applies – procedures for identifying and assessing the risk associated with PEPs, on the basis of which the institution assigns a PEP a risk profile within the appropriate higher-risk category; this process should be automated where proportionate to the size and scope of the institution's activities; the institution assigns a risk profile that corresponds to the specific risk presented by the customer, the products used and the business relationship;
- The institution has established in its internal regulations the measures it applies to PEPs; at a minimum, in addition to standard customer identification and due diligence, it applies the measures required by legislation (determination of the source of wealth, approval by the institution's management, etc.); the institution applies this enhanced due diligence in a manner and to an extent that correspond to the specific risk identified in the relevant business relationship, in particular taking into account the nature of the customer and the services and products provided;

- Relevant staff are adequately trained; in particular, where customer declarations are used as a supporting source of information, customer-facing staff are adequately familiar with the definition of a PEP and the risks associated with PEPs.

Links to other assessed areas

Customer identification and due diligence

- The institution collects all relevant information about the customer.

Risk-based approach to the customer

- The institution assigns an appropriate risk category to PEPs and applies proportionate follow-up measures.

Transaction monitoring

- The institution adequately reflects the risks associated with PEPs in the configuration of transaction monitoring scenarios.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i> • <i>An aggregated overview of the customer portfolio indicating the PEP flag and the risk category;</i> • <i>A sample of customer files where:</i> <ul style="list-style-type: none"> ○ <i>the customer is a PEP;</i> ○ <i>the customer's beneficial owner is a PEP;</i> • <i>The content of AML/CFT training;</i> • <i>The template for PEP declarations for customers, where used;</i> • <i>Interviews with relevant staff, including customer-facing staff (front desk);</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

4. Transaction monitoring and reporting of suspicious transactions

4.1. Transaction monitoring

Legal requirements	
Configuration of transaction monitoring scenarios – compliance with legislation and the institution's ML/FT risk assessment; the set of activities of the institution covered, including the appropriateness of the way any whitelists ²⁹ are used	Articles 6, 9(2)(d) and 21(5)(a) of the AML Act and Supervisory Benchmark No. 2/2023
Monitoring systems – generation of alerts when thresholds and conditions set in scenarios are met	Articles 6, 9(2)(d) and 21(5) of the AML Act, Article 17b of the AML Decree and Supervisory Benchmark No. 2/2023

²⁹ By whitelists we mean internal lists of entities that are automatically excluded from monitoring.

Time limits for generating alerts	Article 17a of the AML Decree and Supervisory Benchmark No. 2/2023
-----------------------------------	--

Audit content

Configuration of scenarios

- The institution has established in its internal regulations – and applies – transaction monitoring scenarios that:
 - are set in accordance with the risk assessment,
 - take into account and manage all relevant risks to which the institution is exposed,
 - reflect the allocation of risk categories, and
 - ensure coverage of all relevant typologies;
- The institution has established in its internal regulations – and applies – thresholds for scenarios that are justified by a risk analysis and are relevant to the customer segment, the product or service used, the risk category and the type of transactions to which they apply;
- Transaction monitoring covers all products and services offered and all customer segments;
 - The institution has established in its internal regulations – and applies – procedures for creating, approving and reviewing whitelists (where used); these procedures are in accordance with the risk assessment, reviews are conducted at frequent, justified regular intervals and are reconstructable, and there are control mechanisms in place for applying them (e.g. four-eyes checks, approval by a superior);
- The institution regularly conducts an analysis of the configuration of transaction monitoring scenarios in order to assess their effectiveness.

Generation of alerts

- The institution has established in its internal regulations – and applies – rules for generating alerts, including time limits for generating alerts, in a manner that ensures that alerts are generated without delay after the substantive criteria for their generation have been met and as close as possible to the actual date of execution of the transaction/trade (in a manner commensurate with the ML/FT typology monitored);
- Any aggregation of values across several alert-generation scenarios is underpinned by an analysis justifying that such an approach does not result in risk situations being missed;
- The IS/IT system used for transaction monitoring generates alerts when the conditions set in the scenarios are met.

Technical solution

- The technical solution used is appropriate to the size and nature of the institution's activities;
- All relevant information available to the institution feeds into transaction monitoring and is available in a clear manner to relevant staff;
- Relevant staff understand how the technical solution for transaction monitoring is configured;
- The technical solution for transaction monitoring provides an audit trail for decision-making processes;
- The quality of the IS/IT environment used for transaction monitoring is verified on a regular basis.

