

Guidelines for Electronic Money and Payment Institutions Regarding the Organisation of the Risk Management Process

Contents

Introduction	2
1. The lifecycle risk maturity model	7
2. Risk culture and governance	9
3. Strategic integrity: risk strategy and risk appetite	14
4. The risk management system	18
5. Risk monitoring and reporting: the rhythm of the institution	21
6. Documentation	24
7. Reviewing and improving the risk management system	28
Annex. The fintech lifecycle risk maturity model	29

Introduction

Lietuvos bankas has prepared the Guidelines for Electronic Money and Payment Institutions Regarding the Organisation of the Risk Management Process (hereinafter, the Guidelines).¹ The Guidelines underline the growing development of the payments market and the challenges and risks that arise during the licensing of new electronic money and payment institutions, and subsequently in the course of their business. They also serve to increase the maturity of the fintech sector and address the need to describe in more detail how to organise the risk management process, taking into account the specific characteristics of the businesses of financial market participants.

In addition, the Guidelines for the Development of the Lithuanian FinTech Sector 2023–2028, published by the Ministry of Finance of the Republic of Lithuania; and the Action Plan for the Development of the Lithuanian FinTech Sector 2023–2028, approved by Order No 1K-247 of the Minister of Finance of the Republic of Lithuania of 27 June 2023 on the approval of the action plan for the development of the Lithuanian financial technology (FinTech) sector 2023–2028, also emphasise the need for fintech companies to ensure timely and high-quality risk management and stress that the qualitative development of the fintech sector and its long-term success go hand-in-hand with the increased maturity of individual companies and the sector as a whole, i.e. with improvements in terms of proper risk assessment and prevention.

These Guidelines have been developed in light of legislation relevant to the activities of electronic money and payment institutions, including:

- the Republic of Lithuania Law on Payment Institutions;
- the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions;
- the requirements of Resolution No 247 of the Board of Lietuvos bankas of 30 December 2009 on the approval of the description of the requirements for electronic money institutions and payment institutions regarding the governance arrangements, internal control system and safeguarding of customer funds.

The Guidelines also take into account the best practices of financial market participants, the recommendations of Lietuvos bankas, various consultations, and the shortcomings identified during inspections.

The organisation of the risk management process, its integration into the internal control systems of fintech companies, and its implementation may differ from the Guidelines, provided that fintech companies ensure the equivalent and effective organisation of the risk management process.

The development and long-term success of fintech companies depends on the adoption of a uniform risk assessment and risk management approach between supervisors, undertakings in the sector, and their associations.

Lietuvos bankas, as a supervisory authority, develops best practices by involving fintech companies and their associations in the development and improvement of risk management implementation practices. Lietuvos bankas seeks to ensure and harmonise the expectations of the fintech sector and related associations regarding the development of individual risks and a common risk management system, as well as to communicate changes in a timely manner, provide advice, and supervise compliance with risk management requirements within fintech companies using prudential means.

¹ The Guidelines have been translated from Lithuanian. In the event of any discrepancies between the English and Lithuanian texts, the Lithuanian version shall prevail.

As part of their mission to develop a strong and credible fintech sector and represent its interests, fintech associations should cooperate with their members and/or Lietuvos bankas, provide feedback, act as intermediaries in market consultations, and promote the dissemination of best practices in line with the highest standards of risk management.

In the case of any questions or suggestions, institutions and/or associations of fintech companies may initiate a dialogue with Lietuvos bankas to supplement or update the Guidelines. When amending the Guidelines on the initiative of Lietuvos bankas, it would be considered best practice to initiate a public consultation with the fintech sector on the practical implementation of the amendments to the Guidelines prior to their adoption.

Definitions

1. **“Description”** means the Description of the Requirements for Electronic Money Institutions and Payment Institutions Regarding the Governance Arrangements, Internal Control System, and Safeguarding of Customer Funds, approved by Resolution No 247 of the Board of Lietuvos bankas of 30 December 2009 on the approval of the description of the requirements for electronic money institutions and payment institutions regarding the governance arrangements, internal control system and safeguarding of customer funds;
2. **“LEMEMI”** means the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions;
3. **“Group of companies”** follows the definition supplied in the Republic of Lithuania Law on Financial Reporting by Undertakings and Groups of Companies;
4. **“Incident Register”** means a document or system for recording information on incidents;
5. **“Institution”** means an electronic money institution or a payment institution licensed by Lietuvos bankas;
6. **“Institution lifecycle (phase)”** means the baby born, grow, scale, and rocket phases in the activities of an electronic money institution or payment institution, as described in Chapter 1 of the Guidelines;
7. **“Small institution”** means an electronic money institution or payment institution that only provides the payment initiation and/or account information services, and/or only engages in the collection of fees for utilities or other services provided on a regular basis for household needs, and/or engages in the collection of fines and/or other charges to public authorities, and in the payment of social benefits;
8. **“LPI”** means the Republic of Lithuania Law on Payment Institutions;
9. **“Risk appetite”** means the defined types and levels of risk that an electronic money institution or payment institution can accept or must avoid in order to achieve its strategic objectives;
10. **“Risk”** means a potential event, circumstance, or situation of uncertainty that could adversely affect the strategic objectives of an electronic money institution or payment institution;
11. **“Risk culture”** means the set of principles, rules, attitudes, beliefs, values, knowledge, practices, understanding, and actions of an electronic money institution or payment institution that determine the approach of its managers and employees towards risk and risk management;
12. **“Risk register”** means a document or database for recording information on risks;
13. **“Risk monitoring”** means a process consisting of monitoring risk indicators, early warning signals, and risk response tasks at specified intervals and reviewing the risk register at least quarterly;

14. **“Risk strategy”** means a strategic decision by an electronic money institution or payment institution on how to manage risks while implementing its business plan and pursuing its strategic business objectives or initiatives;
15. **“Internal document setting out the Institution’s risk strategy and the principles of risk management organisation”** means the internal document of an electronic money institution or payment institution referred to in paragraph 37 of the Description;
16. **“Risk management”** means the systematic and recurrent process of identifying, assessing, monitoring, mitigating, controlling, and responding to potential threats and opportunities in order to minimise adverse effects and ensure the achievement of strategic objectives;
17. **“Risk management officer”** means the owner, coordinator, and centre of excellence for risk management in an electronic money institution or payment institution;
18. **“Risk management system”** means a systematic and iterative process for identifying, assessing, monitoring, mitigating, controlling, responding to, and reporting on risks. This consists of a set of principles, strategies, policies, internal procedures, governance, and communication channels established and applied by an electronic money institution or a payment institution, and the competences, behaviours, and involvement of its managers and employees in the management of its activities, including the risks associated with them;
19. **“Risk tolerance limits (risk limits)”** means threshold levels of risk exposure. If they are exceeded, this must be communicated and should lead to the actions foreseen in the internal document setting out the Institution’s risk strategy and the principles of risk management organisation (e.g. informing the management of the situation for further decision-making and action and/or obtaining the approval management to exceed the risk limits);
20. **“Risk map”** means a document, system, or visual aid that systematically depicts, in a graphical manner, all existing or potential risks, taking into account the likelihood and the potential impact of the occurrence of a particular risk, and showing the possible links between risks, where the occurrence of one risk has an impact on the occurrence of another risk;
21. **“Strategic integrity”** means the ability of an electronic money institution or payment institution to integrate its values, mission, strategic objectives, principles, and decisions into a coherent and seamless whole.

Other terms used shall be understood as defined in LEMEMI and LPI.

Purpose and scope

The purpose of the Guidelines is to elaborate on and help institutions to understand the applicable requirements for the organisation of the risk management process laid down in the applicable legislation and demonstrate their relationship with the institution’s activities; provide institutions with the recommendations of Lietuvos bankas on increasing the maturity of the organisation of the risk management process in light of the institution’s lifecycle; and draw attention to the examples of best practices.

The Guidelines summarise the legal requirements regulating the financial market alongside national and international risk management principles, and are of a recommendatory nature. Institutions are encouraged to keep abreast of new developments in the organisation of the risk management process and to follow the best practices of international risk management standards in the production of their internal documents.

Where the legislation sets out specific requirements/obligations for institutions in relation to risk management, the legal requirements shall apply.

Institutions should make reasonable efforts to implement the best practices set out in the Guidelines, taking into account their size, scale, and the specificity of their activities; establish an effective risk management system which effectively integrates risk management practices at the time of licensing; effectively improve existing practices on the organisation of the risk management process; and enhance the risk culture in their institutions, thus increasing their maturity and sustainability.

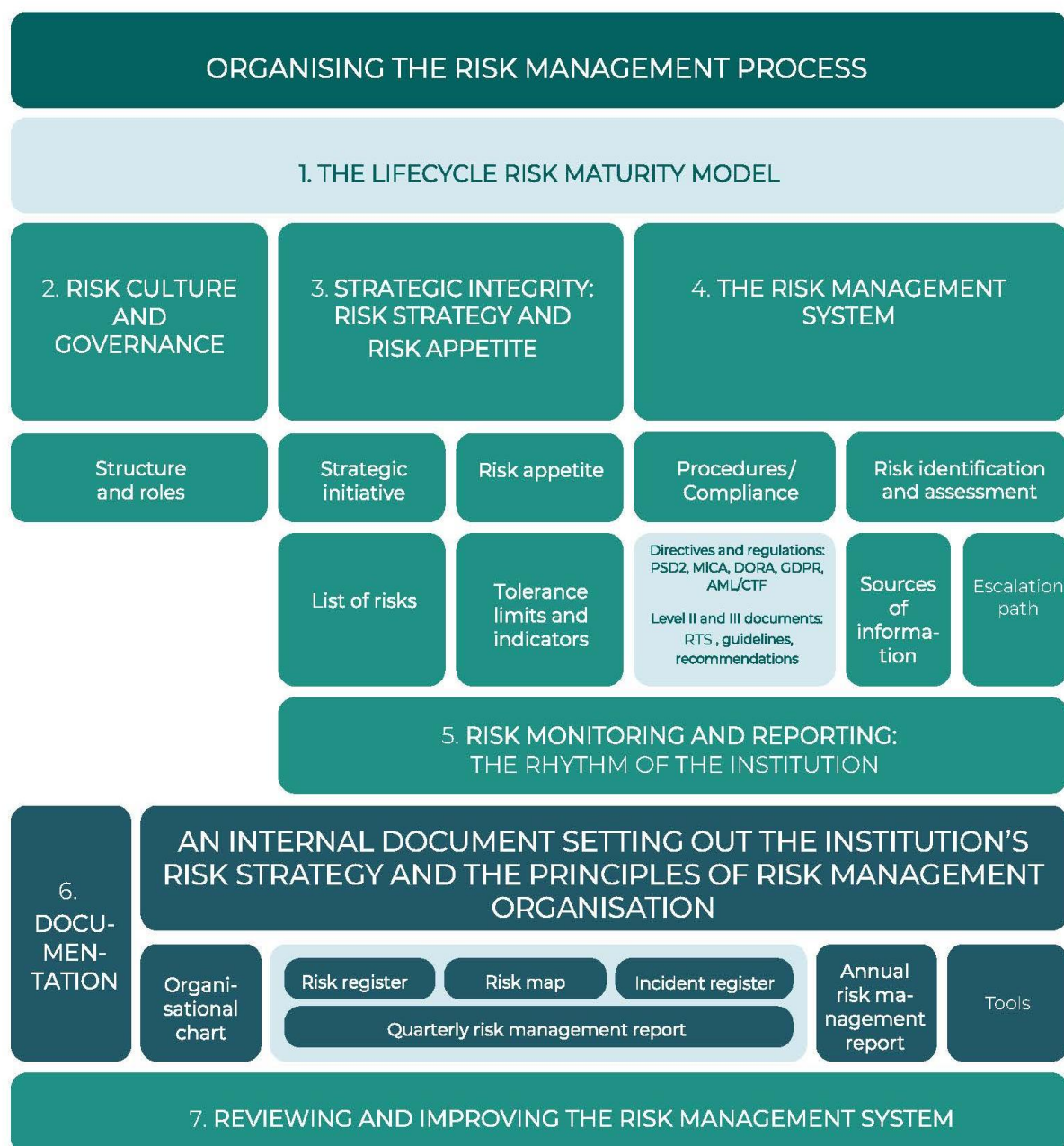
The recommendations of the Guidelines should be followed by institutions and, *mutatis mutandis*, by branches of foreign electronic money institutions, unless otherwise specified in the Guidelines. It is recommended that the Guidelines be applied to small institutions in such a way as to ensure that the recommendations and the examples of best practices given in the Guidelines are reasonably translated in, and adapted to, the day-to-day operations of small institutions, and that an effective risk management process becomes an integral part of the institution's operations. The maturity of the risk management system should be in line with the guidelines for the lifecycle phases of the institution, except where the risk appetite would require higher maturity guidelines.

