CGAP

A Guide to Supervising E-Money Issuers

Denise Dias and Stefan Staschen

A Technical Guide

A Guide to Supervising E-Money Issuers

A Technical Guide

December 2018

Denise Dias and Stefan Staschen

CGAP

Consultative Group to Assist the Poor
1818 H Street NW, MSN IS7-700
Washington DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594

Table of Contents

1. Introduction

A specialized regulatory window for nonbank e-money issuers (EMIs) is one of four basic regulatory enablers for inclusive digital financial services in emerging markets and developing economies (EMDEs) (Staschen and Meagher 2018). For the purposes of this guide, EMI is defined as any regulated entity—bank and nonbank—that is dedicated to issuing e-money or similar stored-value accounts, even if it trades under a different name such as a limited-purpose bank or payments bank.[1]

A special regulatory window for EMIs can be effective only if it is combined with necessary supervisory changes. The role of supervision is threefold: (i) to ensure risks are identified, adequately managed, and mitigated by EMIs; (ii) to enforce compliance with regulatory requirements; and (iii) to create procedures to manage an EMI crisis. Effective supervision helps supervisors identify and manage risks before they reach scale and provides evidence-based input for regulatory changes. The question is: How do we effectively supervise EMIs?

Proportionality in supervision can optimize the efficient use of limited resources and avoid stifling EMI innovation and growth. There is no unique recipe for a proportional approach to EMIs, and what is proportional in one country can be disproportional in another. Defining an approach requires understanding an EMI's inherent risk profile, in line with what EMIs are permitted to do by regulation. Like banks, EMIs collect funds from customers and promise to pay them back, but EMIs do not extend credit facilities or engage in risky operations. In fact, EMIs are usually required to back all e-money issued (the money owed to customers) with liquid funds. Because of this fundamental difference, EMIs have a lower risk profile and, therefore, require less supervisory attention than banks.

A proportional approach also considers whether an EMI has systemic importance because of its size, cross-jurisdiction activity, or other aspect.[2] The level of supervisory

[1] Thus, an EMI can be a nonbank (an entity that does not intermediate deposits collected from the public) or a bank that is specialized in e-money issuing and not permitted to lend, such as payments banks in India, niche banks in Mexico, and payment service banks in Nigeria. It does not include models where customer deposits are held in traditional deposit accounts, even if they are accessed through agents or digital channels such as mobile phones (e.g., branchless banking providers in Pakistan). Unless indicated otherwise, the word "bank" in this publication refers to traditional banks that are allowed to intermediate and leverage customer deposits.

[2] According to BCBS (2016a, p. 2): "[I]n some countries, non-bank financial institutions, while not systemic based on the value of funds they intermediate, may present a systemic dimension due to the number and type of customers they serve."

attention will vary across EMIs as a result. For instance, a light approach that focuses on offsite monitoring and enforcement of fund safeguarding rules might suffice for certain, in particular smaller EMIs in a given country. For other (larger, systemic, or problematic) EMIs in the same country, a proportional approach could mean conducting inspections that cover all topics addressed in this paper and more. Additionally, each country's approach depends on a range of context-specific factors such as concurrent supervisory priorities, available expertise and supervisory technology (SupTech),[3] and the stage of implementation of risk-based supervision.

This paper aims to (i) provide general guidance to EMDE supervisors who are designing proportional approaches to EMI supervision and (ii) serve as a reference for drafting or improving EMI supervision manuals in a few specific areas. After a general introduction to the concept of proportionality and how it applies to EMI supervision, the paper describes supervisory procedures to be adopted during licensing, offsite monitoring (surveillance), and examinations of EMIs. It relies on the authors' own experiences, interviews with a sample of supervisors,[4] and existing literature, including international standards and publicly available supervisory guidance.