Manual monitoring

- Where the institution uses manual transaction monitoring for certain areas of activity, it has established in its internal regulations – and applies – procedures:
 - for carrying out such manual monitoring, including criteria for identifying whether a suspicion exists, and
 - defining the responsibilities of relevant staff tasked with carrying out manual transaction monitoring;
- Relevant staff are adequately trained; in particular, where staff from units other than compliance are used for first-line monitoring (e.g. staff in investment or lending departments), they receive adequate training on AML/CFT risks and obligations.

Links to other assessed areas

Risk assessment

- In configuring transaction monitoring, the institution relies on the risks identified in the risk assessment and manages those risks accordingly.

(Ongoing) customer identification and due diligence

- The institution holds all relevant information on the customer.

Risk-based approach to customers

- The institution configures transaction monitoring scenarios taking into account risk factors and categories.

Investigation of generated alerts and follow-up procedures in the event of suspicion

- The analysis of the effectiveness of transaction monitoring covers the transaction monitoring system as a whole;
- The institution has an effective process in place for investigating generated alerts, ensuring that they are properly reviewed in order to identify any suspicion.

Audit sources³⁰

- *Internal regulations, including:*
 - *an overview of scenarios,*
 - *a description of scenarios and their thresholds,*
 - *justification for the scenarios;*
- *Documentation on the configuration of scenarios, thresholds and changes thereto;*
- *An analysis of the effectiveness of the configuration of transaction monitoring and individual scenarios;*
- *An overview of all alerts, including relevant information (date and time of generation, scenario, transaction monitoring system – where more than one system is used for monitoring transactions);*
- *A sample of alerts from all transaction monitoring systems (including areas where transaction monitoring is performed manually);*
- *A sample of transactions that meet the criteria for generating an alert;*

³⁰ Where deeper verification is required, the transaction monitoring system may also be tested using artificially created transactions corresponding to the typologies identified in the risk assessment, in order to verify whether they would be detected.

- *An analysis of false positive alerts in the context of the effectiveness of transaction monitoring and the use of resources;*
- *Documentation on, and the actual configuration of, the relevant IS/IT system;*
- *Interviews with relevant staff and senior officers;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

4.2. Investigation of generated alerts

Legal requirements	
Procedures and processes for assessing and investigating alerts – configuration and effectiveness	Articles 6, 9(2)(d) and 18 of the AML Act, Articles 17, 17a and 17b of the AML Decree and Supervisory Benchmark No. 2/2023

Audit content

- The institution has established in its internal regulations – and applies – procedures for assessing and investigating alerts, including assessing whether a suspicion exists;
- The institution has established in its internal regulations – and applies – responsibilities and decision-making powers relating to the investigation of alerts, in particular where alerts are investigated at several levels;
- The institution has established in its internal regulations – and applies – procedures for prioritising the investigation of alerts, in particular taking account of risk;
- The institution has established in its internal regulations – and applies – procedures to ensure the quality and depth of investigations of alerts and the scope of required explanations and justifications, including control mechanisms (e.g. regular reports), regular analyses and the allocation of responsibilities to relevant staff;
- The institution has established in its internal regulations – and applies – procedures to ensure the timely investigation of alerts, including control mechanisms (e.g. regular reports), regular analyses and the allocation of responsibilities to relevant staff;
- Where more than one solution is used for transaction monitoring, all information is available in a clear manner to relevant staff across systems;
- The IS/IT system(s) used allow access to the information necessary to investigate alerts in a way that ensures rapid and clear searching and display of information, enabling effective investigation of alerts;
- The institution has established in its internal regulations – and applies – procedures for documenting the process and outcomes of investigations of alerts to ensure that they are reconstructable;
- The institution has established in its internal regulations – and applies – procedures for dealing with customers during the period in which necessary information is being obtained from them (in particular with regard to assessing the length of any delay, unusual customer behaviour and the riskiness of the situation).

Links to other assessed areas

(Ongoing) customer identification and due diligence

- The institution holds all relevant information on the customer.

Risk-based approach to customers

- The institution takes into account risk factors and categories when prioritising the investigation of alerts.