It is recommended that institutions implement the Guidelines on a proportionate basis, taking into account the criteria set out in paragraph 8 of the Description, the lifecycle phase described in Chapter 1 of the Guidelines, the service distribution channels, as well as the institution's risk strategy, risk appetite, and actual risk profile. When assessing the proportionality of activities, institutions should consider whether they are part of a group of companies or not (if so, assess proportionality at the group level). Where institutions decide to increase their risk appetite, i.e. to change the limits of existing risk tolerance (risk limits), to provide riskier services, to deal with higher-risk customers, to change their business model, to increase the volume of service/sales, etc., appropriate risk management maturity must be ensured, and sufficient time and resources for preparation and implementation must be allocated.

Organising the risk management process

The organisation of the risk management process consists of a set of principles, strategies, policies, internal procedures, governance practices, communication channels, and competences, and the involvement of managers, key function holders, and other employees in the management of the activities established and applied by the institution, including the risks associated with those activities (see Figure 1).

Figure 1. The organisation of the risk management process and the structure of the Guidelines



The organisation of the risk management process is an integral part of any institution's activities, and risk management maturity should increase with the institution throughout its lifecycle. Chapter 1 of the Guidelines introduces the maturity of the risk management phases to the institution's lifecycle, which gives a basis for the application of the proportionality principle. Chapters 2 to 7 describe the elements of a risk management system and provide examples of best practices.

Institutions should ensure the high quality and effective organisation of the risk management process in their operations, which is closely linked to the following factors:

- the institution's business model is in line with its current licence;
- the institution complies with its own funds requirements;

- the institution has a common understanding of its strategic objectives, customers, and the scale and complexity of its activities across all management and operational levels;
- the organisation of the risk management process is understood as a means of implementing the operational strategy, and runs through the shareholders, the supervisory and collegial management bodies, and the management of the institution, which promotes a risk culture based on openness;
- the organisation of the institution's risk management process is integrated into other governance processes of the institution;
- the institution's performance, including financial performance and risk-taking, is planned and managed at regular (daily, weekly, monthly, quarterly, etc.) meetings in line with clearly defined and communicated strategic objectives and indicators;
- the institution has adopted a clear approach for identifying and addressing problems and risks, including internal control and audit, and has allocated responsibilities and authorisations at all operational levels of the institution;
- each employee of the institution has a clear understanding of their role, responsibility, and accountability, and the substitutability of competences and prevention of conflicts of interest are ensured;
- risk tolerance limits (risk limits) are regularly monitored; risk management reports, including a risk map, are provided at least quarterly; and an annual risk management report is prepared and submitted to the institution's collegial management body for evaluation;
- the annual review of the risk strategy, risk appetite, and the risk management system, as well as the planning of improvements in the organisation of the risk management process, should be synchronised with the business objectives, the strategy, and the annual Enterprise-Wide Risk Assessment (EWRA), and should not be limited to internal/external audits only.

1. The lifecycle risk maturity model

The lifecycle of an institution starts with obtaining a licence and is divided into four phases: baby born, grow, scale, and rocket.

The risk management system and related competences are developed to match the maturity of the institution and to ensure appropriate risk management in line with the growth rate, the complexity of the business, and the chosen risk appetite.

The evolution of the maturity of the institution's risk management throughout its lifecycle is briefly outlined below, and a more detailed description of the phases in the institution's lifecycle can be found in the Annex entitled "Fintech lifecycle risk maturity model".

The baby born phase

The institution is licensed, with a limited initial team size. Funding is an essential prerequisite for the implementation of the initial business plan and growth. The basic assumptions of the business plan are verified, preparations are made for implementation and start-up, relationships with the first customers are established, competences are developed through experience, and new team members are added. This phase usually lasts between one and two years and is only possible in cases where the institution is not part of a group of companies or a branch of a foreign electronic money institution, but rather a new separate licensed entity that starts its licensed financial activities from scratch, or where a small institution licence is issued.

The licensing process includes the approval of an initial set of documents setting out the principles of the organisation of risk management in the institution and the establishment of essential compliance and cybersecurity processes. The role of the risk management officer may initially be performed by several members of the team. The governance structure is simple, ensuring simplicity and speed of information transfer and decision-making in a risk-sensitive manner (e.g. direct communication and the transfer of information to the management and/or members of the collegial management body of the institution). In addition to formal quarterly reporting to the institution's collegial management body, the team informally assesses and reviews risks on a daily basis. Risk management decisions and actions are taken and implemented immediately or very soon (after between one hour and three days) in response to changes in internal and external factors. The team uses simple tools such as xlsx, ppt, Trello, ClickUp, Basecamp, Microsoft Planner, or MeisterTask, and dashboards such as Miro, etc. to record decisions and report on implementation.

The risk strategy is part of the business plan. The risk management system and culture are developed and adapted according to the chosen growth rate and risk appetite, which is agreed by the shareholders, the collegial management body, the entire original management team, and the team of risk professionals.

The grow phase

Once the institution has started to provide services to its first customers, it enters the grow phase in the market segment identified (selected) in the business plan that has been approved at the time of licensing. The institution then grows somewhat vertically. The team is already larger than in the baby born phase and is continuously growing according to demand, with a strong focus on bringing in new members of staff and developing the competences of current employees. Funding is still important, and there is a gradual focus on efficiency and increasing revenues for profit, but compliance continues to be key in this phase. If key strategic assumptions or the business model change in this phase, then the risk strategy is redefined and the risk appetite is redetermined. Additionally, the whole package of internal documents setting out the principles of the organisation of risk management within the institution is adjusted, the team is strengthened, IT solutions are implemented, etc. The faster the growth rate and/or the more risk posed by the customer, service, or geographic areas that are selected, the faster the risk management system must be improved. Risk management from the very top of the management of the institution is seen as an essential part of the implementation of the business plan.

The risk management system and key processes are not only documented, but also consistently applied through established procedures. The same simple tools, including xlsx, ppt, Trello, ClickUp, Basecamp, Microsoft Planner, MeisterTask, or dashboards such as Miro, etc., are still used to record decisions and report on implementation. Activities and risks are planned and monitored on a regular basis, with weekly or monthly reporting, and managers gradually involve all staff of the institution and ensure that everyone understands their role in risk management.

The risk strategy, the identification of material risks and risk appetite, and the need for all necessary resources are planned annually along with the planning/review of the operational strategy, more often taking the top-down approach. These processes are primarily the responsibility of the collegial management body, the managers, and the risk management officer, and ensure effective communication with all employees of the institution.

The scale phase

The *grow* phase is more vertical, whereas the *scale* phase is more horizontal. This consists of expanding the range of services and/or customer segments, and/or entering new markets, and/or using agents or partners to develop services. In this phase, the team significantly increases in size, and there is an increase in complexity and the role of technical innovation in managing compliance requirements and risks. The management structure also moves to become in line with cross-jurisdictional requirements and ensures efficient resource allocation and risk management.

Risk management is fully integrated into the business strategy and data analytics and insights are used to develop the business strategy and make business decisions in this phase. More sophisticated risk management tools, such as Jira, Asana, Monday.com, Smartsheet, or in-house tools, are used, and automated technical control solutions are deployed and integrated into day-to-day processes.

During the *scale* phase, there is continuous or regular feedback, and a well-established cycle of planning, monitoring, reporting, and review ensures that information is shared both horizontally and vertically within the institution. At the same time, risk maturity is increased to meet to the needs of the business, and global involvement in risk management is encouraged not only from the top down, but also from the bottom up. Compliance is a particular focus in this phase.

The rocket phase

The institution enters this phase either as an entity of public interest or as a result of its own strategic decision. As a significant and growing player in the financial market, the institution not only continues to develop its activities in all areas in order to maintain its competitive advantage, growth, and profitability, but also pays particular attention to compliance. In this phase, preparations for an initial public offering (IPO) may be underway, which may include a merger or other exit strategy.

The institution's risk management practices may influence and/or set, change, determine market-wide standards. Risk management tools are now fully automated, and risk management is no longer simply part of the operational strategy, but rather prompts the need for new innovations and strategic solutions.

2. Risk culture and governance

Risk culture broadly refers to an institution's comprehensive understanding of, assessment of, and response to risks. In addition to its ability to effectively identify, assess, and manage risks, the risk culture has a direct impact on the achievement of the institution's business strategy and objectives.

Paragraph 12 of the Description provides that the management bodies of the institution must establish an integrated, reliable, and consistent risk culture within the Institution.

A sound and consistent risk culture is an essential component of an effective risk management system in any institution, and ensures risk-based and informed decision-making. The risk culture includes: the clear communication of risk tolerance limits (risk limits), the involvement of staff in the organisation of the risk management process, leadership by example in risk management practices, the discussion of risks as a common practice in the institution's daily or weekly processes, continuous learning and development, and the communication of risks. Institutions should integrate a risk culture into their internal control system based on a holistic approach to risk, and taking into account their risk appetite and risk tolerance limits (risk limits). They should also continuously monitor, identify, assess, and manage the risks arising in their activities in a timely and appropriate manner.

The internal controls of the institution should ensure sound and prudent governance, while effective risk management should form an integral part of the institution's good governance. Thus, the development of an institution-wide risk culture should become one of the institution's priority objectives, as this has a direct impact on increasing the institution's risk maturity, as appropriate, on a lifecycle basis.