This paper focuses on protection of customer funds and addresses operational risk, money laundering and financing of terrorism (ML/FT) risk, and EMI business plans and offsite monitoring. There are certainly other areas that are relevant for EMI supervision that go beyond the scope of this paper. For instance, this paper does not address corrective and enforcement measures, EMI resolution, fit-and-proper analyses, cross-border aspects of EMI supervision, and the role of interoperability, cloud computing, and APIs in EMI supervision. It also does not cover every important risk area, partly because some of these areas are addressed in other papers. (See Table 1 for definitions of the most relevant risks in EMIs, some of which are discussed in this paper).[5]

While some supervisors may find the combination of all the procedures described in this paper to be excessive or complex, others may find it insufficient and lacking depth. Our intent is to illustrate how analyses in the areas covered could be done; it is not to propose an ultimate list of topics and procedures. In line with their general supervisory approach, supervisors can incorporate some or all procedures in their supervision

[3] SupTech is the use of innovative technology by supervisory agencies to support supervision. See Broeders and Prenio (2018) and Dias (2018).
[4] In-person, phone, or written interviews were done in 2017 with financial supervisory authorities responsible for e-money issuers in Austria, Colombia, France, Ghana, Hong Kong, India, Luxembourg, Malaysia, Mexico, Myanmar, Nigeria, Peru, the Philippines, Singapore, Tanzania, Uganda, and the United Kingdom.
[5] Consumer protection, data collection for supervision of EMIs, and the implications of EMIs operating through agents are covered in Dias (2013); Dias and Staschen (2017); and Dias, Noor, and Staschen (2015), respectively.

manuals and deploy them in comprehensive or focused examinations, offsite monitoring, or thematic reviews.

Finally, the procedures are described in a manual, labor-intensive "version," which is all that is possible in several EMDEs where SupTech is incipient. The paper highlights examples where SupTech could lessen the burden on the supervisor. The degree to which technology is leveraged will affect the effectiveness and proportionality of EMI supervision.

The primary audience of this paper is EMDE supervisors who oversee EMIs. Regulators, policy makers, and international organizations that promote effective EMI supervision to foster healthy financial inclusion in EMDEs may also find this of interest.

2. *A proportional approach to EMI supervision*

2.1 Proportionality in EMI supervision

In a proportional supervisory approach, the supervisor's expectations should be commensurate with the EMIs' risk profile (the risks inherent to EMI activities) and their systemic importance. These expectations determine the supervisory intensity to be applied and the consequent use of supervisory resources. Generally, EMIs require a lower level of scrutiny as compared to traditional banks. Across EMIs, different levels of intensity are warranted: large, systemic, or problematic EMIs may require supervision on all topics included in this paper and more, while a lighter approach (e.g., limited to offsite monitoring and/or assessing fund safeguarding) may be appropriate for small EMIs that do not present particular problems.

There is no single recipe for a proportional supervisory approach to EMIs. What one supervisor considers to be proportional may be considered disproportional by another. Supervisors have differing views on the use of supervisory tools (market monitoring, offsite and onsite examinations, and thematic reviews), the scope of supervision (the topics covered), and the depth of supervision (the level of detail in the examinations, the techniques used—analytical and audit procedures—and their frequency).

2.2 Banks and EMIs: Different scope of activities and different risk profiles

In earlier times, banks collected cash and other assets (e.g., gold) from customers for safekeeping (*fiduciary function*). After realizing that not all customers (depositors) requested all their assets at the same time, banks started to lend part of these assets to other customers (*intermediation function*). This was the birth of modern banking, with its key inherent risks (credit, maturity mismatch, liquidity, and capital). By assuming such risks, banks have a critical role in allocating funds in the economy. Financial intermediation and leverage create basic risks, but banks also engage in many other risky operations, including among themselves and across national boundaries. They also provide payment services. Because of their complexity and risks (which small depositors are unable to assess at a reasonable cost) and their importance to the economy, banks have been heavily regulated for generations.