Transaction monitoring

- The analysis of the effectiveness of transaction monitoring covers the transaction monitoring system as a whole;
- The institution has an effectively configured system for identifying unusual transactions, including ensuring that alerts are generated in a timely manner.

Audit sources
<ul style="list-style-type: none"> • <i>Internal regulations;</i> • <i>An analysis/reports on the effectiveness of transaction monitoring;</i> • <i>An overview of generated alerts, including the date and time the alert was generated and closed, the manner and justification for its resolution, and the person responsible for resolving the alert;</i> • <i>A sample of generated alerts, including related relevant information (e.g. the institution's communication with the customer, and documentation on the transaction provided by the customer);</i> • <i>Reports for the institution's management containing information on transaction monitoring;</i> • <i>An overview of control mechanisms;</i> • <i>The KPIs of relevant staff;</i> • <i>Information on the training of relevant staff;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i> • <i>Interviews with relevant staff;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

4.3. Follow-up procedures where a suspicion is identified

Legal requirements	
Procedures for the timely reporting of suspicious transactions	Articles 6, 9b, 18 and 19 of the AML Act
Procedures for meeting the substantive requirements for suspicious transaction reports	Article 18 of the AML Act
Procedures for postponing the execution of a customer's order	Article 20 of the AML Act

Procedures for following up on the identification and reporting of a suspicion, with regard to the approach towards the relevant customer	Article 7(6) of the AML Decree
---	--------------------------------

Audit content

- The institution has established in its internal regulations – and applies – procedures for submitting suspicious transaction reports to the FAU; these procedures ensure at least that:
 - suspicious transaction reports are submitted without delay,
 - the substantive requirements for suspicious transaction reports are met, and
 - confidentiality is maintained in respect of all matters relating to suspicious transaction reports;
- The institution has established in its internal regulations – and applies – procedures for determining situations in which it is necessary to postpone the execution of a customer’s order, and follow-up procedures, including time limits;
- The institution has established in its internal regulations – and applies – responsibilities and decision-making powers in the process of identifying and reporting suspicious transactions and of postponing the execution of a customer’s order, including follow-up procedures;
- The institution retains all documents and records relating to decisions taken in the context of reporting suspicious transactions in a manner that ensures that they are reconstructable;
- The institution has established in its internal regulations – and applies – procedures for not performing customer due diligence where this could frustrate or jeopardise the investigation of a suspicious transaction (tipping-off), including the submission of the related suspicious transaction report and follow-up procedures vis-à-vis the customer after its submission;
- The institution has established in its internal regulations – and applies – procedures ensuring that an identified suspicion is adequately reflected in the customer relationship and in follow-up measures vis-à-vis the customer across all its business relationships and across related business relationships.

Links to other assessed areas

Customer identification and due diligence

- The institution has anti-tipping-off procedures and follow-up procedures in place.

Transaction monitoring and investigation of generated alerts

- The institution has an effective system in place for detecting suspicions.

Follow-up procedures where a sanctions element is identified

- The identification of a sanctions element is always reported to the FAU as a suspicious transaction.

Audit sources
<ul style="list-style-type: none"> • <i>Internal regulations;</i> • <i>A sample of suspicious transaction reports;</i> • <i>A sample of suspicious transaction reports for which the execution of the order was postponed;</i>

- *An aggregated overview of the customer portfolio indicating the risk category and whether a suspicious transaction report was submitted in relation to the customer;*
- *A sample of customer files where a suspicious transaction report was submitted in relation to the customer;*
- *Documentation on, and the actual configuration of, the relevant IS/IT system;*
- *Interviews with relevant staff;*
- *Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

5. Implementation of sanctions measures

5.1. Identification of sanctions elements

Legal requirements	
Procedures for identifying sanctions elements; the set of international sanctions taken into account, including sanctions lists	Article 2 of Act No. 69/2006 Coll., Articles 6(2), 8(8), 9(2) and 21 of the AML Act, Article 12 of the AML Decree, FAU Methodological Instruction No. 5 and Supervisory Benchmark No. 2/2018
Subjects of sanctions screening – the set of persons; types of fields in payment messages and payment systems screened (SWIFT, SEPA and CERTIS)	Article 6(2) of the AML Act, Article 12 of the AML Decree and Supervisory Benchmark No. 2/2018
Investigation of alerts of potential matches with sanctions lists generated by the information system – method, time limits, effectiveness	Article 12 of the AML Decree and Supervisory Benchmark No. 2/2018