It is recommended that risk culture within institutions be based on at least the following three principles:

A top-down approach to risk management: The institution's supervisory and collegial management bodies and other senior managers take responsibility for shaping the approach to risk management as a prerequisite for the implementation of the institution's business strategy. They also set an example in terms of how to approach risk,

emphasise strategic and value integrity, and ensure resources and conditions for the independent operation of risk professionals.

Openness and accountability: Every staff member must understand their role in the risk management process. Everyone should know how to act and/or initiate change in risk management as a result of changes in risk observed through indicators and early warning signals (see Chapter 3), and be responsible and accountable to the team for their actions, results, and mistakes.

Global involvement: Risk appetite (see Chapter 3) is integrated into decisions in a way that is understandable to everyone, and the risk management system (see Chapter 4) is integrated into day-to-day operations. The risk management system is improved and competences are developed with the help of self-assessment and open and constructive feedback at all levels.

As an institution's risk culture should be implemented at the institution-wide level, the risk management process within the institution should not only involve risk professionals or internal control functions, but also managers and other departments of the institution and their staff.

The risk culture of the institution should start first and foremost with the responsibility of the institution's supervisory and collegial management bodies for defining the core values and expectations of the institution. The supervisory and collegial management bodies of the institution should demonstrate these values and expectations in their day-to-day behaviour and communicate them to the institution's employees, either verbally or through certain actions/decisions. It is the responsibility of the supervisory and collegial management bodies of the institution to clearly communicate to the staff their responsibility for risk-taking behaviour, to train and develop an open, constructive, and critical approach, and to encourage active involvement and participation in the day-to-day running of the institution.

The institution should choose means of communication, training, and involving staff in the organisation of the risk management process in such a way that the staff have a proper and clear understanding of the institution's core values and expectations and are able to act within their remit in their day-to-day activities in compliance with all applicable legal requirements. Staff should have a clear understanding of their responsibility for the day-to-day risk management of the institution, i.e. they should know and understand the core values of the institution; understand that they will be held accountable for their actions in relation to risk management; and, to the extent necessary for the performance of their duties, be aware of the institution's risk appetite and the limits of its risk tolerance (risk limits).

The supervisory and collegial management bodies of the institution must continuously monitor, assess, and maintain the risk culture in the institution and monitor its impact on internal governance, and make changes where necessary.

It is best practice, through transparent communication, to notice and identify errors, assessing and addressing them before they are noted and assessed by supervisors. The case study method, which involves sharing/discussing lessons learned and best practices through communication at all levels of the institution (with managers, unit employees, and cross-functional teams), could be an effective tool to develop a risk culture.

Structure and roles

Compliance with the requirements of paragraph 28 of the Description is essential in order to ensure that the organisational structure of the institution is appropriate and comprehensible. However, regardless of the governance model/organisational structure chosen, the institution should have an effective risk management system in place, with internal documents clearly defining the roles and responsibilities of all supervisors,

collegial management bodies, managers, employees, and related parties in the risk management process, along with their accountability and communication channels.

Paragraph 37 of the Description sets out that **the supervisory body of the institution** must approve an internal document setting out the Institution's risk strategy and the principles of risk management organisation.

In assessing the effectiveness of the risk management system, best practice involves an institution having ad hoc meetings, initiated by the institution's own supervisory body, with the institution's collegial management body or risk management professionals to clearly identify and communicate the formats in which information must be provided in order to avoid potential abuses or delays in communicating emerging risks. Failure to implement this would not only lead to late risk management decisions, but could also have a significant impact on the implementation of the operational strategy.

Subparagraph 28.1 of the Description requires **the collegial management body of the institution** to approve the institution's detailed organisational chart. Moreover, paragraph 42 requires the institution's collegial management body to establish procedures for keeping the registers referred to in paragraphs 40 and 41 of the Description (risk and incident registers). It also requires them to assess the institution's quarterly risk management report, which must include a risk map, at least quarterly, and assess the annual risk management report at least once a year (paragraphs 43 and 44 of the Description).

The supervisory and collegial management bodies of the institution should continuously monitor, assess, and maintain the risk culture of the institution; consider the impact of the risk culture on the financial stability, risk appetite, and sound governance of the institution, and make adjustments, where necessary; integrate the risk culture into the institution's internal controls system, within the defined remit; ensure the establishment of risk-based governance within the institution; and approve the institution's well-defined business strategy and other internal documents (policies, procedures, processes). The latter documents should clearly define the institution's risk appetite and risk tolerance limits (risk limits), along with the responsibilities and accountabilities of the institution's managers, holders of key functions, persons responsible for implementing internal controls, heads of units, and their subordinates in the area of risk management, and should be reviewed and approved at least once a year.

Failure to do so in a timely manner risks delays in informing the supervisory and collegial management bodies of the institution about emerging risks, which not only leads to late risk management decision-making, but may also have a significant impact on the effectiveness of those decisions and increase the cost of implementation.

Best practice regarding governance encourages collegial decision-making, and it would therefore be appropriate to create advisory committees within the institution involving operational managers (process owners) and the risk management team, such as a Compliance Committee, a Risk Committee, a Partner Risk Committee, etc. These advisory committees should address risk-related issues, as well as consider the selection and effectiveness of controls. In addition to formal advisory committees, regular meetings of cross-functional teams could be used to support collegial decision-making and should be integrated into the overall business cycle of the institution (see Chapter 5).

Subparagraph 20.3 of the Description stipulates that the institution must designate a person responsible for ensuring risk management (risk management officer) who must meet the requirements of paragraph 25 of the Description.

Risk management officer. This person should be the owner of the risk management process, the coordinator of risk management, and the centre of excellence within the institution. They should have sufficient knowledge, skills, and experience of risk management practices and procedures, the services and products provided by the institution, the channels through which they are provided, customers, and the jurisdictions in which they

operate. The appointment and accountability of the risk management officer is described in a greater detail in paragraphs 20 to 26 of the Description.

The responsibilities of the risk management officer include monitoring and analysing risk trends, assessing risk appetite and risk maturity, proposing risk strategies to the collegial management body and coordinating their implementation, initiating proposals for the development of the overall risk management system (policies, processes, procedures, tools, technologies), coordinating the development of staff competence in the area of risk management, and ensuring the quality and regularity of timely data-based internal communication and reporting.

Paragraph 39 of the Description provides that the risk management officer must be involved in the preparation of the internal document setting out the Institution's risk strategy and the principles of risk management organisation, and should take part in all decisions regarding the management of significant risks. The risk management officer should be able to directly inform the supervisory body and the collegial management body of the Institution of existing or potential changes in risks that may have a negative impact on the Institution.

Paragraph 12 of the Description sets out that risk management responsibilities must be delegated not only to the risk management officer, but also to all the departments of the institution, taking into account the acceptable level of risk and the risk-taking capacity of the institution.

Institutions should allow the risk management officer to be independent from the business units they control with regard to risk management, but should not be prevented from maintaining contact with them. Institutions should provide the necessary conditions, authorisations, and access for the risk management officer to address all business lines and other internal units of the institution that may be exposed to risk, as well as to subsidiaries and associates of the institution; obtain full information that may be relevant to risk management; and have access to both the information necessary for the performance of their duties and the necessary information technology (e.g. access to the relevant databases, systems, reports, and reporting access).

The risk management officer should be actively involved in all major risk management decisions. They should have the right and real opportunity to attend meetings of all supervisory and collegial management bodies of the institution, advisory committees (in particular the risk management committee, if any), project teams, and other business units, regardless of whether or not they are a member; and receive all the information necessary for such decision-making; ask questions, express their views, and make proposals to the management of the institution concerning the allocation of sufficient human resources and/or working time to risk management activities and the other resources necessary to ensure risk management. The institution should enable the risk management officer to engage in regular training and continuous professional development through a variety of external training formats and/or allow for the recruitment of an independent risk expert, or for the outsourcing of some risk management functions.

Paragraphs 43 and 44 of the Description provide that the risk management officer must submit the institution's quarterly risk management report to the institution's collegial management body, including a risk map, at least quarterly, and the annual risk management report should be submitted once a year.

The role of the risk management officer should evolve according to the lifecycle and maturity of the risk management system: as maturity increases, more and more day-to-day controls and decisions should be transferred to innovative performance management processes and delegated at all staff levels. In the baby born phase of an institution, the role of the risk management officer can be aligned with that of another officer (e.g. for compliance or cybersecurity, Chief Information Security Officer, CISO), and as the institution grows, each position should be filled by employees with the appropriate expertise.

This practice applies not only to the risk management officer, but also when a combination of roles is chosen to perform the function, and when the functions of the institution's risk management officer are combined with the outsourcing of some of the operational risk management functions.

Best practice is to provide for the substitutability of the risk management officer at the outset, taking into account potential conflicts of interest, and to ensure that the risk management officer is involved in the strategic planning process and in regular meetings of the collegial management body and other senior managers, and feels the pulse of the business from the very beginning.

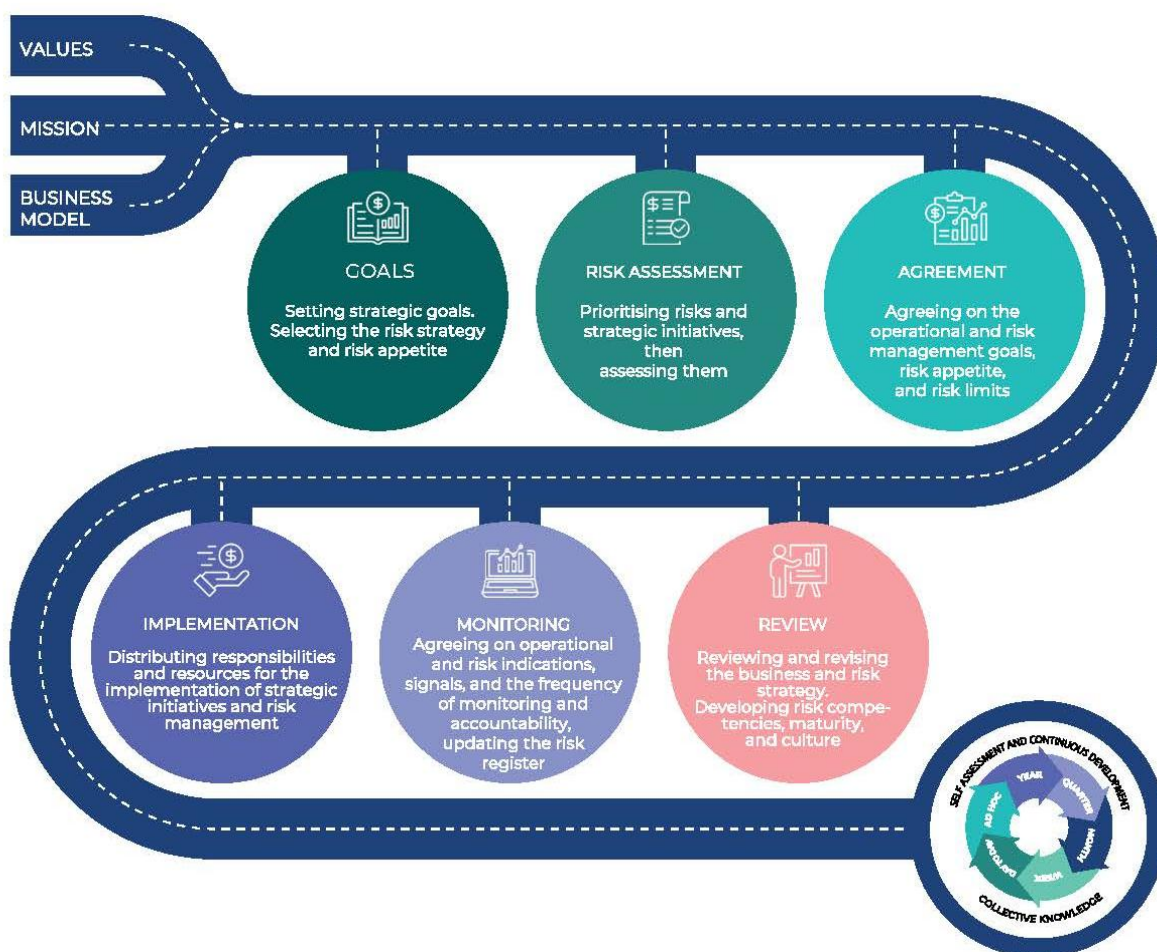
The institution's internal documents should provide for effective conflict of interest management measures to identify and effectively manage conflicts of interest – both at the level of the collegial management body and at the staff level – that could lead to biased, arbitrary, or unjustifiably risky decisions. They should also ensure the independence of members of collegial management bodies in terms of their views and the impartial and independent functioning of the internal control/risk management functions, as defined in paragraph 13 of the Description.

