

Comments and responses given at the hearing of the Advisory Guidelines of Finantsinspektsioon “Application of international financial sanctions in credit and financial institutions” (hereinafter *guidelines*)

Commented part (clause number)	Comment of market participant¹¹	Response of Finantsinspektsioon (Estonian Financial Supervision Authority, hereinafter FSA) to comment²²
1.3.	Duplicates clauses 1.2, 2.1.2 and 2.1.3. Delete the proposal.	Not taken into account. For the sake of clarity, we wanted to clarify the role of the Financial Supervision Authority in more clauses.
1.4.	“Person with specific obligations” – used as a concept for the first time in clause 1.4, but defined in 2.2.1. Proposal to add the definition with footnote 14 to clause 3 as a footnote to clause 1.4.	Taken into account. Footnote added to clause 1.4.
1.5 and 1.6.	Proposal to change the order of the clause for a more logical sequence.	Taken into account. Guidelines amended as proposed.
2.1.1.	“The activities for the implementation of financial sanctions have been specifically kept in mind where obligations or sanctions and their implementation in general have been referred to in the Guidelines/ – As the guidelines are aimed at subjects of the supervision of the FSA who can apply a sanction, we request replacing the word ‘implementation’ with the word ‘application’ when speaking of the tasks of the subjects of supervision related to financial sanctions.	Taken into account. Guidelines amended as proposed.
2.1.1.	“Consequently, the implementation of trade sanctions as one of the sub-types of economic sanctions is not covered by the Guidelines.” – the sentence is irrelevant in its content considering the first sentence. However, if adding the sentence to the text is considered necessary, the service provision sanction could be highlighted alongside the trade sanction, for which the ISA allows obligated persons to share information with the competent authority.	Taken into account. The sentence specified in the comment has been deleted.
2.1.2.	Duplicates clauses 1.2., 1.3. and 2.1.3. Proposal to merge with clause 2.1.1.	Not taken into account.
2.1.2.	The text refers to EU decisions, but the financial sanction is imposed and its application becomes mandatory for persons with specific obligations through EU regulations. Please correct the	Taken into account. Guidelines amended as proposed.

¹ The comments in Estonian are given in their original form, i.e. the Financial Supervision Authority has not edited or changed the wording. The comments in English have been translated, but the content has been kept as close as possible to the texts received from market participants.

² The acronyms used in the responses (including for laws and guidance material) are the same as those used in the guideline on which the comments are made.

	wording.	
2.2.1.	Proposal to add the definition of a person with specific obligations to clause 1.4. where the expression is first used.	Partly taken into account. Due to the context, the definition has been left under clause 2.1.1, but a reference to 2.1.1 has been added as a footnote to clause 1.4.
2.3.1.	Duplicates clause 2.1.2. Delete the proposal.	Taken into account. The sentence specified in the comment has been deleted.
2.3.13	<p>Clause 2.3.12 stipulates the principle that a person with specific obligations does not remove themselves from communication with clients and, if necessary, explains the necessity of the requirements in public interest.</p> <p>In financial sector practice, restrictions resulting from sanction controls (e.g. closure of accounts, suspension of transactions) are often inseparably linked to suspicions of money laundering and terrorist financing (e.g. as a predicate offence for suspected sanctions evasion, use of fronts). The obligation to explain the reasons for the restriction to the client may lead to a situation where the person with specific obligations inadvertently tips the client off about supervisory measures or risk models. However, this is in direct contradiction with the mandatory prohibition to disclose information or to give hints set forth in § 51 of the Money Laundering and Terrorist Financing Prevention Act (MLTFPA).</p> <p>In addition, in a situation where a false positive response has been generated, mentioning sanctions to the client (“Your transaction is under sanctions control”) creates undue anxiety and a negative client experience that market participants try to avoid.</p> <p>The proposal is to amend the wording and to add a clear restriction that giving explanations to the client is only allowed to the extent that it does not jeopardise the confidentiality of the procedure, does not disclose the logic of the risk models of the person with specific obligations and is not conflict with the restrictions set out in § 51 of the MLTFPA.</p>	Partly taken into account. A footnote has been added to the guidelines following the recommendation in the comments. At the same time, we would like to point out that pursuant to § 17 of the ISA, a person who is subject to a financial sanction or who is involved in a transaction that is subject to a financial sanction has the right to submit a request to the Financial Intelligence Unit (FIU) to verify whether the application of the sanction was lawful. It is therefore necessary that the client is aware that a sanction has been applied to them. At the same time, the guidelines refer to compliance with requirements arising from legislation, among other things, i.e. in the case of a suspicion of money laundering or terrorist financing, the person with specific obligations complies with the requirements of the MLTFPA and the instructions of the Financial Intelligence Unit.
2.3.5.	The clause could also include a reference to the fact that the definitions in the guideline are also set out in clause 2.4., or make this point a part of clause 2.4.	Taken into account. Guidelines amended as proposed.