Audit content

- The institution has established in its internal regulations – and applies – comprehensive procedures for implementing relevant international sanctions;
- The institution has established in its internal regulations – and applies – procedures for determining, updating and implementing all directly applicable sanctions lists (the institution uses all directly applicable lists in their current versions); these procedures proceed without delay;
- The institution has established in its internal regulations – and applies – procedures for detecting entities listed on sanctions lists (sanctions screening); these procedures ensure that:
 - entities listed on sanctions lists are always detected when a list is amended,

- entities listed on sanctions lists are always detected when there is a change in relevant persons in the institution's portfolio or before a business relationship is established/a one-off transaction is executed,
- screening is carried out in all relevant processes (including one-off transactions, payments, cash transactions and the establishment of business relationships) and for all relevant persons (the customer, the beneficial owner, persons in the ownership structure, authorised representatives, transaction counterparties, persons in supplier-customer relationships vis-à-vis the institution, etc.),
- the established processes proceed without delay;
- The institution has established in its internal regulations – and applies – procedures for investigating alerts or otherwise identified potential matches with sanctions, and a process for deciding whether or not a match has been identified;
- The institution has established in its internal regulations – and applies – procedures that follow up on the identification of a match with sanctions lists; these procedures always fulfil at least the requirements laid down in legislation, ensuring that:
 - no funds are made available (all funds are blocked),
 - a suspicious transaction report is submitted to the FAU,
 - a risk factor is applied;
- The institution has established in its internal regulations – and applies – the responsibilities and obligations of staff in procedures relating to international sanctions;
- The institution has established in its internal regulations – and applies – procedures for implementing international sanctions across all of its business activities, including, for example, cash desks and other one-off transactions;
- The institution has established in its internal regulations – and applies – procedures for implementing all non-name-based sanctions;
- The institution has established in its internal regulations – and applies – procedures for implementing international sanctions in a manner that ensures that individual processes are documented and reconstructable;
- The institution has an appropriate and sufficient technical solution for implementing international sanctions in a manner commensurate with the size and nature of its activities, where:
 - this technical solution ensures that all relevant information is processed,
 - relevant staff understand how it is configured and are able to influence that configuration adequately,
 - the technical configuration adequately ensures that the system is effective (for example, the configuration of fuzzy logic does not adversely affect the effectiveness of detecting relevant persons);
- The institution has sufficient staffing capacity to implement international sanctions and has established procedures to ensure that all relevant staff possess appropriate expertise specifically in the area of international sanctions (including, for example, cash desk staff).

Links to other assessed areas

Customer identification and due diligence at the start of and during a business relationship

- The institution holds all necessary information about customers and other relevant persons.

Follow-up procedures where a sanctions element is identified

- The institution has in place comprehensive procedures for implementing international sanctions, from the detection of sanctions elements through to the application of follow-up procedures.

Audit sources
<ul style="list-style-type: none"> • <i>Internal regulations;</i> • <i>A list of international sanctions implemented</i> • <i>A list of amendments to the sanctions list used and the dates of those amendments;</i> • <i>An overview of sanctions alerts;</i> • <i>A sample of sanctions alerts;</i> • <i>Records of investigations carried out and decisions taken, including justifications;</i> • <i>Testing of the customer portfolio/transactions against sanctions lists (system testing in a test environment using artificially created customers/transactions), including verification of the configuration of fuzzy logic;</i> • <i>Agreements with the provider of the commercial solution;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i> • <i>The content of training sessions for relevant staff, and a list of training sessions and their participants;</i> • <i>Interviews with relevant staff, including staff implementing non-name-based sanctions, cash desk staff, etc.;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

5.2. Follow-up procedures where a sanctions element is identified

Legal requirements	
Procedures for complying with the statutory reporting obligation	Article 10 of Act No. 69/2006 Coll., Articles 6(2) and 18 of the AML Act and FAU Methodological Instruction No. 4
Rules and procedures for further steps vis-à-vis the customer where a positive match is identified	Articles 10 and 11 of Act No. 69/2006 Coll., Articles 6(2) and 18 of the AML Act, Articles 9 and 12 of the AML Decree and FAU Methodological Instruction No. 1

Audit content

- The institution has established in its internal regulations – and applies – procedures to be followed when a sanctions element is identified;

- The institution has established in its internal regulations – and applies – procedures to be followed when a sanctions element is identified for submitting a suspicious transaction report to the FAU, including its formal requirements and the information it must contain;
- The institution has established in its internal regulations – and applies – the obligations, competences, decision-making roles and responsibilities of relevant staff, including measures to ensure their expertise and knowledge.