3. Strategic integrity: risk strategy and risk appetite

Strategic integrity ensures that all components of the institution's business (culture, structure, processes, resources, agreements, decision-making, etc.) work in synchrony and contribute to the long-term success of the institution. Strategic integrity helps the institution to maintain a focus on its long-term objectives, regardless of internal or external changes, and to achieve consistent growth, ongoing progress, and competitive and sustainable development.

The principles for the organisation of the risk management process should be developed in light of the institution's lifecycle, strategic objectives, and initiatives. The recommended actions for an integrated process at the strategic level are shown in Figure 2.

Figure 2. Integral process at the strategic level



The strategic initiative forms an integral part of the evolution and maturity of the institution's lifecycle. It enables the institution to act originally and/or promptly react to new opportunities, adapt to ongoing changes and, accept new challenges in order to achieve its long-term objectives or improve its performance. Strategic initiatives may include such areas as the development of new services or products, the implementation of technology, changes in the culture of the institution, refocusing, expanding into new markets, marketing activities, etc., and should be closely linked to the institution's risk strategy, risk appetite, and the design of the implementation of the risk management process.

The risk strategy refers to a strategic decision by an institution on how to manage risks while implementing its business plan and pursuing its strategic business objectives or initiatives. The risk strategy defines the risk appetite and sets out plans regarding the organisation and development of the risk management system (see Chapter 4). The principles for the organisation of the risk management process should be developed in light of the institution's lifecycle, strategic objectives, and initiatives.

The risk strategy should not only be described in an internal document setting out the Institution's risk strategy and the principles of risk management organisation, but should also be integrated within the overall operational strategy of the institution and described in a document that elaborates on it (an operational or business strategy).

Paragraph 37 of the Description provides that the internal document setting out the Institution's risk strategy and the principles of risk management organisation must include the list of risks, the description of the risk appetite, and tolerance limits for each risk.

Adequate risk identification and assessment are key factors in assessing the effectiveness of the institution's internal control system for risk management. Only by following the proper identification and assessment of risks relevant to its business is the institution able to put in place sufficient controls to manage those risks, to determine its risk appetite and, to make decisions related to those risks.

Paragraph 36 of the Description provides that the institution shall have in place an effective risk management system covering the management of the actual and probable risks that arise or could arise from the issuance by the institution of electronic money, the provision of payment services and other services, the investment of funds received from holders of electronic money and/or payment service users or other payment service providers, and other steps taken to safeguard customer funds or as part of other activities. The latter may include: the management of settlements, liquidity, operational funds, money laundering and/or terrorist financing, international sanctions, fraud, information and communication technology, security, data protection, compliance, markets, counterparty credit, concentrations, customer behaviour, etc. The Description provides a minimum **list of relevant risks**, which is to be expanded to include risks relevant to the institution in question depending on the scale of the institution's operations, the nature of the services provided, and other circumstances.

This list of risks should additionally cover at least the risk of third-party influence and, where relevant, risks related to agents, distributors, or partners, taking into account the need to include strategic, political, reputational, social, and cultural risks. Risks may be described individually or aggregated into categories at the discretion of the institution. However, it is important not to limit the description to general risk categories, but rather to show the relevance of each risk by combining factual data and forward planning.

Best practice is considered to include sustainability risks. Sustainability risks include events or situations arising from environmental, social, or corporate governance domains which, if they were to occur, could potentially have a negative impact on the institution's assets, financial position, or profits, as well as its reputation (for further details on sustainability, please refer to relevant sustainability-related legislation, such as Regulation (EU) 2019/2088 on sustainability-related disclosures in the financial services sector, etc.).

The amount of risk that an institution is willing to assume and the scale and nature of the associated risk management actions should be consistent with and aligned towards its strategic objectives. For this purpose, institutions need to determine the risk they are willing to accept (risk appetite).

Risk appetite refers to the maximum risk that an institution is willing to accept in relation to its chosen business model, customer segments, and factors such as its reputation, capital, assets, and ability to attract additional investment. Given the licensing of its activities, the institution, in identifying/reviewing its risk appetite, should take into account guidance from supervisory authorities, recommendations, and best practices, and follow their

changes on an ongoing basis. The acceptable level of risk is described by **key performance indicators (KPIs)**, **key risk indicators (KRIs)**, and **early warning indicators (EWIs)**, which not only reflect the actual situation, but also provide a warning of possible changes in the future and the need for action.

In light of changes in the institution's strategic objectives, performance (e.g. the institution's operational efficiency, the positive view of its performance by its customers, supervisory authorities, and shareholders, and the improvement of the institution's reputation), and the regulatory environment, risk appetite should be regularly reviewed in response to changes, striking a balance between exploiting its business potential and mitigating risks.

One of the key objectives of risk management is to keep up-to-date and high-quality information on the risks relevant to the institution and to inform, in a timely manner, the management at all operational levels of the institution to ensure that decisions posing a risk to the institution's operations are only taken when subject to a full assessment of their potential impact and the status of risk management. The main tool used to achieve this objective is, in practice, the setting and adaptation of risk tolerance limits (risk limits) to the strategic objectives set by the institution.

Risk tolerance limits (risk limits) are threshold levels of risk exposure that should prompt the notification of management if they are exceeded. They should be included in the risk strategy, and actions should be taken in accordance with the internal document setting out the Institution's risk strategy and the principles of risk management organisation (e.g. obtaining management approval for exceeding risk limits, informing the management of the situation for further decision-making (planning actions), implementing additional risk management tools, etc.).

Paragraph 37 of the Description provides that the internal document setting out the Institution's risk strategy and the principles of risk management organisation must determine tolerance limits for each risk.

It is considered to be best practice if risk tolerance limits (risk limits) are also established for risk categories (if risks are aggregated into categories), taking into account the specific nature of the institution's business and the interactions and interrelationships among the risks specific to the institution.

Risk tolerance limits (risk limits) define acceptable deviations from the targets set, which are linked to **performance and/or risk indicators (KPIs, KRIs, and EWIs)**.

KPIs are used as a quantitative or qualitative performance measure to assess the performance, efficiency, and progress of an institution in relation to its objectives. KPIs help to identify areas where changes are needed and to monitor ongoing progress towards strategic initiatives/objectives.

KPIs are key performance management tools for measuring the institution's effectiveness and decision-making on the basis of actual data. KPIs should be linked to a specific objective or area, and contribute directly to the evaluation of strategic initiatives/objectives. They should be objective and easily measurable over a period of time. Examples of KPIs include profit margin, revenue growth, cost reduction, error rate in payment transactions, speed of processing transfers, increase or decrease in complaints, etc.

KRIs are quantitative or qualitative data and/or measures used to identify, at an early stage, the likelihood of the occurrence of a risk and its potential impact on the institution's objectives.

KRIs both serve as an indication of the current level of risk and are used to plan and monitor identified risks. KRIs help an institution to be proactive as they allow for the early identification of risks and the implementation of risk mitigation measures before those risks significantly affect the institution's operations.

KRIs are designed to assess a specific area or factors and are used to focus on the most important risks that could significantly affect the institution's performance, and should be clearly defined and regularly measured to

be effective and informative regarding potential increases in risk, enabling the institution to address the potential impact of risks in a timely manner. Examples of KRIs include debt-to-asset ratio, number of security incidents, incidents of data breaches and frequency of data loss, interruptions in outsourcing, etc.

EWIs include information or signals that enable an institution to anticipate changing levels of risk or threats, to identify potential deviations from the institution's plans, and to promptly respond in order to avoid adverse consequences.

EWIs are designed to monitor risk warning signs before they materialise, allowing an institution to detect potential deviations at an early stage and to take effective and timely decisions.

As EWIs help the institution to foresee future risks and/or problems, they should be defined in concrete numbers or monitored using qualitative parameters, focusing on critical areas which would enable the institution to receive early warnings of potential risks in order to allow sufficient time for necessary actions or decisions. Examples of EWIs include deviation of fund flows from financial forecasts, increase in debt, high staff turnover, declining number of customers, increase in outsourcing costs, disruption of payment processes, liquidity ratio approaching a critical threshold, etc.

The institution should ensure compliance with the established risk tolerance limits (risk limits) and the recording of their deviations, which is why the establishment and monitoring of these indicators is a key tool for setting risk tolerance limits (risk limits), thereby giving the institution an early warning of the potential realisation of a risk.

It is important not only to identify, but also to actively use such performance/risk indicators as a basis for decision-making, both at the strategic and project levels of the institution. This enables it to improve existing processes, products, and services, introduce new processes, products, and services, and monitor processes on a regular basis.

Best practice is to interconnect and regularly monitor KPIs, KRIs, and EWIs as a whole on dashboards.

The requirements and timeframes for risk appetite, risk tolerance limits (risk limits), KPIs, KRIs, and EWIs should be regularly reviewed within the institution. An effective internal communication mechanism and an effective decision-making process should ensure that every employee of the institution is involved, informed of the established risk tolerance limits (risk limits), held accountable, and encouraged, and that managers are notified of breaches of the institution's internal controls, their ineffectiveness, and the identification of additional risks. In the event that such a breach or ineffectiveness would exceed the institution's risk tolerance level, steps should be taken to make sure that the management is informed.

Risk appetite and risk tolerance limits (risk limits) form an important part of business and risk planning and monitoring, as they serve as a basis for the risk registers and maps described in Chapter 6.

While the *baby born* phase in an institution's life focuses on liquidity and compliance risks, it should not be forgotten that the types and extent of risks relevant to an institution begin to change rapidly once the institution becomes active. The qualitative assessment incorporates actual data and indicators, and it is therefore important not only to set risk tolerance limits (risk limits) in the internal document setting out the Institution's risk strategy and the principles of risk management organisation, but also to actively use them as a basis for decision-making, both at the strategic level and at the project level. This would promote the improvement of existing processes, products, and services and the introduction of new processes, products, and services, as well as the consistent monitoring of processes.