2.3.6.	“Compliance with the requirements for the implementation and application of international sanctions is, within the meaning of these Guidelines, all of the activities expected from EU, UN and FATF Member States” – have Estonian requirements been intentionally excluded from this clause?	Taken into account. Guidelines amended according to the question given in the proposal. In addition to the above, a person with specific obligations must comply with the requirements of the competent authorities of the Republic of Estonia.
2.3.7. and 2.3.8. and 2.3.9.	Are the guidelines applied, complied with or implemented? A single term should be used throughout the text. For example, implementation is used in clauses 2.1.4, 2.3.11.	Partly taken into account. The definitions used in the guidelines are different because of their different content. For example, the state implements an international financial sanction, but a person with specific obligations applies it.
3.1.2	Please clarify what is meant by a change in ‘risk position’. Does it mean changes in the ‘assessment of the risk position of the restrictive measures’ as specified in the EBA <u>Guidelines</u> on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/GL/2024/14)?	Taken into account. This EBA Guideline on Restrictive Measures is also referred to in the guidelines, inter alia in relation to the use of the terms it contains.
3.2.3.1.	Proposal to replace ‘One of the characteristics is’ with ‘One of the most common characteristics is ...’, as this is not always an applicable risk.	Taken into account. Guidelines amended as proposed.
3.2.3.1.	Please clarify what is meant by ‘or entails another risk’ in the 4th sentence of the clause – do you mean other types of risks, e.g. ML/TF risks, or other sanction risks?	Partly taken into account. Clarified here: the guidelines address the management of sanction risks, but it is important to recognise that these may be linked to and coincide with money laundering or terrorist financing risks, i.e. a person with specific obligations must be able to take into account the broader profile of the client risk associated with them.
3.2.3.1 and 3.2.6	The scope of the risk management related to proliferation financing remains unclear, which may be in conflict with the overall focus of the guidelines on ensuring the application of legally binding international and domestic financial sanctions. The scope, purpose and basic principles of the guidelines repeatedly emphasise that the guidelines are intended for the effective application of financial sanctions imposed by a UN, EU or governmental resolution, decision or regulation (e.g. clauses 1.4, 2.1.2, 2.3.3). The definitions given in clause 2.4 of the guidelines define a financial sanction on the basis of an existing legal act or list (targeted) or on the basis of a limited sector/region (activity-based). However, clause 3.2.6 on the risk of proliferation financing states that a person with specific obligations must ‘separately assess the risks of money laundering, terrorist financing and financial	Not taken into account. Based on international standards (including the FATF Guidelines on Combating Proliferation Financing), it is important that persons with special responsibilities separately address, inter alia, proliferation financing risks, including by assessing their own risks (e.g. due to their client base and the geographical scope of their business) and vulnerabilities to being exploited for proliferation financing. According to the guidelines, proliferation financing and evasion risk assessments may be included in the same document as other risk assessments, but they must be assessed separately. It is acceptable if the person with specific obligations has found, as a result of the assessment, that the risks associated with its business activities are minimal (e.g. as a result of the circumstances described in the commentary) and the measures applied are appropriate.

sanctions' and must have 'separately identified and understood, among other things, the proliferation financing risk associated with its business'. Whilst clause 2.4 states that 'financial sanctions /.../ are one of the main tools for the prevention of proliferation financing', the definition of proliferation financing in the same clause is much broader, referring to a broader and distinct approach to the risk of financial crime. This contradicts the general focus of the Guidelines (and the name of the Guidelines), which is rule-based compliance with sanctions.

Clauses 3.2.3.1 and 3.2.6 of the Guidelines emphasise the need to assess the risk of proliferation financing separately within the scope of client risk. Pursuant to § 13 (2) of the MLTFPA, risk assessment measures must be proportionate to the nature and scope of the activity.