Links to other assessed areas

Follow-up procedures where a suspicion is identified

- The identification of a sanctions element is always reported to the FAU as a suspicious transaction.

Identification of sanctions elements

- The institution has in place comprehensive procedures for implementing international sanctions, from the detection of sanctions elements through to the application of follow-up procedures.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>A sample of customers for which a sanctions element has been identified;</i> • <i>A sample of sanctions alerts (true and false hits) and how they were handled;</i> • <i>The content of training sessions for relevant staff, and a list of training sessions and their participants;</i> • <i>Interviews with relevant staff, including staff implementing non-name-based sanctions, cash desk staff, etc.;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

6. Other

6.1. Correspondent banking

Legal requirements	
Prohibition on engaging in correspondent relationships with shell banks ³¹ (directly or indirectly) and institutions that do not apply AML/CFT measures at least equivalent to the requirements under EU law	Article 25(1) of the AML Act

³¹ An institution that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Procedures for obtaining and updating information relating to the correspondent relationship	Article 25(2) and (4) of the AML Act
Obligation to document mutual AML/CFT-related obligations and responsibilities in connection with the correspondent relationship; approval of the statutory body or the manager of the branch of the institution before establishing the correspondent relationship	Article 25 of the AML Act; Article 13(1) of the AML Decree
Obligations applicable to correspondent relationships; enhanced customer due diligence measures	EBA/GL/2021/02
Access to information about customers of the respondent institution in the case of payable-through accounts ³²	Article 13(2) of the AML Decree
Procedures for conducting ongoing due diligence with respect to the respondent institution	Article 13(3) of the AML Decree

Audit content

- The institution has defined, in the risk assessment, its risk appetite in relation to the provision of correspondent banking services, including:
 - a prohibition on accepting shell banks as respondent institutions,
 - procedures for assessing the admissibility of customers (respondent institutions),
 - procedures for assessing the admissibility of nested accounts;³³
- The institution has established in its internal regulations – and applies – procedures for obtaining detailed information on respondent institutions, in particular concerning the quality of supervision to which they are subject, any administrative proceedings conducted against them, and the quality of the measures they apply;
- The institution has established in its internal regulations – and applies – procedures for concluding agreements on the provision of correspondent banking services, including:
 - the allocation of decision-making powers,
 - the process for concluding these agreements,
 - the content of agreements, setting out at least all mutual obligations and responsibilities and the method for monitoring their fulfilment;
- The institution has established in its internal regulations – and applies – procedures for managing ML/FT risks in a manner appropriate to this type of customer and its specific characteristics, including:
 - ongoing customer due diligence, in particular updating of the customer information held by the institution,

³² A correspondent relationship that allows the respondent institution's customers access to the correspondent account.

³³ The principle whereby a respondent institution allows another financial institution access to its correspondent account. The nested financial institution thereby gains the benefit of correspondent status without having its own correspondent relationship with the correspondent. This results in a chain of correspondent banking relationships where the customers of the nested financial institution use a product provided by the correspondent to the respondent (without having a business relationship with either of them).

- monitoring of the fulfilment of mutual obligations and the quality of the AML/CFT measures applied by the customer,
- transaction monitoring, including adequate configuration of the look-through approach to monitoring the transactions of the customer's customers,
- access to information on the customer's customers in the case of payable-through accounts;
- The institution has established in its internal regulations – and applies – control mechanisms to ensure compliance with the conditions and obligations imposed on the respondent institution (including, where relevant, on-site testing of the respondent institution's control environment);
- The institution has established in its internal regulations – and applies – analogous procedures for all correspondent relationships in the broader sense, including those with other financial institutions.