It is best practice to have an effective internal communication mechanism and escalation path in place at all phases in an institution's life, thus ensuring that every employee of the institution is involved, informed of the established risk tolerance limits (risk limits), held accountable, and encouraged. This also ensures that

managers are notified of breaches of the institution's internal controls, their ineffectiveness, and the identification of additional risks. Where such a breach or ineffectiveness would exceed the institution's risk tolerance level, this would ensure the timely and proper notification of the management.

4. The risk management system

Paragraph 36 of the Description provides that institutions must put an effective risk management system in place in order to ensure that risks that may affect the institution's activities are identified and assessed on an ongoing basis, that new or previously uncontrolled risks are identified and appropriately assessed, and that the institution takes appropriate measures to control/mitigate the risks.

A risk management system is a systematic and iterative process for identifying, assessing, monitoring, controlling, and responding to risks. It consists of a set of principles, strategies, policies, internal procedures, governance mechanisms, and communication channels established and applied by an institution. Additionally, it entails the competences, behaviours, and involvement of its managers, holders of key functions, and employees in the management of its activities, including the risks associated with them. The risk management system should therefore be integrated into the internal control system of the institution and apply to all activities of the institution, its management bodies, and its business units, including those performing internal control functions. The risk management system should enable the institution to make informed decisions on risk-taking.

As the activities of the institution are licensed and regulated, the institution should remember to integrate, in the application of the risk management system, other compliance elements that are closely related to the regulation of activities and have a direct relation to the identification, assessment, monitoring, and control of potential risks. The institution should assess the responsibilities arising from legally binding EU legislation (directives and regulations) and should integrate second- and third-level documents for the implementation of the measures imposed by directives and regulations, such as regulatory technical standards (RTS), guidelines, and recommendations.

In accordance with paragraph 37 of the Description, the institution should draft and approve an internal document setting out the Institution's risk strategy and the principles of risk management organisation. In addition, steps should be taken to draw up and regularly update other **documents relevant** to the seamless organisation of the risk management process, such as an organisational chart, risk maps, a risk management improvement plan (if relevant), an annual risk management report, as well as risk and incident registers (see Chapter 6).

Paragraph 38 of the Description states that the institution must establish internal procedures to identify, assess, monitor, and control/mitigate risks. The institution is free to choose the format (digital or documentary) for internal procedures, but it is important that they comply with the content requirements set out in paragraph 18 of the Description. **Internal procedures** must specify how regular and continuous compliance control is carried out, the frequency of such control, and the human resources allocated for this purpose; the measures to ensure the dual internal control of operational procedures (e.g. the four-eyes principle); the decision-making procedure; the functions, rights, duties, and accountability of the responsible bodies and persons of the institution; the information and communication technologies used for such control; the sources of information; and, where applicable, the means of ensuring that the necessary information is obtained from third parties.

In order to facilitate and streamline the organisation of the risk management process within the institution, it is recommended to produce a description of the risk management system process to identify how the risk management system is implemented in the institution, i.e. establish **the process of the risk management system, covering risk identification, assessment**, monitoring, mitigation, and other controls. The description of the risk management system process should detail the roles, responsibilities, accountability, and reporting frequency for each manager and employee; decision-making procedures; human resources; information and

communication technologies used; procedures for the approval and use of other resources needed for the risk management system; the processes, procedures, and tools implemented in relation to the risk management system; and document templates used (e.g. risk management procedures, change management, escalation path, risk communication, decision-making, conflict of interest management, handling resources for risk management, etc.).

It is recommended that the description of the risk management system process should include the following provisions describing risk management and the risk strategy:

- the flow of the risk management system process;
- the detailed responsibilities and accountabilities of the staff responsible for the risk management system process;
- a glossary of risk terms;
- risk appetite, detailing the identifiable risk appetite for each type of risk;
- risk tolerance limits (risk limits) (allocating risk appetite and setting risk tolerance limits (risk limits) for a functional unit of the institution and/or a project or activity, depending on the scope of the activity);
- the assessment criteria, content, likelihood, impact, and significance of each risk;
- risk control measures (setting EWIs and KRIs for the implementation of continuous control);
- risk mitigation actions along with their implementation cost, resources, and the evaluation of their effectiveness;
- the content of the risk management reports and their submission to the institution's collegial management body (paragraphs 43 and 44 of the Description) and other stakeholders, i.e. the procedure for the preparation of quarterly risk management reports, including risk maps; the annual risk management report; the types of monitoring; as well as the deadlines and procedure for submitting the results of these reports to the institution's collegial management body and other stakeholders;
- the decision-making process for the inclusion of new risks and risk management measures;
- the principles of the annual evaluation, development, and maturity of the risk management system process, taking into account the lifecycle (phases) of the institution.

As the risk management system is developed and refined throughout the lifecycle of the institution, the institution may also develop other internal documents or create smart active links in its internal systems (e.g. a risk management system process tree, etc.) describing the provisions of the risk management system process. Measures may also be developed to identify the need for and importance of integrating changes into the risk management system.

It would be considered best practice to develop individual risk management process flowcharts with specific functions and document templates and incorporate them into internal documents, while keeping the links and references to them up to date.

In order to properly **identify and assess the risks relevant to it**, the institution should first clearly define them, as described in Chapter 3.

In order to have a proper understanding of the likelihood of occurrence and the potential impact of each risk, it is also recommended to assess and describe risk factors in advance. These factors should be understood as the

events, situations, circumstances, or particular causes that could lead to or increase the likelihood of occurrence of a risk. Examples include a weak internal control mechanism within the institution which would increase the likelihood of a financial risk, a lack of staff competence which would increase the likelihood of operational risk, or incomplete and inconsistent internal documentation which would increase the likelihood of compliance risk. Risk factors would help the institution to understand why and how a risk occurs, as without identifying risk factors and analysing their causes, real situations, and scenarios, the institution would not be in a position to effectively assess the likelihood of occurrence of a risk and its potential impact, and to put in place effective risk management measures.

The following **sources of** internal and external **information** are used to identify risks depending on the scale, complexity, and lifecycle phase of the institution: (a) anticipated regulatory and legislative changes; (b) risk indicators and risk management reports; (c) internal and external audit reports; (d) insights and recommendations from an independent consultant specialising in risk management (if engaged by the institution) and/or the institution's team with control functions; (e) incident register; (f) operational risk assessment; (g) business strategy assumptions and planning; (h) financial forecasts and/or operational budget planning; (i) performance indicators and their dynamics; (j) innovations and planned changes and the implementation of lessons learned; (k) customers and partners; (l) data generated with the help of analytical and information technology tools; and (m) regular EWRA, an institution-wide process of the reassessment of risks and the evaluation of the effectiveness of the risk management system on at least an annual basis.

Best practice would be to involve customers, agents, and/or partners in the institution's business strategy and risk planning process, wherever possible, through periodic surveys of (dis)satisfaction with the use of services or products, feedback analysis, etc.

While an institution may choose how to identify and assess the risks relevant to its activities, it is important to apply effective and appropriate methodologies and tools that include not only the identification and assessment of existing risks, but also the identification of the likelihood of reoccurrence of past factors, their actual impact, and the identification of potential new factors in the future. These methodologies and tools should enable institutions to properly assess whether the relevant risks and their estimates are consistent with the institution's stated risk appetite (see the "Risk assessment process" table).

With the increasing volume and complexity of activities, best practice would be to automate, at least partially, the identification and assessment of risks and to integrate technical and technological solutions into institutions' internal procedures.

Escalation path. The internal procedures developed by institutions must set out not only the procedure for setting and including new risk tolerance limits (risk limits) in the risk register, but also a clear method of communication.

This process must clearly define which important or critical information related to a risk, incident, or problem must be communicated in a timely manner to the responsible persons and/or managers. The escalation path should ensure that the supervisory or collegial management body of the institution, or the managers of the institution or the responsible professionals/teams, make timely decisions on the necessary and imminent actions to be taken. If the situation involves legal, regulatory, or public aspects, the institution should determine when, by whom, and how information should be communicated to the supervisory authorities (not only Lietuvos bankas, but also the State Data Protection Inspectorate, the National Cyber Security Centre, the Financial Crime Investigation Service, etc.), partners, etc. In order to ensure effective decision-making, the document describing the escalation path should clearly define when and how the information is to be communicated and who is responsible for its communication.

Risk assessment process

Risk assessment				
Purpose	Tasks	Information to be obtained	Information to be prepared	Tools and methodologies to be used
To identify individual key risks in order to clearly distinguish the risks requiring urgent action, to understand the likelihood of realisation, the realisation potential, and the potential impact of each threat, as well as its proximity (when they will be realised).	To determine the likelihood of realisation and the impact of the identified threats and opportunities and include the results in the risk register: - to ensure that risk descriptions are clear and revise them as necessary; - to assess the likelihood of realisation and the impact of risks, as well as the proximity of each identified risk; - to record the assessment results in the risk register.	Information is collected to determine with maximum accuracy the likelihood of realisation, the realisation potential, and the impact of threats now and in the future: - anticipated regulatory and legislative changes; - risk indicators and risk management reports; - internal and external audit reports; - incident register; - EWRA; - operational/business strategy assumptions and objectives; - planning of financial forecasts; - performance indicators and their dynamics; - market/partner information. The risk register is used to record the identified likelihood of realisation and the realisation potential of threats, categorise risks, assign unique numbers for ease of use, and identify the owner of each risk.	Information summarising risks and their impacts is compiled to be used in planning and subsequent risk management phases: the risk register is updated to include the likelihood of realisation, the realisation potential, and the potential impact of each threat; - the quality of the records must be such that the risks with the highest and lowest impact can be clearly identified, which in turn will enable the critical risks to be identified and effectively addressed; - the monitoring indicators (KRIs or EWIs) and the frequency of monitoring are revised/determined.	The institution may choose to use one or more of the following risk assessment tools or to use other tools and methodologies that the institution considers more appropriate for its risk assessment: - probability assessment: the likelihood of realisation and the realisation potential of a particular threat is assessed with regard to the period in question. Use is made of historical data, expert assessments, statistical methods, and subjective probability analysis; - impact assessment: it is determined how the institution will be affected by the realisation or the realisation potential of a threat. The impact is assessed both quantitatively and qualitatively. Use is made of historical data, expert assessments, the analysis of different scenarios, the modelling of probabilities, and possibilities employing simulation methods; - value estimation: provides an estimate of potential losses. The expected value is calculated according to the following formula: $expected\ damage = probability \times scope\ of\ loss$. Use is made of historical data, expert assessments, scenario analysis, and statistical modelling.

5. Risk monitoring and reporting: the rhythm of the institution

The risk monitoring and reporting cycle includes such components as performance and risk indicators; the regular collection of data on risk factors and developments; ongoing risk assessment and analysis; the analysis of reports from internal or external audits and/or visits or inspections by supervisory authorities; the timely communication of risks; the prompt identification and communication of changes; technological tools and the direct monitoring of risk platforms/systems (not applicable in the *baby born* and *grow* phases of the institution); having a regular review process in place; the monitoring of critical incidents and issues, the recurrence or spread of which could have a significant impact on the continuity of the institution's operations; and coordination and cooperation within the risk management team of the institution.

