DLA
The Power of Fintech Lending

Industry Standard on Enterprise Risk Management

A. Preamble

The subject of this standard is the firm establishment of a comprehensive risk management system at company level that takes particularly into account the mutual interdependence of risks to ensure that the company's business objectives can be achieved.

B. Definitions

I. Risk: The impact of uncertainty on goals, activities, and requirements.

II. Enterprise Risk Management (ERM): The systematic identification, evaluation and monitoring of risks connected to the business at the same time aiming to manage the adverse influence of risk on capital and profit.

III. Risk Culture: Set of internal processes and policies, describing values, beliefs, knowledge, attitudes and understanding about risk shared by the organization.

IV. Customers: Investors and debtors as well as potential investors and debtors.

V. Employee: A person who is permanently, temporarily or voluntarily employed. Interns and apprentices are also employees for this purpose.

VI. Business Partner: Any third party with whom the member maintains a business relationship and who is not a customer or employee in this respect.

C. Industry Standard on Enterprise Risk Management

The members are responsible for leading an effective organization that ensures compliance with supervisory, legal, as well as other business requirements. For this to be achieved, when making business decisions, members should consider potential threats, risks, and damages to their businesses.

European legislation as well as auditing standards require companies to implement the systems for the timely risk recognition, monitoring and reporting. Appropriate and effective risk management includes the definition of strategies and the establishment of internal control procedures. Furthermore, the development of processes and systems for ERM is not only in the interest of the organization, but also customers and business partners. By building and promoting a risk culture within the company, members can either entirely avoid or at least minimize the potential damages to the business. Hence, good decision making at all levels of the company should include comprehensive understanding of the risk associated with the decision.

Risk management is therefore an integrated component of the company’s performance and organizational processes and supports the management in making informed decisions.

Proper risk management empowers the organization in recognizing the chances and threats and managing those, but also increases trust of interested stakeholders and improves the efficiency of the whole organization.

D. Industry Standard on the Proper Conduct of Enterprise Risk Management

The member's management is responsible for the proper conduct of the business development. This responsibility of the management refers to all key elements of risk management, also considering outsourced activities and processes. The managers can only meet this responsibility if they are able to assess the risks and take the necessary measures to limit them. This includes the development, promotion, and integration of an appropriate risk culture within the member.

I. Enterprise Risk Management Process

When developing an ERM process, members should focus on the goal of adequate identification, pragmatic evaluation, efficient mitigation and monitoring of risks that could impact an the organization's ability to achieve its objectives. An effective ERM strategy should be aligned with the organization's overall mission, vision, and values, as well as its risk tolerance and appetite.

In designing its processes, members are confronted with many internal and external requirements. Internal requirements include the protection of sensitive data and assets, the conduct of managers and employees, and the stability of systems and processes. The external requirements mainly relate to market conditions, developments in the Digital Lending industry and its regulatory framework. The following steps should be followed, when developing and implementing a risk management methodology:

- The Risk Manager should be appointed by the management of the member. He or she is responsible for the implementation of the risk management strategy and governance and should regularly report to the management about the enterprise's risks. The risk manager should have a broad range of practical experience and sufficient professional competence to adequately perform the function.

- Next to the central risk management role, members can alternatively establish individual risk owners in different departments, which are then responsible for managing and reporting of the individual risks within the organization. They are accountable for identifying and assessing risk within their area of responsibility.

II. Risk Identification and Assessment

When identifying risks, members should aim to recognize the majority of risks, so that any negative threats and its implications to the business can be as minimized as practically possible. For the avoidance of potential amplifying impacts, risk identification should also include determination of interdependencies between different types of risks. For the completion of this task, members can develop different methods (such as comprehensive risk and threat analysis, scenario, trend and/or empirical analysis, etc), which is at the discretion of the member. The result should be systematic listing of risks which can be determined at different organization levels and departments.