For market participants in the financial sector that are not involved in trade financing or the documentation of the physical movement of dual-use goods, the risk of proliferation financing is predominantly related to general sanction and geographical risks. The requirement to develop a separate technical 'proliferation financing risk level' (separate risk level) would be unreasonably resource intensive and duplicative for such market participants, and would not add any meaningful value to risk mitigation.

Proposal to clarify in the guidelines beforehand, either in terms of the objective (2.1) or principles (2.3), whether the objective of the risk of proliferation financing is:

1. sanction-based, i.e. addressed only through the implementation of existing targeted and action-based financial sanctions related to proliferation financing, or
2. a separate financial crime risk, i.e. addressed as a separate financial crime risk (such as money laundering or terrorist financing risk) that requires the development of internal controls in addition to formal checking of sanctions lists in order to detect and reduce unsanctioned proliferation-related transactions.

	<p>This clarification is necessary to ensure that subjects of supervision establish a compliance framework of the right scope and resource allocation. If it is a separate risk, its integration into the AML/CFT framework should be clearly stated in the introductory sections, together with the obligation to apply financial sanctions. While the guidelines are aimed at the financial sector as a whole (credit and financial institutions), the risks of financial crime vary widely across sectors, depending on the business operations and the target markets. Please at least clarify in the guidelines that market participants may assess and manage the proliferation financing risk as part of the overall risk profile of the client (client's risk level), incorporating relevant risk factors, but without having to create a separate assessment model/level for the risk of proliferation financing.</p>	
3.2.3.2.	<p>'payable-through accounts' (kasutusõigusega kontod) – pursuant to the MLTFPA, payable-through accounts has been translated into Estonian as 'laiendatud kasutusõigusega kontod'. Proposal to harmonise the terminology.</p>	<p>Taken into account. Guidelines amended as proposed.</p>
3.2.3.5.	<p>"It is important to note that even small parts of a system have a significant impact on the system as a whole, so any decision affecting the effectiveness of the system should be based on a prior risk analysis (be risk-based)." – this wording imposes the obligation to carry out a risk analysis in any case, even if the impact of the decision on the effectiveness of the system is minimal/insignificant. Is this necessary?</p>	<p>Not taken into account. This sentence refers to all decisions that affect the effectiveness of the system, not those that do not. No formal requirements for a risk analysis are foreseen here, the important thing is that it reflects why a decision has been made and what the implications are. The risk analysis makes it possible, among other things, to assess the impact of the decision on the effectiveness of the system. The analysis should be carried out in a proportionate manner, i.e. if there is a reasonable expectation that the impact of the decision on the system will be very small, the analysis should be based on this, taking into account the interaction of the changes resulting from the decision with other factors and the system as a whole.</p>
3.2.6.	<p>"The evasion risks must therefore be assessed separately, appropriate measures must be created to manage this risk, and compliance with and monitoring of them must be ensured." – does this sentence refer to a separate assessment of the risks of proliferation financing evasion, or does the last sentence refer to evasion risks more broadly? As the identification of proliferation financing risks as a whole in the risk assessment is complex for persons with specific obligations</p>	<p>Not taken into account. The EBA Guidelines on Restrictive Measures require the separate acknowledgement and management of evasion risk. The guideline refers to the assessment of risks of all categories, including the risks of evasion of prevention of proliferation financing. According to the NRA, the risk of evasion of a targeted financial sanction is average. It must be kept in mind here that according to the NRA methodology, the sanctions against Russia that pose a threat to the activities of</p>