Risk monitoring could be carried out as part of the internal audit of the institution, as part of the assessment of the effectiveness of the institution's risk management system as a whole or of its individual elements, as part of the stages of the risk management process, or in any other manner determined by the institution. Risk monitoring involves reassessing risks and adding new risks, assessing the effectiveness of controls, analysing

indicators and early warning signals, and approving material changes. The results of such assessment are documented and communicated to the institution's collegial management body responsible for adopting measures for eliminating any shortcomings found, for managing/mitigating risks, and/or for controlling their implementation.

The risk management measures established by the institution must be regularly reviewed and revised, and the institution, having selected risk management measures to address the identified risks, must ensure their timely and proper implementation through the continuous monitoring of the process, and must respond to identified irregularities by taking timely and effective corrective actions. Effective communication plays an important role here.

Subparagraph 29.4 of the Description stipulates that, in the performance of their duties, the staff of the institution must immediately inform the relevant persons of the risks to which the institution is exposed, other deficiencies in the internal control system, breaches of legal acts, and the institution's internal documents in accordance with the procedure laid down in the institution's internal documents. The implementation of this requirement is an integral part of the institution's business cycle, contributing to the development of the institution's risk culture at the institution-wide level and to the maturity of the institution.

The risk culture of the institution should foster the creation and nurturing of an environment of open communication and critical thinking within the institution, and the decision-making process within the institution should rely on a wide diversity of views. It should enable staff to test existing practices, encourage a constructive critical approach, and create an environment of open and constructive participation. The institution should use effective and secure communication channels, establish and implement clear and effective organisational stages in the risk management process, and promote the engagement, knowledge, and competence of staff in the areas of risk management.

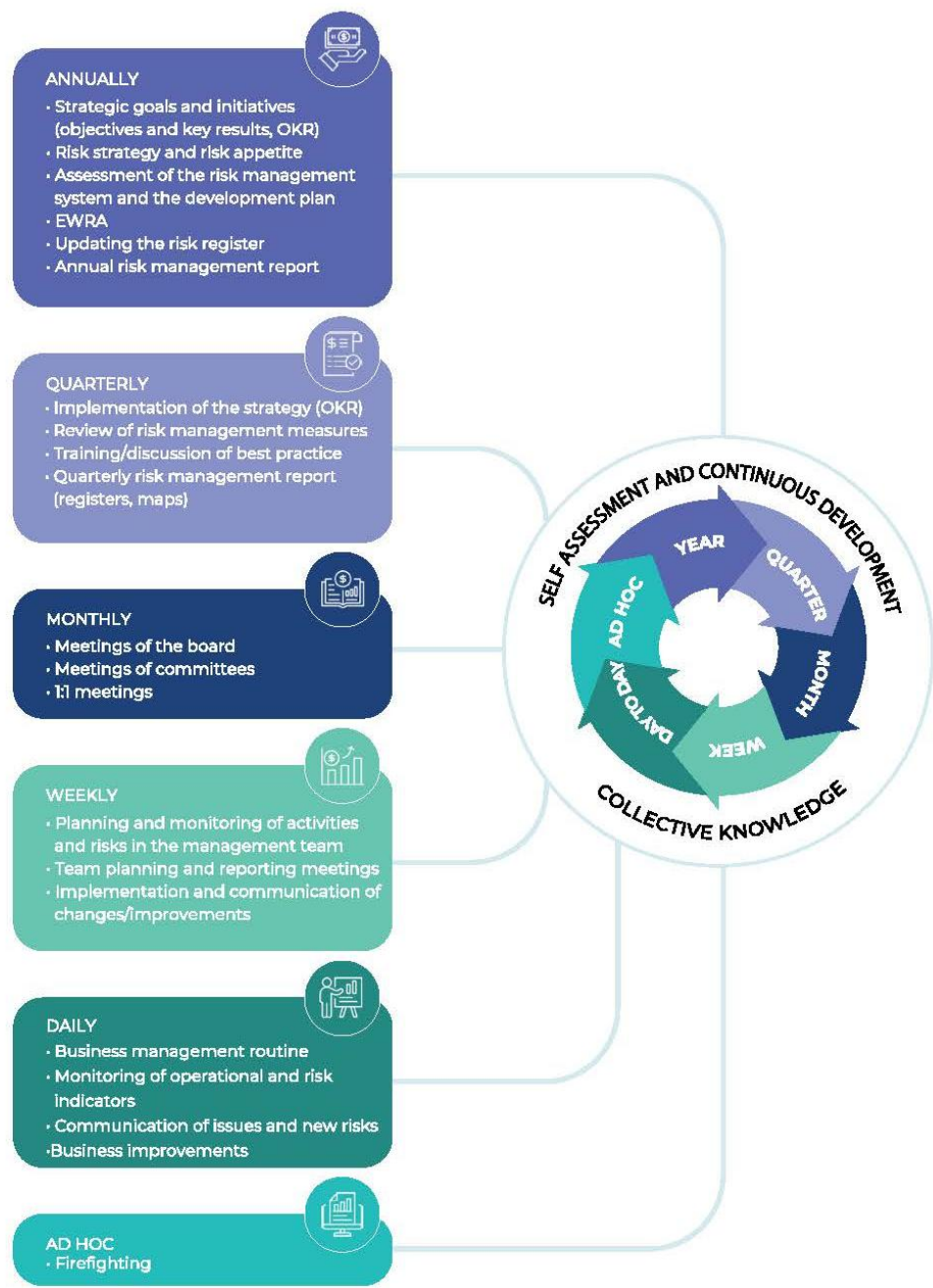
The monitoring and analysis of KPIs, KRIs, and EWIs, the communication of early warning signals, operational and risk planning, and mutual accountability within teams are effective measures of control to ensure engagement with and the maintenance of a risk culture. The integration of risk controls into processes, their automation, and the increasing complexity of the institution lead to the greater importance of monitoring and mutual accountability.

The institution is recommended to determine, in its internal procedures, the periodicity of the assessment of the risk management system, the persons responsible for conducting the assessment, the assessment methodology, the procedure for communicating the results of the assessment, the details of a plan for addressing irregularities, the monitoring of its implementation, clear accountability and responsibility for the implementation of the actions set out in the plan, and the allocation of the resources necessary for this purpose.

Best practice would be to standardise the institution's business cycle. This would give a clear and detailed view of this process, specifying the activities and risk practices that should occur on an annual, quarterly, monthly or weekly basis, etc. The rhythm of the institution could be in document or digital form; it is important to ensure engagement and communication within the institution's organisational structure both horizontally and vertically. This would ensure speed of decision-making and implementation, while maintaining the chosen risk appetite.

A recommended example of the rhythm of the institution is shown in Figure 3. This rhythm of the institution has been developed from a synthesis of best practices applied by some institutions. If an institution decides to standardise its business cycle, then it should develop a tailor-made approach that takes into account its size, scale, and specific characteristics in order to be effective in handling existing risk management practices and enhancing the risk culture, maturity, and sustainability.

Figure 3. The rhythm of the institution (summarised best practice for institutions)



6. Documentation

This chapter covers the risk management documents that institutions are required to prepare, approve, and use in the process of the organisation of risk management, from the selection of the risk strategy (see Chapter 3) and the implementation of the risk management system (see Chapter 4) to the continuous improvement of the risk management system (see Chapter 7).

Paragraph 37 of the Description provides that the supervisory body of the institution must approve **an internal document setting out the Institution's risk strategy and the principles of risk management organisation**. It must describe the main steps in the implementation of the institution's risk management process and shall set out at least the objectives of risk management; the main stages of the risk management process; the participants in the risk management process and their main roles, responsibilities, and accountabilities; the requirements for providing information to the supervisory body on risk management issues; and a list of risks, types of risk appetite, and the limits of tolerance.

The purpose of the internal document setting out the Institution's risk strategy and the principles of risk management organisation is to: (a) define risk appetite, risk tolerance limits (risk limits), and monitoring principles; (b) set out the institution's risk management objectives and the strategic initiatives for the development of the risk management system and competences; (c) describe how risk management is integrated with the institution's overall business strategy and day-to-day management; and (d) provide an understanding within the institution that risk management is not just formal compliance with a legal requirement, but is an effective **tool** for achieving the institution's objectives at the strategic, project, and operational levels.

The internal document setting out the Institution's risk strategy and the principles of risk management organisation covers the essential aspects of the institution's approach to risk management. It must clearly describe the key steps in the implementation of the institution's risk management process, i.e. identify the risk management objectives and key stages in the risk management process; provide a list of risks, risk appetite for each type of risk, and the risk tolerance limits (risk limits); provide the clear organisation of the risk management process in an organisational structure that clearly defines the rights and duties, functions, responsibilities, and accountabilities of the institution's managers, holders of key functions, and employees in the area of risk management; and set out internal procedures outlining the requirements for the provision of information to the supervisory body on risk management issues and other risk controls to ensure timely, accurate and consistent risk identification, assessment, monitoring, management, mitigation, and control.

Best practice is to regularly update references to relevant procedures and documents in the internal document, setting out the risk strategy and the principles of the organisation of risk management within the institution while developing the risk management system process. In a small institution, this document may be integrated with other documents. For example, the internal document setting out the Institution's risk strategy and the principles of risk management organisation may form an integral part of the business strategy. Each institution may choose the form and type of documentation to describe/document the risk management system. It is important that the documentation is based on the principles of clarity, traceability, and interconnection.

The internal document setting out the Institution's risk strategy and the principles of risk management organisation is to be reviewed in the event of changes in the business strategy, business direction, the lifecycle of the institution, risk appetite, the organisational structure, and any other material changes. However, this must occur no less frequently than once per year.

Best practice involves synchronising reviews of risk strategy and operational strategy. The development of the risk management system and the improvement of competences should be designed to prepare the institution for its timely transition to the next lifecycle, and/or to operate in a riskier environment, and/or to take on more risk and/or to make other fundamental changes.

In accordance with subparagraph 28.1 of the Description, **the institution's collegial management body** must approve the institution's detailed **organisational chart**. This must show each body, structural, and functional unit of the institution; the position in the organisational structure of the persons responsible for the control functions referred to in paragraph 20 of the Description; a general indication of each of the functions carried out by the agent(s) and/or the person(s) to whom the operational functions have been delegated; an indication of the persons responsible for the monitoring and supervision of the activities of such units and of the agent(s); and the person(s) to whom operational functions have been delegated. In the event that the institution is a subsidiary within the meaning of the Republic of Lithuania Law on Financial Reporting by Undertakings and Groups of Companies, the organisational chart of the institution shall show the parent company and its bodies, units and the specific persons who have the right to take decisions on the governance of the Institution.

Paragraph 40 of the Description provides that the institution must maintain **a risk register** recording each inherent risk. This must include at least a description of the risks, indicating the exposure limits and which limits are to be strictly observed (hard limits) and which are to be used only as a means of early warning (soft limits); the type of risk to which the specific risk has been attributed; the units responsible for identifying and communicating the risks; and changes in the impact of the risks and the reasons for such changes.