Links to other assessed areas

Risk assessment

- The institution has assessed the risks and defined its risk appetite in relation to the provision of correspondent banking services.

Customer identification and due diligence

- The institution has procedures in place ensuring it has sufficient information about its customers.

Transaction monitoring and investigation of alerts

- The institution has effective procedures in place for monitoring transactions conducted in correspondent banking relationships to identify potential suspicions.

Training

- The institution ensures that relevant staff receive targeted training on correspondent banking.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution, including the risk assessment;</i> • <i>A sample of correspondent banking agreements and documentation evidencing their approval and execution, including, for example, the opinion of the AML unit;</i> • <i>An overview and sample of requests for information from the institution made by its correspondent institutions;</i> • <i>An overview and sample of requests for information from institutions made by their respondent institutions;</i> • <i>Documentation of due diligence conducted with respect to each respondent institution prior to establishing the business relationship;</i> • <i>Documentation of ongoing due diligence conducted with respect to each respondent institution during the business relationship, including an assessment of actual payments/transactions, particularly compared with information about the intended form of payment;</i> • <i>Organisational rules, including the roles and responsibilities of relevant staff;</i> • <i>Interviews with relevant staff;</i> • <i>The content of training sessions for relevant staff, and a list of training sessions and their participants;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i>

- *Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;*
- *Reports from previous internal/external audits and compliance reports for the institution and the group, where available;*
- *The internal audit plan;*
- *The compliance monitoring plan;*
- *Reports on relevant supervisory investigations/inspections.*

6.2. Requirements relating to information accompanying transfers of funds

Legal requirements	
Information accompanying transfers of funds – procedures when acting as the originating institution	Articles 4–6 and 10 of the TFR
Information accompanying transfers of funds – procedures when acting as the beneficiary or intermediary institution	Articles 7 and 8 and 10–12 of the TFR
Procedures for handling problematic counterparties in transfers of funds	Articles 8 and 12 of the TFR

Audit content

- The institution has established in its internal regulations – and applies – procedures to fulfil the requirements relating to information accompanying transfers of funds, including the verification of information, where it acts as the originating institution, in particular procedures to ensure that:
 - transfers of funds are accompanied by the required information on the payer, the payee and the transaction,
 - the accuracy of the information is verified before the transaction is executed,
 - it does not execute transactions without fulfilling the aforementioned obligations, unless permitted to do so under the relevant legislation;
- The institution has established in its internal regulations – and applies – procedures to fulfil the requirements relating to information accompanying transfers of funds where it acts as the beneficiary institution, in particular procedures for:
 - verifying whether transfers of funds are accompanied by the required information,
 - deciding whether to execute, reject or suspend transfers of funds that lack the required information or where the information is incomplete,
 - taking measures against a payment service provider that repeatedly fails to provide the required information, including notifying the competent authority responsible for AML/CFT supervision;
- The institution has established in its internal regulations – and applies – procedures to fulfil the requirements relating to information accompanying transfers of funds where it acts as the intermediary institution, in particular procedures for:
 - ensuring that all information that accompanies a transfer of funds is retained with the transfer,

- verifying whether transfers of funds are accompanied by the required information,
 - deciding whether to execute, reject or suspend transfers of funds that lack the required information or where the information is incomplete,
 - taking measures against a payment service provider that repeatedly fails to provide the required information, including notifying the competent authority responsible for AML/CFT supervision;
- The institution has clearly defined the responsibilities and obligations of staff and relevant units to ensure compliance with the requirements relating to information accompanying transfers of funds.

Links to other assessed areas

Information retention

- The institution retains the information accompanying transfers of funds.

Customer identification and due diligence

- The institution holds all necessary information about the customer.

Transaction monitoring

- The institution monitors all relevant transfers of funds.