	<p>and requiring a separate in-depth analysis of evasion would not add value, inter alia considering the low risk of NRA proliferation financing in the state. Delete the last sentence of the proposal.</p>	<p>companies due to our geographical location were not addressed. At the same time, it is stated in the NRA that <i>the level of evasion risk is increased by Russia's close cooperation with Iran and North Korea</i>. Compliance with the clause of the guidelines specified in the commentary must be based on proportionality, i.e. the assessment of each risk does not require an in-depth analysis, extensive documentation, etc., but it is important that the person with specific obligations is aware of the potential evasion risk, both in the case of financial sanctions in general and in the case of proliferation financing in particular, and has analysed, among other things, where such risks lie in its business and how to deal with them.</p>
<p>3.4.11.</p>	<p>Clause 3.4.11 of the Guidelines stipulates: “The person with specific obligations carries out media monitoring /.../” The words ‘carries out’ impose an unambiguous obligation.</p> <p>The current law (the due diligence section of the MLTFPA) does not provide for a general obligation to carry out media monitoring for all clients or transactions. This is a measure that is usually implemented in higher risk cases as part of enhanced due diligence measures. The guidelines should not extend the statutory due diligence obligation to a general duty.</p> <p>Proposal to make the wording of the clause risk-based: “A person with specific obligations must carry out media monitoring if necessary and on a risk-basis /.../”</p>	<p>Not taken into account. Media monitoring is an important part of managing sanction risk, including the underlying KYC principle. This requirement is also included in the EBA Guidelines on Restrictive Measures and the current guidelines. The scope and frequency of media monitoring may be applied on a risk-basis and may be chosen by the person with specific obligations, including through or with the support of the services provided by third parties.</p>
<p>3.4.13.</p>	<p>“The person with specific obligations thereby takes into account all the sanction regimes implemented in the Republic of Estonia, including the sanctions of the Government of the Republic”/ – since persons with specific obligations are obliged to identify and apply financial sanctions, is this also the content and purpose of this sentence, or do the guidelines extend the obligations of person with specific obligations, and do the entry and transit restrictions established by the Government of the Republic also have to be followed? If entry and transit restrictions must also be monitored, what are the expectations for persons with specific obligations?</p>	<p>Partly taken into account. The guidelines have been clarified and now state that according to the guidelines, the sanctions that primarily concern the activities of the person with specific obligations must be taken into account. However, it is important to note that compliance with sanctions is mandatory for all, including persons with specific obligations. The Financial Supervision Authority supervises persons with specific obligations in the application of financial sanctions, including financial sanctions of the Government of the Republic. These guidelines are also addressed for this, and persons with specific obligations may consult competent authorities about the application of other sanctions.</p>

3.4.13.	<p>“In addition, internal controls must include monitoring to ensure that systems, including procedures, are in place to identify the risks of evasion of sanctions, including measures to prevent proliferation financing.” – Does the monitoring of procedures mean a specific separate process or can a person with specific obligations perform this obligation by including the amended procedures in the approval process? Also, for example, by mapping new legislation and similar existing processes.</p>	<p>Partly taken into account. Clarified hereby: both a separate process and monitoring through involvement in other processes are possible. It is important that, among other things, the monitoring of processes is covered, and that no significant issues are overlooked when internal controls are carried out.</p>
3.5 (Reporting proliferation financing)	<p>The requirements for reporting proliferation financing are not sufficiently differentiated from the general expectation of compliance with the financial sanction reporting requirements in practice.</p> <p>Proposal to create clearer guidelines specifically for reporting proliferation financing or to create a form with all the additional information etc. needed compared to a normal sanction report.</p>	<p>Not taken into account. The FSA is not legally the addressee of the reports of financial sanctions or proliferation financing. The Financial Intelligence Unit is the addressee. Therefore, these guidelines do not contain precise instructions in this respect, including on how to submit a report.</p>
3.6.1	<p>This clause requires the retention of data relating to checks on whether a proposed transaction breaches a financial sanction. The wording is too broad and could lead to the interpretation that monitoring results should be retained for all AST false positives, which are also immediately discarded as irrelevant by the AST. In the case of large-scale systems, such massive retention of technical noise would impose an unreasonable administrative and data burden on market participants and would be contrary to the data minimisation principle of the General Data Protection Regulation.</p> <p>Please clarify that the retention obligation only covers actual suspicions, cases requiring human analysis (alerts) and measures applied, not automatic technical noise that is systematically discarded.</p>	<p>Not taken into account. The wording of this clause follows from the law. Pursuant to § 22 (1) of the ISA, there is an obligation to retain the data proving the fulfilment of the obligations under § 21 of the ISA. If the AST used by the person with specific obligations works effectively, it will not generate large volumes of unnecessary alerts, which in turn will not lead to an obligation for the person with specific obligations to retain these excessive false positives. Due to the use of different solutions by persons with specific obligations, the guidelines do not restrict which data should be retained and which should not. There are a number of reasons why data could be retained in the case of false positive matches. Firstly, they show that the transaction or person has been checked. Secondly, should a false positive later prove to be a correct match, the person with specific obligations has a documented situation where best efforts were made but no positive match was identified based on the information available at that time. In addition, it is important for internal control to check that false positives were correctly identified and that the system is working effectively.</p>
3.7.2.	<p>What is covered by the obligation to control the means used by the obliged entity? Does it mean the use of tools or something else? What is its purpose?</p>	<p>Taken into account. The Guidelines have been clarified according to the comment. It refers more broadly to the means used by a person with specific obligations to fulfil their duties. This includes, for example, technological tools such as AST. As the quality and</p>