EMIs are much less complex; they do not intermediate and leverage customer funds. However, they have the fiduciary function in common with banks: they collect customer

Box 1. Approaches to EMI supervision

All the supervisors interviewed for this research conduct some supervisory activities on EMIs, even in jurisdictions where the legislation allows exemption of small EMIs from licensing and supervision (e.g., France, Luxembourg, and the United Kingdom). All of them, at a minimum, collect periodic statistics for market monitoring purposes, and some (e.g., Luxembourg) include safe and soundness—checking whether an EMI is in good financial health—as well as institution-focused examinations. Most supervisors interviewed have established supervisory procedures that cover a few risks at the institution and market levels, which vary widely in their scope and depth from covering only a few system-level issues, such as efficiency and competition through bi-annual statistics (e.g., Central Bank of Brazil), to collecting a wealth of frequent data and conducting periodic onsite inspections on key risks, including consumer protection and fund safeguarding (e.g., most of the supervisors in Sub-Saharan Africa), to using a risk-based methodology addressing all types of risks (e.g., Luxembourg's Commission de Surveillance du Secteur Financier).

funds and promise to pay back at a future, undetermined date.[6] Like banks, EMIs need to manage risks to keep that promise. The fundamental difference is that while banks manage a complex array of intertwined risks and are leveraged (they do not have enough funds to pay back all depositors at once), EMIs, by regulation, are mandated to always have enough funds to pay back all customers in full. Fund safeguarding requirements aim to protect customers and allow for a lighter supervisory approach. EMIs are required to keep a segregated pool of liquid funds equivalent to the sum of funds collected from customers and are prohibited from intermediating them. Additionally, regulations often cap e-money transactions and accounts to limit customer, operational, and money laundering risks.[7] EMIs do not have most of the financial risks faced by banks.

Still, EMIs do have risks. Most importantly, EMIs offer payment services (withdrawals, transfers, and purchases) through a variety of channels, using IT systems, telecommunications, business partnerships, outsourcing arrangements, widely dispersed staff and agents, connection to merchants, and payments infrastructures, such as switches and other payment systems. These elements create operational, ML/FT, and consumer risks, among others. Table 1 lists the most relevant risks of EMIs on an institutional level, some of which are covered in this paper.

[6] This fiduciary function exists regardless of how a country defines e-money as opposed to bank deposits.
[7] See Staschen and Meagher (2018) and CPMI (2016, pp. 26–27).

Table 1. EMI risks

Risk	Description
Risk of loss or misuse of customer funds (covered in paper)	This is the risk that (i) EMI employees, agents, or third parties access and misuse customer funds, including for lending or investing purposes, (ii) EMIs fail to manage customer account balances, and (iii) customer funds are unavailable because of bankruptcy of the EMI or the bank holding customer funds. Although this risk may appear to be part of the other risks in this table, it is emphasized because it is at the center of the supervisory review.
Operational and IT risks partially covered in paper)	Governance and internal controls—lack of good risk governance, board oversight, and an effective corporate control environment can lead to the materialization of risks.
	Data and cybersecurity risk—risk that physical and digital assets, such as customer data, hardware, and networks, are compromised. This risk is closely related to fraud risk and data privacy risk.[a]
	Settlement risk—the risk that the settlement will not take place as expected. It comprises counterparties' credit and liquidity risk. Operational failures at the EMI or counterparties can be a source of settlement risk.
	Fraud risk—internal (e.g., by employees) and external (e.g., by customers and cyber-criminals) frauds. The number of reported fraud cases in EMIs globally continues to grow, particularly the number of internal frauds by EMI staff, sometimes in collusion with agents.
	Business continuity risks—weaknesses in the management, maintenance, or soundness of equipment, networks, connections, and physical facilities; inability to prepare for and act on disasters (e.g., flood, fire); and the lack of critical staff. This risk can lead to disruption of operations.
	Agent risks—a key piece of EMI operational risk that can enhance ML/FT, consumer, and other risks. Not all operational risks are attributed to technology. Many arise from people's behavior, such as failure to follow policies because of lack of training or enforcement. For EMIs there is the risk of lack of cash (often referred to as "agent liquidity") at agent points and the risk of poor customer due diligence.
	Third-party risks—in addition to agent risks, EMIs face risks through their business relationships (e.g., payment system operators, card companies, telecommunication companies, cloud computing providers, and entities linked through application programming interfaces).
Liquidity risk (not covered in paper)	The risk of not having enough funds for the EMI to meet its obligations (e.g., suppliers, outsourced parties, employees) when they are due. This is different from EMI agents not having cash to serve customers.
ML/FT risk (covered in paper)	The risk that e-money accounts and transactions may be used to fund terrorist activities and launder proceeds of crimes. To limit this risk, e-money transactions and e-money customer account balances usually are capped by regulation.
Consumer risk (not covered in paper)	Ineffective or no disclosure of key information, unfair contractual terms and conditions, product unsuitability, unfair business and sales practices, no out-of-court redress mechanisms (including internal complaints handling channels). Data privacy risks, the risk of loss of funds, and delays in transaction completion are also concerns.
Strategic risk (partially covered in paper)[b]	The risk of large losses from poor strategic decisions (e.g., expansion into new markets) that could lead EMIs to stop operating.
Legal risk (not covered in paper)	Situations when the rights and obligations of parties involved in a contract (e.g., liability toward customers in case of transaction failure) are subject to uncertainty. It may include the failure to give legal protection of customer funds pooled in trust accounts and the potential costs of legal demands against the EMI for failing to comply with laws (e.g., labor law).