To assess the materiality of risks, the management must obtain an overview of the risks (overall risk profile) on a regular and ad hoc basis. In principle, at least the following risks are to be classified as material:

- default risks (including country risks where applicable),
- market and strategic risks,
- liquidity risks,
- compliance and regulatory, and
- operational risks.

In the next step, impacts of the risks identified on the organization as whole should be evaluated, so that relevance of each risk can be established and used for the purpose of making business decisions.

While risk evaluation could be quantitative (i.e., likelihood/impact matrix) and qualitative (mathematical and statistical techniques i.e., Monte Carlo simulation), the member shall examine which risks could have a material adverse effect on its financial position (including capital resources), results of operations and/or liquidity position. The choice of method for risk assessment will depend on the type and complexity of the risk being assessed, as well as the available data and resources. However, the assumptions underlying the methods and procedures must be justified in a comprehensible manner. The member shall ensure that it has a complete and up-to-date overview of the methods and procedures used to assess risks.

The appropriateness of the methods and procedures shall be reviewed at least annually by the responsible departments. The stability and consistency of the methods and procedures as well as the meaningfulness of the risks determined using them must be critically analyzed in this respect.

III. Risk Management

After the enterprise risks have been assessed, members should develop and implement proper risk management strategies and controls, not only to mitigate or manage the risk identified, but also to recognize potential chances on the market. When preparing appropriate risk response, members have options to fully avoid, reduce, transfer, accept or exploit the risks, depending on their overall impact and likelihood. Implementation of appropriate measures are not only in the responsibility of the management of the organization, but also of the risk manager and/or risk owners. For this purpose, management can decide to set the risk appetite for the organization.

IV. Communication and Monitoring of Risks

The basis of an effective ERM is appropriate risk culture and understanding of the importance of this topic on all operational levels of the company. For establishing such a risk culture, communication plays an important role.

For the purpose of effective communication and risk monitoring, regular enterprise risk meetings should be established between the management, risk manager and/or risk owners. A risk manager should report to the management in text form about key risk measures and controls at least once in a year. The risk report should at least include the following elements:

- Extensive overview of enterprise risks identified with information about their interdependencies;
- Information about the qualitative and/or quantitative impacts of these risks;
- Proposal of the key risk management measures to be implemented;
- Presentation of the results of the monitoring as well as main process deficiencies established;
- Review of methods, premises, and processes.

In case that new, significant risks are discovered, or new circumstances have been recognized that could cause a significant change in a potential of the risk, management should be informed immediately. For this purpose, an ad-hoc report could be submitted.

The last step in the process is continuous monitoring risk and optimization of risk methodologies and processes. For this purpose, there should be ongoing review of the risk development, either by the risk manager or by the individual risk owners. Best practices, benchmarking or maturity models can be used to assess the relevance and improvement potential of risk management. In addition, the risk monitoring and improvement process should not only review the risks that have been identified and assessed, but also those risks that have not (yet) been identified in the identification phase. This step should ensure that the process remains up to date and sustainable.

E. Training of the Risk Managers and Employees

Risk managers and risk owners should be trained in their specific area of business and responsibility, when deemed appropriate.

Employees should be regularly trained by the risk managers and owners, to be able to recognize the main risks in day-to-day business (first line of defense).

F. Controls of Compliance with this Industry Standard

The members shall have plans for regular monitoring of compliance with this industry standard and specify the allocation of responsibilities. The results shall be reported to the management.

G. Comply or Explain

As a general rule, there shall be no deviation from the provisions of this industry standard.

As business models differ quite significantly from each other, depending on the size, type, scope, complexity and risk level of business activities, the standard is open to implementation in different dimensions or even only partially. In case the members deviate from the standard, they shall disclose which parts they implement differently and provide comprehensible reasoning on their website.

H. Review clause

This industry standard shall be subject to revision by the Committee on Risk & Compliance Management of the Digital Lending Association at two-year intervals. Any amendments and/or additions shall be adopted by the General Meeting by qualified majority.