		efficiency of work depends largely on the tools used, it is important to ensure that the tools are controlled.
3.7.3	Clause 3.7.3 and Annex 1 refer to internal control and testing. In practice, it is important to distinguish between regular validation and independent audit.	Partly taken into account. This clause is already included in the current guidelines and does not contradict the EBA Compliance Guidelines (EBA/GL/2022/05). The guidelines address the general and common part of internal control, and the first sentences of the clause do not prescribe when internal control is to be carried out and when an internal audit must be performed, but provide general guidelines for the entire internal control.
	Proposal to specify for the sake of legal clarity that the regular testing and validation of the AST may be performed by the compliance review of the second line of defence, provided that it is independent of its operational processes and the internal audit (as the third line of defence) periodically assesses the adequacy of the control framework of the second line of defence and the integrity of the validation process. This would ensure flexibility and compliance with EBA Guidelines (e.g. EBA/GL/2022/05, p. 31).	However, in light of this comment, we have clarified the independence (clause 3.7.1) and the distinction (clause 3.7.3) between the internal control performed by the second line of defence and the internal audit performed by the third line of defence. In addition to the regular control carried out by the second line of defence, including the testing of the AST, the recommendations for internal control and testing set out in the guidelines are also intended for internal audit. Thus, the recommendation in the comment to limit AST testing to the second line of defence has not been taken into account.
3.8.2.	Please add to the clause the clarification that training on sanctions must be completed within a reasonable time after the commencement of employment, not just as a general principle of 'commencement of employment'. The guidelines could also explicitly refer to the fact that this sanction training is in particular mandatory for the employees described in clause 3.8.1, i.e. those whose job duties include establishing business relationships or carrying out transactions, and for other roles according to the risk assessment (referring for example to clause 2.3.9 – the principle of a risk-based approach must be taken into account in compliance with the guidelines).	Partly taken into account. Clause 3.8.3 of the guidelines has been clarified, stating that the employee must have completed the training before the performance of tasks that require the training. Taken into account. The guidelines have been amended in line with the proposals made in the comment (the clauses differ from those referred to in the comment, but the content has been changed according to the commentary).
3.8.2.	We understand that the EBA <u>guidelines</u> include the requirement to prove the effectiveness of training. Please clarify in the guidelines what kind of evidence is specifically meant that the person with specific obligations could provide to demonstrate the effectiveness of the training. Since statistics consist up of many variables, it is highly unlikely that a causal link can be established to prove effectiveness.	Taken into account. The Guidelines have been clarified. The effectiveness of training can be proven, inter alia, by checklists filled in after training, which show whether the employee has understood and retained the key aspects relevant to their job. Another measure is, for example, internal control, which includes, among other things, the monitoring of the activities of the employees for which they have received training. This also helps understand further training needs.