The risk register, which is the main tool for risk management and communication, is to be used and continuously modified at each stage of the organisation of the risk management process. The risk register should systematically record, monitor, and evaluate the risks identified by the institution and provide strategies for managing each risk.

It is recommended to include in the risk register: the date of identification of the risk; the likelihood of realisation of the risk; the impact of the risk; the expected value of the individual risk (threats are indicated in the positive and opportunities in the negative); the preferred response to the risk (acceptance, mitigation, etc.); the existing controls; the expected risk mitigation steps and their timeframes; residual risks and their impact; potential derivative risks (arising as a result of the risk response); indicators; frequency of monitoring and reporting; and the risk owner (the person responsible for all aspects of managing and controlling the risks assigned to them, including the implementation and monitoring of the chosen risk response).

It is considered to be best practice for the risk owner to coordinate the work and involve other members of the team (which may include owners of related processes, colleagues contributing to the implementation of response actions, etc.) in the implementation of a response action for a specific risk or group of risks. When developing a risk culture within the institution, it would be best practice to increase the number of risk owners and those involved in risk management.

The risk register should be actively used in institutions for decision-making at different levels, as well as for risk monitoring and mandatory **quarterly reporting**. Its purpose is not only to assess the actual level of risk and its consistency with the established risk tolerance limits (risk limits) based on historical data, but also to plan future risk tolerance limits (risk limits). A risk map may be integrated into the risk register.

It is best practice to demonstrate, in the risk register, the dynamics of the level of individual risks and the correlation between the risk appetite and the established risk tolerance limits (risk limits).

Paragraph 43 of the Description states that a quarterly risk management report for the institution must, at least on a quarterly basis, be submitted by the risk management officer and considered by the institution's collegial management body, and shall include **a risk map** that assesses the exposure to risks specific to the Institution (e.g. very high, high, medium, low, random, etc.) and the probability of their occurrence.

A risk map is a graphical representation of all existing or potential risks, taking into account the likelihood of occurrence of a particular risk and the potential impact of its occurrence. It shows the possible links between risks, where the occurrence of one risk has an impact on another risk. The risk map is commonly used as a visual decision-support tool and is intended to provide the collegial management body of the institution with a

clear visual breakdown of existing risks in terms of their impact and likelihood (e.g. rare, unlikely, possible, likely, and frequent), to facilitate the identification of risks or the position of a risk in the overall system of inherent risks, and to simplify decision-making with regard to risk management measures.

For the design and content of the risk map template, an institution may use templates already available on the market, but may also create and design its own templates adapted to its risk management process. The risk map can be in the form of a document or in a digital form (e.g. dashboards), and can be integrated into the risk management tools used by institutions through a number of information technologies. For effective risk monitoring and sound decision-making in terms of risk management, it is important to accurately capture risk dynamics in risk maps, reflect changes in the internal and external environment (e.g. by linking risk map data to other documents and reports produced by the institution), and monitor the impact of changes on indicators, using up-to-date data from the risk register, incident register, risk management improvement plan, or other data.

Best practice is to use colour coding according to risk levels, and it is recommended to involve risk and operational managers, depending on by the phase in the institution's lifecycle, in the development of the risk map and the review and analysis of the risk register to ensure effective, informed, and risk-based decision-making.

The risk map and risk register are interconnected elements of risk monitoring, which makes it possible to integrate them into a single document.

Paragraph 41 of the Description provides that the institution must maintain **an incident register**, in which each incident must be recorded, including at least: a description of the incident; the dates of the incident and its entry in the register; the person(s) responsible for the resolution of the incident; the causes of the incident; the timeframe for the resolution of the incident; steps taken to resolve the incident; actions taken and their dates; and the person(s) responsible for the follow-up of the resolution.

The incident register is used to record all risk events and unplanned situations encountered by the institution which have affected its operations, security, and compliance. This document links the institution's risk management and incident management processes (problems, benefits, enquiries, complaints, etc.), as incidents might signal new risks.

Best practice is to have in place and regularly update such a document, even if no events have been recorded, i.e. the institution should indicate in the incident register the period of time and confirm that there were no events to be included in the register during this period.

Paragraph 42 of the Description provides that the collegial management body of the institution must identify procedures for keeping by the institution of the registers (risk and incident registers) referred to in paragraphs 40 and 41 of the Description to ensure that the data in the registers are up-to-date and are analysed and evaluated for risk management purposes.

Paragraph 44 of the Description provides that the risk management officer must submit **an annual risk management report** to the collegial management body of the Institution for evaluation on an annual basis.

The annual risk management report shall include an overall risk assessment, including information on the risks to which the institution is exposed; the risk management improvement measures and other risk management measures implemented and their impact on risk management; the proposed measures to improve risk management; and the expected change in risk as a result of their implementation.

The annual risk management report is an important document for the provision of risk management-related information to the institution's collegial management body and is intended to provide the institution's

management with a summary of the relevant risks and risk management actions taken by the institution during the preceding reporting period (previous year).

In practice, institutions often combine the annual risk management report and the periodic risk management assessment into a single document, i.e. the annual report. This practice is acceptable, but it is important that this report includes an assessment of the risk management system (see Chapter 7), depending on the phase of the institution's lifecycle, the maturity sought in terms of its risk management, the extent to which risks are addressed in practice, and the effectiveness of management.

Paragraph 45 of the Description provides that the collegial management body of the institution, taking into account the results of the assessment of the risk management system, shall periodically, but not less than once a year, assess whether there is a need to improve the risk management system. Having determined the need for such improvement, it shall approve **the plan for the improvement of the risk management**, which shall include measures to improve risk management; the persons responsible for the implementation of these measures and the timeframe for the implementation of the measures; the persons responsible for the control of the execution of this plan; and the persons responsible for the assessment of the change in risk after the implementation of the measures.

Following the assessment of the risk management system, the institution is advised to prepare a risk management improvement plan, which is a document summarising all the actions needed to improve risk management within the institution and to improve the institutional and/or risk culture at the level of the institution or its relevant business unit. The purpose of this document is to integrate risk management into the rhythm of the institution and to document planned improvements. It documents the current health/maturity of the institution's risk management system (the institution's ability to properly assess and effectively manage, including prevent, operational risks) and its consistency with the lifecycle, the approach to be taken and the risk assessment in the institution, the objectives set for improvement, the timeframes for their implementation, and the means to attain them.

The development and updating of this document is to be coordinated by the institution's risk management officer or a person performing that function, with the involvement of managers and the collegial management body, gradually increasing the number of participants to include staff members, i.e. combining top-down and bottom-up approaches and processes.

It is best practice to develop a risk management improvement plan regularly, but no less than once a year, along with a review of the risk strategy, and to use visual task management with dedicated tools, as well as to have weekly team reporting (for measures with longer deadlines due to objective reasons, such as procurement, system development, etc., periodic reporting may be used to discuss the intermediate stages of the implementation of measures), which may be integrated in operational and risk planning and monitoring meetings.

The results of the implementation of this document and the information recorded during its implementation, including glitches identified in the risk management process, are to be used to review and update the internal document setting out the Institution's risk strategy and the principles of risk management organisation, as well as the individual risk management procedures and processes. The envisaged changes should be coordinated at the institution-wide level, with clear reporting requirements and deadlines. Information on progress in implementing the risk management improvement plan can be provided in risk management reports, which include risk maps, the risk register, the incident register, and an annual assessment of the risk management system.

7. Reviewing and improving the risk management system

Strategic planning (the review and approval of annual objectives) should also include a review of the internal document setting out the Institution's risk strategy and the principles of risk management organisation, taking into account the chosen direction and pace of growth, defining the maturity of the risk management to be pursued, and setting out the objectives and the pace at which the risk management system will evolve. The risk strategy must ensure that it is adequately supported in all phases of the institution's growth.

It is recommended that the institution also assess the adequacy and effectiveness of the risk management system in the following cases:

- the emergence of new risks that have a significant impact on the operations of the institution;
- material changes in the risks identified by the institution, their exposure, expected risk appetite, and/or risk tolerance limits (risk limits);
- where the institution starts providing new services or products, introduces new service channels, expands into new jurisdictions, or otherwise changes the business model presented at the time of licensing and approved by Lietuvos bankas;
- material changes in the legislation governing the institution's business and/or the emergence of new regulations that may have a significant impact on the institution and/or its operations;
- significant anticipated changes in the institution's operations, management, or organisational structure;
- where Lietuvos bankas or any other supervisory or competent authority identifies deficiencies in the institution's internal control system and/or risk management system.

A regular review/assessment of the risk management system (the effectiveness of the institution's risk management system as a whole or of its individual elements, or of the stages of the risk management process) could be carried out by means of an internal audit, by engaging an independent consultant, by forming a group of staff members with control functions in the institution, or by any other means of control chosen by the institution (e.g. analytical, information technology, technological solutions and tools).

The results of such an assessment are to be documented and communicated to the institution's collegial management body in order to effectively address the irregularities identified during the assessment.

Paragraph 45 of the Description provides that the collegial management body of the institution, taking into account the results of the assessment of the risk management system, must periodically, but not less than once a year, assess whether there is a need to improve the risk management system. Having determined the need for such improvement, they must approve the plan for the improvement of the risk management (see Chapter 6).

Best practice would be to involve all stakeholders in the evaluation of the risk management system, including employees, managers, management bodies, and risk professionals, in order to maintain a common understanding of risk and the effectiveness of controls.

Annex. The fintech lifecycle risk maturity model

INSTITUTIONAL LIFECYCLE (PHASE)
Key characteristics of risk management in institutions

RISK CULTURE AND GOVERNANCE

GOVERNANCE
The role of the risk management officer ↓

RESPONSIBILITIES
Alignment of responsibilities ↓

CREATING THE RISK CULTURE ↓

BABY BORN
The entire start-up team is involved in risk management. There is a common knowledge of risk management and responsibilities are shared as everyone is responsible for risk management. Key risk management processes are defined. Action plans are implemented on an ad hoc basis in response to major and priority risk events.

Risk management is the responsibility of the entire small team and/or the founders of the institution. Monthly or quarterly reviews involve the whole team, often assessing ongoing activities and operational/ business plans.

Initially, risk and compliance responsibilities may be combined or the risk management function may be temporarily performed by the chief executive officer or the executive director. Eventually, at least two risk management professionals are appointed to ensure the substitutability of responsibilities and the continuity of risk management and system development, as well as to increase risk awareness for risk-based decision-making within the growing team.

The key challenge is to start building an effective risk management system and to develop risk awareness and competence to ensure the continued growth of the institution. Shareholders and both supervisory and collegial management bodies shape attitudes towards risk through their behaviour.

GROW
The risk management system and processes are documented. Risk management is seen as a business enabler. Most processes are consistent, and simple and/or technical controls are used. Regular risk monitoring and reporting is in place.

Risk management is a shared responsibility of all, which is clearly identified, has defined roles, and follows the principle of independence. The risk management officer is actively involved in strategic planning, and attends monthly/quarterly meetings of the collegial management body and weekly management meetings. The role of the risk management officer is crucial and is more closely related to day-to-day activities in the development of the risk management system than to consultancy.

