A risk assessment methodology for EMIs

This additional example is part of the CGAP Technical Guide, *Digital Financial Services for Financial Inclusion: Tools for Supervisors.* It provides a practical illustration produced during CGAP's work with several country supervisors on DFS supervisory frameworks. This document is part of the Technical Guide's collection of Additional Examples and Guidance. Its utility and applicability to specific country contexts depends on factors such as the availability of data and other resources, the stage of development of DFS markets, experience with risk-based supervision, and institutional arrangements for supervision.

Introduction

Risk-based supervision of nonbank electronic money issuers (EMIs) must be commensurate with their risk profile, namely the risks inherent to the EMI's activities—and their systemic importance. Risk-based supervision thus relies on systematized identification of risks and their relative importance within and across EMIs. Adopting a risk-based approach (RBA) can help supervisors increase or reduce the intensity of supervision of different EMIs over time, in a flexible yet structured manner. To take full advantage of an RBA, supervisors should have in place a process that maintains an up-to-date understanding of the risk landscape. Supervisors should also systematically and periodically identify and assess the level of risks in individual EMIs, taking into consideration their inherent risks and the controls applied to them.

Developing a risk assessment process

The risk assessment process plays a strong role in shaping supervisory priorities, the level and duration of supervisory scrutiny, how supervision should be conducted, the appropriate balance among supervisory activities (e.g., between offsite supervision and onsite/remote inspections), and the resources allocated to ensure that the required experience and skill sets are assigned to assess risks. Risk assessment is not a static process, but rather continuous and dynamic to reflect the changes in risks arising from both the EMI itself and its external environment (e.g., macroeconomic situation, sectoral conditions).

Past supervisory activities (e.g., thematic reviews, offsite supervision, onsite/remote inspections) are essential inputs to the risk assessment process. Throughout the process, the supervisor should consider findings, assessments, recommendations and action plans, ratings, and remedial actions and sanctions from previous supervisory cycles and reports.

Data analysis and continuous monitoring are also necessary for proper risk assessment (see the Technical Guide, section 4.6: Improving supervisory data). These activities help supervisors to identify—and compare over time—variations in EMI risk profiles. The ability to collect diverse data from different sources has a direct impact on the depth of an assessment under each inherent risk type considered in the risk assessment methodology. It also impacts the supervisor's ability to maintain an up-to-date risk assessment.

If the supervisor recently started to implement an RBA to EMI supervision, they should put together an initial and comprehensive risk assessment (see the Technical Guide, section 4.1: Conducting an initial risk assessment) that also benefits from any previous assessment of individual EMIs, even if the previous cycle was not risk-based. In a small market, the supervisor of EMIs may be able to cover the risk assessment of all EMIs—and even all relevant risks. But in other markets, the process would not be possible due to limited supervisory resources relative to the number of EMIs.

Assessing inherent EMI risks

Supervisors should initially understand the overall risk profile of EMIs as a provider type, which is first determined by regulatory requirements and permitted activities. EMIs are not allowed to intermediate customer funds or engage in risky operations, such as trading and foreign exchange. While banks manage a complex array of intertwined risks and are leveraged (i.e., do not have enough funds to pay back all depositors at once), typically EMIs are mandated to always have enough funds to pay back all customers in full. These fund safeguarding requirements aim to protect EMI customers and permit a lighter supervisory approach (Kerse and Staschen 2018). Additionally, regulations often cap e-money transactions and account balances to limit certain risks (Staschen and Meagher 2018).

However, these requirements do not ensure that EMIs are free of risk. EMIs offer payment services (e.g., withdrawals, transfers, purchases) through a variety of channels using IT systems, telecommunications, business partnerships, outsourcing arrangements, widely dispersed staff and agents, connection to merchants, and payments infrastructure such as switches and other payments systems. These elements create operational, market conduct, and money laundering and financing of terrorism (ML/FT) risks, which supervisors of EMIs often consider the most important risks (Dias and Staschen 2018). EMIs may also face other risks, such as strategic, liquidity, and legal risks.

Supervisors must next understand that not all EMIs pose the same level of risk. Some EMIs and certain activities in the e-money industry may be considered potential sources of systemic risk, with a substantial or high impact on customers, industry, and/or the economy as a whole. There are others that are not of systemic importance but still have medium impact. Also, not all activities are equally risky within EMIs.