<p>Annex 1. (footnote number 25)</p>	<p>Footnote 25 in Annex 1 states: “For CASPs and PSPs, the use of a technological solution for screening is required”.</p> <p>§ 23 (1) of the ISA obliges a person with specific obligations to establish rules of procedure that allow for the immediate identification of the entry into force of a financial sanction. The legislator has left the choice of method (manual vs. automatic) to the market participant, on the basis of the proportionality principle. The guidelines cannot impose an imperative obligation to purchase an IT solution unless required by law. For smaller volumes, a manual check can be just as effective.</p> <p>Proposal to change the wording and replace ‘is required’ with a recommendation or add the proportionality clause: “The use of an AST is strongly recommended, but a person with specific obligations may use other measures if they can demonstrate their equivalent effectiveness”.</p>	<p>Not taken into account. This clause refers to the EBA Guidelines on Restrictive Measures. For crypto service and payment service providers, this includes guidance on the use of ASTs to ensure that sanction risks arising from their business activities are appropriately managed. The EBA Guidelines have been transposed by the FSA and are already in force, so there is no additional or new requirement for persons with specific obligations (in particular for crypto asset service and payment service providers).</p> <p>The provision of crypto asset and payment services carries a higher risk of sanction violations. The guideline is subject to the ‘comply or explain’ principle. It is up to the person with specific obligations to assess whether it is possible to properly screen transactions and the client base in the case of its service, including the provision of the crypto asset service or payment service, only manually.</p>
<p>Annex 1, p 1</p>	<p>“It is important to ensure that all the sanction regimes implemented in the Republic of Estonia are covered, and the sanctions list must also include the subjects covered by the sanctions of the Government of the Republic”/ – since persons with specific obligations are obliged to identify and apply financial sanctions, is this also the content and purpose of this sentence, or do the guidelines extend the obligations of persons with specific obligations, and do the entry and transit restrictions established by the Government of the Republic also have to be followed? If entry and transit restrictions must also be monitored, what are the expectations for persons with specific obligations?</p>	<p>Not taken into account. See the response of the FSA to the comment of the Banking Association on clause 3.4.13 of the guidelines.</p>
<p>Annex 1, p 2</p>	<p>“For this purpose, the Person With Specific Obligations must determine which official updated data concerning sanctions of competent authorities the employees must follow as well as determine the adequate frequency of checking the respective updates.” – please specify if possible what is meant by adequate frequency of checking, e.g. once, twice or three times a day.</p>	<p>Not taken into account. It is good practice for larger organisations to introduce automated systems that update the lists used by persons with specific obligations and the additional information associated with them as soon as changes have been made in the official sanction publication channels (e.g. the Official Journal) and in the information provided by the competent authorities (e.g. information published on the FIU website). The size of the person with specific obligations, the client base, etc. are important in the case of regularity. This is why a specific period of time is not defined in the guidelines.</p>

Annex 1, p 3	<p>“If the person with specific obligations decides to use outsourced services in the case of a monitoring or screening system, including AST, the requirements applied to outsourcing in the FSA Outsourcing Guidelines are applied.” – the sentence duplicates the sentences on page 1 of the same annex. The AST may be outsourced or developed in-house. In the first case, the requirements for outsourcing in the FSA’s advisory guidelines “Requirements for outsourcing by persons subject to financial supervision” and in the EBA Guidelines on Restrictive Measures must be followed among other things. Delete the sentence on page 3.</p>	<p>Taken into account. The sentence specified in the comment has been deleted.</p>
Annex 1, p 3 (testing)	<p>Annex 1 details the requirements for AST testing (including noise simulation, checking the algorithm logic, etc.). Many market participants use standard solutions from reputable service providers or cross-group central systems where the local entity may not have access to the source code and algorithms to perform the specific type of in-depth testing described. Access to such information is often restricted due to the service provider’s intellectual property rights and ownership of its screening algorithms.</p> <p>Please clarify that in the case of testing performed by a service provider or across the company, the technical requirements are met if the local entity supervises the service provider (e.g. through cooperation agreements and reports), regular audits of the service provider are relied upon, and regular functionality checks (e.g. in the form of list testing) are performed. The solution described ensures that the person responsible for the AML/CFT compliance check understands the operation and design of the system in accordance with EBA/GL/2022/05 paragraph 52(a).</p>	<p>Not taken into account. This clause is already included in the current guidelines. This does not prevent testing from being adapted and carried out, if necessary, in a situation where a person with special obligations uses an external AST provider. This is a guideline for testing, not a mandatory testing methodology. It is important that the person with specific obligations understands the functioning of the AST used to manage their risks and that it is regularly monitored and adapted to the needs of the person with specific obligations.</p>
Annex 1, p 5	<p>Please clarify what is meant by ‘significant deficiencies and weaknesses’ in the last sentence.</p>	<p>Taken into account. In particular, weaknesses that affect the functioning of the system to an extent that may prevent the person with specific obligations from fulfilling its legal obligations, e.g. where the weakness is not mitigated by other measures, are relevant.</p>
Annex 1, p 5	<p>The guidelines state that corrections to the AST must be made without delay. The term is vague and there is no specific timeframe for its application.</p>	<p>Not taken into account. The requirement to make improvements without delay arises from the EBA Guidelines on Restrictive Measures, which have been transposed and adopted by the FSA</p>