Implementation of international sanctions

- The institution performs checks to identify any sanctions elements in all relevant information accompanying transfers of funds.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>A sample of transfers of funds;</i> • <i>An overview of information requests sent to and received from other institutions, including the date of the request and the manner and date of resolution;</i> • <i>A sample of information requests sent to other institutions;</i> • <i>A sample of information requests received from other institutions;</i> • <i>The job descriptions of relevant staff;</i> • <i>Interviews with relevant staff;</i> • <i>Documentation on, and the actual configuration of, the relevant IS/IT system;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

6.3. Confidentiality

Legal requirements	
Procedures to ensure confidentiality	Article 38 of the AML Act

Audit content

- The institution has established in its internal regulations – and applies – procedures ensuring that confidentiality is maintained in relation to:
 - the investigation and reporting of a suspicious transaction,
 - requests for information from the FAU and the fulfilment of cooperation obligations towards the FAU.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>Interviews with relevant staff;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

6.4. Identification of discrepancies

Legal requirements	
Procedures for cases where a discrepancy is identified	Article 15a of the AML Act

Audit content

- The institution has established in its internal regulations – and applies – procedures for identifying any discrepancies pursuant to the act governing the register of beneficial owners;
- The institution has established in its internal regulations – and applies – procedures for implementing follow-up measures where it has reasonable grounds to believe that, when conducting customer due diligence, it has identified a discrepancy pursuant to the act governing the register of beneficial owners, including procedures:
 - for notifying the customer,
 - for cases where the customer fails to remedy or disprove the discrepancy under the act governing the register of beneficial owners,

- for situations where the institution has been instructed by the FAU not to apply the prescribed procedure;
- The institution has clearly defined the responsibilities and obligations of staff and relevant units to ensure compliance with the requirements relating to the identification of discrepancies.

Links to other assessed areas

Customer identification and due diligence

- Customer due diligence procedures ensure the identification of any discrepancies;
- The follow-up procedures for resolving discrepancies identified are linked to the customer due diligence procedures for ensuring the completeness and accuracy of information.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution;</i> • <i>An overview of discrepancies identified, including the date of identification and the date and manner of resolution;</i> • <i>A sample of discrepancies identified;</i> • <i>A sample of corporate customers, identifying their beneficial owners;</i> • <i>The job descriptions of relevant staff;</i> • <i>Interviews with relevant staff;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>

6.5. Information duty towards the CNB

Legal requirements	
Procedures for promptly informing the CNB in the event of operations with selected high-risk counterparties or geographical areas	Article 115 of Decree No. 163/2014 Coll. and Supervisory Benchmark No. 4/2022
Procedures for promptly informing the CNB of a potential significant reputational threat	Article 116 of Decree No. 163/2014 Coll. and Supervisory Benchmark No. 4/2022

Audit content

- The institution has established in its internal regulations – and applies – procedures for informing the CNB where it has entered into an arrangement with, or is otherwise active with respect to a counterparty or in a country that is non-transparent or high-risk, including a specification of the content of such notifications;

- The institution has established in its internal regulations – and applies – procedures for informing the CNB where it identifies a potential significant reputational threat (especially in connection with criminal activity that may endanger or is endangering the performance of its activities, or a material trend in the AML/CFT area).
- The institution has clearly defined the responsibilities and obligations of staff and relevant units to ensure compliance with the requirements relating to informing the CNB of operations with high-risk counterparties or geographical areas and of (potential) significant reputational threats identified.

Links to other assessed areas

Risk assessment

- The institution considers, in its risk assessment, all situations that could affect or do affect its ML/FT risks, and documents these considerations;
- The institution has established in its internal regulations – and applies – follow-up procedures for managing risks arising from operations with high-risk counterparties or geographical areas and from (potential) significant reputational threats identified.

Internal control mechanisms

- The institution's communication and control mechanisms ensure that the governing and control bodies are informed in a timely and complete manner of operations with high-risk counterparties or geographical areas and of potential significant reputational threats.

Audit sources
<ul style="list-style-type: none"> • <i>Relevant internal regulations of the institution, including the risk assessment;</i> • <i>An overview of notifications sent to the CNB;</i> • <i>A sample of notifications sent to the CNB;</i> • <i>The job descriptions of relevant staff;</i> • <i>Interviews with relevant staff;</i> • <i>Minutes of meetings of the institution's governing, advisory and control bodies and committees where AML/CFT issues were discussed, including the documentation made available to the members for the meeting;</i> • <i>Internal AML/CFT reports, especially those prepared for governing bodies and staff (within the institution and the group), including assessment reports;</i> • <i>Reports from previous internal/external audits and compliance reports for the institution and the group, where available;</i> • <i>The internal audit plan;</i> • <i>The compliance monitoring plan;</i> • <i>Reports on relevant supervisory investigations/inspections.</i>