To assess inherent risks, supervisors should first identify the **significant activities** of EMIs that pose the greatest risk to supervisory objectives. The degree of importance of impact indicators would be factored in to determine the significant activities and their respective level of significance (see the Technical Guide, Additional Examples and Guidance

2: Examples of impact indicators). Many supervisors also prefer to assign quantitative weights to activities to indicate their **level of significance.** After determining the significant activities, it is essential to assess the level of key inherent risk each poses. Inherent risk is the level of risk present in an EMI's activities, without considering its risk mitigation measures and the quality of risk management and internal control practices. It is the probability of a loss due to the EMI's exposure to current or potential future events or changes in its business or the country's macroeconomic situation, which may also lead to potential damage to its customers. An inherent risk assessment considers the probability of the materialization of an event and the potential size of its adverse impact on the EMI's earnings and overall financial situation. Some supervisors prefer to give numerical ratings to such risks. Others prefer to go with different ratings categorizations (e.g., high, medium high, medium, medium low, low) where each rating has a specific definition that helps the next supervisory team and others in the supervisory authority easily understand it.

Assessing the net risks of EMIs

Finally, the risk assessment process requires that supervisors understand how **inherent risks** turn into **net risks** for each EMI. To achieve this, supervisors must assess the status and effectiveness of each EMI's internal controls, risk management, and governance measures against its inherent risks. Supervisors often assign ratings to the quality of risk management, control, and governance measures (e.g., strong, acceptable, needs improvement, weak). Net risks are those that remain after the EMI has applied all measures to reduce inherent risks. Supervisors should recognize that no matter how robust an EMI's board and senior management oversight, internal controls, and risk management process are, inherent risks cannot be eliminated and will never be zero. In their assessment of net risks, supervisors should also be able to reflect major concerns they have about an EMI's potential risk impact on the financial system.

An EMI with weak risk management and internal controls may not be high risk if the inherent risks arising from its operations and activities are already at a low level. At the same time, an EMI with a high level of inherent risks should not be considered high risk in advance. Since it may have appropriate internal controls that are properly applied, its net risk could be low. However, such EMIs, —for instance, the EMI with the greatest number of customers—will always be high on the supervisor's list.

Supervisors in many jurisdictions use risk matrices to summarize the risk profile of financial services providers (FSPs). A **risk matrix** often presents all risks inherent to a type of business, according to activity. It assigns weights to activities according to their relative importance to the business type. Based on actual provider risk assessments, supervisors indicate how well or how poorly a provider mitigates inherent risks through governance, risk management, and internal controls. The methodology produces and assigns each provider with a risk rating that is comparable across providers. Thus, the risk matrix allows for better supervisory planning and use of resources (Wright 2018).

However, no single risk-based methodology and risk matrix model works for all supervisors of EMIs. Supervisors often define risks differently and choose different inherent risk types and respective relative weights for their risk matrices. They also create different risk ratings and trend assessment methods. A risk matrix generally designed for banks or other FSPs (e.g., insurance providers) will not fit the risk profile of EMIs. Risk matrices for EMIs are significantly more simplistic than matrices used for banks, as banks usually have a more complex combination of activities that makes their inherent risk profiles more complex.

FIGURE 1. **Example risk matrix for EMIs**

Significant activity	Inherent risks								Governance, control, and management				
	Operational Risk (1)	ML/TF Risk (1)	Market Conduct Risk (1)	Risk 4 (1)	Risk 5 (1)	Risk 6 (1)	Total Inherent Risks (1)	Direction of Total Inherent Risks (3)	Internal Controls (2)	Risk Management (2)	Corporate Governance (2)	Net Risk (1)	Direction of Net Risk (3)
Fund safeguarding													
Cross-border transactions													
Bulk transactions, including payments of salaries, benefits, and pensions													
Cash-in and cash-out transactions													
Insurance products in partnership with an insurance company													
Outsourcing arrangements													
Activity 7													
Activity 8													

Key

(1) Categories for risk level	High	Medium high	Medium	Medium low	Low
(2) Categories for governance, control, and management	Strong	Acceptable	Needs improvement	Weak	
(3) Categories for direction of risk	Increasing	Constant	Decreasing		

References

Dias, Denise, and Stefan Staschen. 2018. "A Guide to Supervising E-Money Issuers." Technical Note. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/guide-supervising-e-money-issuers

Kerse, Mehmet, and Stefan Staschen. 2018. "Safeguarding Rules for Customer Funds Held by EMIs." Technical Note. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/safeguarding-rules-customer-funds-held-emis

Staschen, Stefan, and Patrick Meagher. 2018. "Basic Regulatory Enablers for Digital Financial Services." Focus Note. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/basic-regulatory-enablers-digital-financial-services

Wright, Paul. 2018. "Risk-based Supervision." TC Notes. Toronto Centre. https://www.torontocentre.org/videos/Risk-Based_Supervision.pdf