	<p>Proposal to define the term more clearly or provide an indicative timeframe (e.g. in working days) based on the criticality of the identified deficiency or error to ensure consistent and appropriate application of the requirement in the guideline.</p>	<p>as its own guidelines. Therefore, this is not a new requirement, nor is it a requirement imposed only by the FSA in Estonia, but a principle that applies throughout the European Union.</p> <p>According to supervision, the purpose of the use of the AST requires corrective action to be taken as soon as a deficiency or failure is identified. Depending on the deficiency, this may affect the ability of the person with specific obligations to continue to provide the service lawfully. Therefore, it is important to ascertain the nature and extent of the deficiency at the earliest opportunity and to remedy it without delay.</p>
Annex 2 and Annex 3	<p>In the annexes to the guidelines, a lot of attention is given to the substantive inspection of goods (including dual-use goods), supply chains and the purpose of end-use. Many persons with specific obligations (e.g. investment firms, payment institutions) provide services with financial instruments or cash as underlying assets, rather than goods, and do not have access to commercial documents (delivery notes, HS codes). Requiring them to physically inspect the goods as part of the transaction is disproportionate and impractical.</p> <p>Proposal to include in the guidelines the principle that the scope of financial risk due diligence measures depends on the type of service provided. In the case of investment and payment services not related to trade financing, controls should be limited to the verification of counterparties and sanctions on instruments and the assessment of geographical risks.</p>	<p>Not taken into account. This requirement is already included in the current guidelines. A person with specific obligations has a duty to know its client and, where the client's business is likely to have contact with sanctions, the person with specific obligations must apply due diligence measures to the extent that allows the person to ascertain, inter alia, that the client's transactions do not breach sanctions, including by financing proliferation.</p>
Annex 2, p 3 (cyberattacks)	<p>The inclusion of cyberattacks as a method of evasion of sanctions is welcome, but there are no practical examples or clear danger signs for market participants to follow.</p> <p>Proposal to add specific examples or a list of red flags regarding cyberattacks related to sanctions to help market participants accurately reflect these risks in their internal typologies.</p>	<p>Partly taken into account. Proposal partially implemented by this clarification. The guidelines describe the method that organisations must take into account when building their systems. The possible connection of one's client base and transactions to breaches of sanctions through cyberattacks or evasion is one of the factors that an organisation can identify through media monitoring (e.g. currencies stolen via cyberattacks, volumes, links to specific wallets, as well as the time of movement of funds obtained through ransomware, regions and persons involved). For example, there have been previous media reports of a North Korean cyberattack</p>

		to steal crypto assets, which later led to money laundering. ³ In addition to media monitoring, it is important to follow the typology announcements published on the website of the Financial Intelligence Unit (https://fiu.ee/juhendid-analuusid-ja-materjalid/tupoloogiateated).
General information (risk-based documentation)	<p>It follows from the guidelines that decisions (e.g. on the frequency of screening or on the updating of lists) can be based on a risk-based approach. However, it does not specify the expectations of documenting the reasoning behind this decision.</p> <p>Proposal to include in the guidelines examples or a framework for the documentation etc. that the FSA expects in the exercise of supervision to justify a market participant's risk-based decisions.</p>	<p>Not taken into account. This clause refers to the guidance to document risk-based decisions arising from the EBA Guidelines on Restrictive Measures. Documenting the reasons for making risk-based decisions is a standard part of the risk management system. § 13 (1) of the MLTFPA prescribes the obligation to draw up a risk assessment and the risk categories that must be addressed in the assessment.</p> <p>According to subsection (3) of the same section, the risk assessment must be used to define the lower and higher risk areas (clause 1), the risk appetite (clause 2) and the risk management model, including the application of due diligence measures (clause 3). Subsection (4) stipulates that the risk assessment and the establishment of the risk appetite are documented, and the documents are updated where necessary and based on the published results of the national risk assessment. The law has therefore established a framework that specifies the decisions that must be documented and retained. Documentation must make it possible to understand at a later stage, for example, which decision has been adopted and why. This is important when the supervisory authority carries out supervision as well as when the person with specific obligations carries out an internal audit and makes management decisions.</p>

³ See e.g.: <https://majandus.postimees.ee/7430348/pohja-korea-hakkerid-varastased-mullu-400-miljonit-dollarit-krupitoraha> (accessed on 05.02.2026).