Responsibilities become more complex as the institution grows. In the transition phase, an effective solution is to combine the duties or function of officers with the outsourcing of part of the operational risk management function. If responsibilities are combined (e.g. risk management + cybersecurity officer, risk management + compliance officer, or risk management officer + outsourcing), this is clearly defined, ensuring competence and substitutability. As the risk assumed and/or the pace of growth increases, greater risk competence and more resources are required.

Training is provided to all employees on general risk perception, and specialised training is provided on high-risk areas. Teams are encouraged to share lessons learned from risk events and near misses. This helps to increase the team's understanding of risk. Cross-functional teams and/or advisory committees are best practice for risk-based decision-making.

SCALE
Risk management is proactive, integrated throughout the institution, and linked to business strategy and operations, with more sophisticated tools in place and in use than in previous lifecycles. Continuous feedback helps to shape the risk strategy and develop capacities. The risk management process involves everyone, with top-down and bottom-up communication.

Managers understand all business aspects and can effectively manage risks, especially as the institution grows and its activities become more complex. A well-structured risk management system is established within the institution. The risk management officer becomes the centre of excellence and coordination for developing risk competence within the institution.

All risk management functions are essential. It is necessary to have several officers already in place tasked with risk management, cybersecurity, compliance, anti-money laundering, business continuity, financial control, and other areas. The functions of each post are clearly defined. These functions can no longer be combined, as was possible in the previous lifecycle phases. In order to increase the competence of the risk management team, the recruitment of an additional risk management professional/expert through outsourcing could be considered.

The main difference from the grow lifecycle phase is a clear decision-making structure and knowledge of which team makes decisions on each risk. It is essential to ensure sufficient staffing for each function and that responsibilities, accountability, and escalation path are clearly defined. The practice of taking risks into account in day-to-day tasks is developed, and open discussions about risks at all levels are encouraged, including daily briefings and feedback on the risk management system.

ROCKET
The institution applies best practices in risk management and influences fintech industry standards. Risk management drives innovation and strategic decisions. A holistic approach and the visual management of operations and risks supports a sound risk culture.

Clear understanding of roles and responsibilities at all levels; visibility of team responsibilities, escalation path, and robust change management processes. This structure ensures that even unconventional ideas are well tested at different levels of governance. Governance structures are designed to facilitate quick and informed decision-making and risk awareness without creating unnecessary bureaucracy. An effective risk management system and risk culture is high on the agenda of the risk management officer.

The mandatory functions of risk management, cybersecurity, anti-money laundering, business continuity management, compliance, finance, etc. can no longer be combined. Risk management competences are maintained at the highest level. External suppliers are only engaged for expert the assessment of specific risk management issues/situations.

All team members are involved in strengthening a proactive risk management culture. Quality and rapid communication between departments, both bottom-up and top-down, is essential. Decentralised responsibility for risk and consistent comprehensive visual reporting allow teams to address risks in accordance with their functions without losing sight of the big picture.



INSTITUTIONAL LIFECYCLE (PHASE)

Key characteristics of risk management in institutions

BABY BORN

The entire start-up team is involved in risk management. There is a common knowledge of risk management and responsibilities are shared as everyone is responsible for risk management. Key risk management processes are defined. Action plans are implemented on an ad hoc basis in response to major and priority risk events.

GROW

The risk management system and processes are documented. Risk management is seen as a business enabler. Most processes are consistent, and simple and/or technical controls are used. Regular risk monitoring and reporting is in place.

SCALE

Risk management is proactive, integrated throughout the institution, and linked to business strategy and operations, with more sophisticated tools in place and in use than in previous lifecycles. Continuous feedback helps to shape the risk strategy and develop capacities. The risk management process involves everyone, with top-down and bottom-up communication.

ROCKET

The institution applies best practices in risk management and influences fintech industry standards. Risk management drives innovation and strategic decisions. A holistic approach and the visual management of operations and risks supports a sound risk culture.

RISK MANAGEMENT SYSTEM

RISK MANAGEMENT SYSTEM. Process and documentation



COMMUNICATION AND TOOLS



Basic procedures ensure internal control and compliance, including anti-money laundering/counter-terrorist financing (AML/CTF) and the key requirements of the Regulation on digital operational resilience for the financial sector (DORA), in customer onboarding and in the management of key risks. There is a clearly defined risk appetite. The initial risk register and a risk map form part of the quarterly risk management reports and can be integrated into AML/CTF and cybersecurity manuals and/or governance reports.

The risk management documentation is produced as a “minimum viable policy” that is simple, implementable, and can be quickly updated to support business development and risk competence. Key features include the following:

- financial management, liquidity, and compliance (AML/CTF, information systems, and information and communication technologies) management procedures;
- links established between risk and the business plan;
- the development of a risk management system depending on the sector and strategy.

As the activity is not yet mature enough, communication is less formal, and mainly takes place through emails. Simple tools, such as xlsx, are sufficient to document basic principles and decision-making processes. Risks are managed through simple internal controls and risk maps, which become more reliable at later stages. Effective communication and ongoing compliance are essential.

The initial risk register and a risk map are integrated and used for risk monitoring and reporting at least on a quarterly basis. A risk management plan is in place, and risk monitoring and the implementation of the plan are subject to regular reporting. As the institution grows, a formalised system of policies, procedures, training, and technical controls (automation, standardised tools and processes, data management solutions, etc.) is put in place. The implementation of these measures is determined by the growth rate of the institution and its strategic business objectives.

Robust data management systems become increasingly important as new employees are recruited.

Existing tools help the institution to grow; use can be made of Trello, MS Planner, or similar tools, or standardised and simple tools for transparent task management.

Risk management tools such as risk maps or risk registers are integrated into the management policy, and the risk appetite is clearly defined. Decisions regarding the use of risk management software or tools developed by the institution are made taking into account the growth strategy.

As the scale of operations increases, governance is strengthened, and the team grows with a clear understanding of the evolving risk environment. Risk is seen not only as an operational activity, but also as part of a long-term strategy.

Procedures for managing the business continuity plan, information and communication technology incidents, projects, changes, and risks, as well as reporting practices, are integrated and developed through a holistic systemic approach. Monitoring, reporting, and communication are part of the business cycle of the institution.

The automation of risk tools and the integration of technical controls into operations accelerates. Change management processes allow rapid adaptation to new risks and ensure the continuous improvement of management. A clear and consistent risk management process and documentation is in place to ensure risk competence and to maintain a risk culture within the institution.

Tools and processes are appropriate for the scale and complexity of operations, with a focus on automation and data integrity to enable effective risk management.

The systems in place provide clear and practicable insights that enable managers and employees to effectively manage information in a complex environment. As the institution grows, the risk management approach becomes more holistic and sophisticated, incorporating advanced financial controls and liquidity management to support growth.

The need for structured management and the clear segregation of duties becomes evident. The risk management system is continuously reviewed, improved, and communicated. Appropriate change management and decentralised solutions allow speed and entrepreneurship to be maintained.

As the institution becomes truly large and has much to lose, the focus is on data management and information flow to facilitate decision making and risk management, as well as strong and robust change management based on appropriate measures and behaviours. Highly automated technical controls, business and risk management dashboards, effective communication, feedback sessions, and ongoing training support the risk culture.

INSTITUTIONAL LIFECYCLE (PHASE)

Key characteristics of risk management in institutions

BABY BORN

The entire start-up team is involved in risk management. There is a common knowledge of risk management and responsibilities are shared as everyone is responsible for risk management. Key risk management processes are defined. Action plans are implemented on an ad hoc basis in response to major and priority risk events.

GROW

The risk management system and processes are documented. Risk management is seen as a business enabler. Most processes are consistent, and simple and/or technical controls are used. Regular risk monitoring and reporting is in place.

SCALE

Risk management is proactive, integrated throughout the institution, and linked to business strategy and operations, with more sophisticated tools in place and in use than in previous lifecycles. Continuous feedback helps to shape the risk strategy and develop capacities. The risk management process involves everyone, with top-down and bottom-up communication.

ROCKET

The institution applies best practices in risk management and influences fintech industry standards. Risk management drives innovation and strategic decisions. A holistic approach and the visual management of operations and risks supports a sound risk culture.

RISK IDENTIFICATION AND ASSESSMENT

RISK ASSESSMENT AND DECISION-MAKING



IDENTIFICATION OF NEW RISKS AND CHANGE IN RISK



The whole team is involved in decision-making and ad hoc risk assessments. The lack of historical data and tools is offset by the close collaboration and expertise of managers and risk professionals. Accurate forecasts of fund flows are used to ensure liquidity and to make decisions on resource allocation at the start of operations.

Risks are managed daily, usually on an ad hoc basis, through close team communication and joint decision-making.

Risk assessment is integrated into strategic initiatives and leads to adjustments to the long-term perspective. Both the strategy and risk appetite are adjusted in light of data and risk assessments, and modified as necessary. Risk assessments help to identify gaps and align efforts with long-term objectives. To address these gaps, risk mitigation measures need to be implemented in small and manageable steps. This approach allows progress to be integrated into day-to-day tasks, ensuring consistent input and continuous improvement.

Regular risk monitoring, the enterprise-wide risk assessment (EWRA), and a detailed assessment of emerging risks and new strategic initiatives ensure that the institution adapts to changes, including political and economic developments, which are particularly relevant to its core business. Vigilance and the planning and monitoring of business and risks are combined with a new method of communication to detect and report new risks in a timely manner. The analysis of business and risk indicators, the incident register, and risk monitoring are important sources of risk identification.

Risk assessment shifts from a reactive to a forward-looking approach, taking into account how potential risks may affect not only immediate business plans, but also longer-term strategies. Risk assessments are included in every business case study before any new activity is launched. Data-based decision-making, especially in guiding strategic decisions and resource allocation, is emphasised. Key performance indicators (KPIs) together with risk indicators (KRIs) and early warning indicators (EWIs) are used for risk and business planning and monitoring. Risk assessment is essential in order to align day-to-day tasks with long-term business priorities, addressing both issues without compromising the overall strategic objectives of the institution.

Vigilance, effective communication, and prompt responses to changes become even more important as the institution grows and their potential impact increases. Risks are assessed proactively, rather than being responded to once they occur. Vigilant monitoring and structured risk assessment, synchronised reporting, the use of business and risk indicators, and a risk-based decision-making mindset prevent unexpected challenges even when entering new markets/segments.

Data quality and consistency are essential. Data-based decisions are part of the risk culture. Early signs of potential risks are observed and used to forecast and mitigate risks more effectively and to reduce uncertainties. The risk approach is embedded at the strategic and operational levels and seamlessly implemented in routine work.

Early warning indicators (EWIs) allow the forecasting of risks. Everyone thinks about risk and understands the importance of liquidity and fewer uncertainties. Internal and external sources of information to identify risks are complemented by feedback, experience in change management, and customer and partner insights. Open communication, accountability, scenario analysis, the communication of forecasts, and the sharing of experiences support the approach to risk within the institution.



APPROVED

by Decision No V 2025/(1.160.E-9004)-441-45 of the Financial Market Supervision Committee of 1 April 2025.

EFFECTIVE as of 1 January 2026.

© Lietuvos bankas, 2025

Gedimino pr. 6, LT-01103 Vilnius

www.lb.lt