Source: CPMI (2016, 2014, 2000).

[a] See CGAP (2018).

[b] Part of strategic risk analysis is done through the analysis of business plans, which is addressed in Section 3.

2.3 Do EMIs pose systemic risks?

Banks may face intense scrutiny because of their systemic importance. Basic considerations include the (i) relevance of bank financing to the economy, (ii) the size of a bank or bank group, (iii) the risk of bank runs (including by contagion from a troubled bank to a healthy bank), and (iv) the interlinkages among banks. For example, a bank can have large corporate clients that play a key role in the economy; if the bank suddenly stopped financing these clients, the country could suffer. Or a bank may have millions of customers who run to withdraw their deposits because they heard the bank is in trouble. This can lead to runs on other banks. Finally, because banks lend and borrow from one another in a dynamic web of interbank operations, the more banks depend on a certain bank (e.g., for intraday liquidity), the more systemic that bank is. And if that bank fails, other banks may fail, too.

All supervisors interviewed—including those in countries where EMIs have reached a significant scale—agree that EMIs in their countries pose limited or no systemic risk.

Although EMIs do not provide finance, they can provide fund storage and payment services to customers. EMDE supervisors need to assess whether an EMI poses systemic risk and understand that some EMIs can grow very large very fast. To determine the systemic importance of EMIs, supervisors should ask the following questions:

- Can an EMI become so large (i.e., number and types of customers) that the welfare of many people would be significantly affected if the EMI goes bust and thus can no longer provide a critical or highly valued service?
- Could the failure of one EMI deteriorate the public confidence in the EMI sector and, thus, trigger contagious effects?
- Could the failure of an EMI affect public confidence in banks or other regulated financial institutions?
- What types of businesses (e.g., government services, private sector companies) rely significantly on the EMI? How would a disruption in the EMI's operations affect these businesses? Are major losses expected?
- Has an EMI become a systemically important payment system?[8]
- Can an EMI introduce risks to the national payment system?[9]

[8] CPMI (2001, p. 14) provides guidance on how to identify systemically important payment systems. The guidance focuses on financial sector stability and does not cover consumer protection, competition, and crime prevention, which might be relevant to EMIs.
[9] EMIs can participate in the national payment system—more specifically by directly linking to the real-time gross settlement system—in only a few countries (e.g., the United Kingdom).

- Can an EMI affect banks by increasing banks' exposure to large depositors (large balances in the e-float accounts)?[10]
- Can an EMI affect the profitability of banks by competing for clients, limiting access to agent networks, etc.?
- Can an EMI be a conduit for laundering large amounts of illicit money?

2.4 Increasing efficiency of onsite visits with better offsite preparation

Proportionality requires seeking efficiencies on offsite monitoring and onsite or offsite procedures during an examination.[11] For example, frontloading offsite preparation work (i.e., doing ongoing high-quality offsite monitoring and, during examinations, requiring and analyzing documents and data before going onsite) can optimize onsite time. To prepare for an onsite visit, you may need to ask the EMI for information (e.g., policies/procedures and a granular dataset) and then to follow up with specific requests (e.g., for a sample of transactions).

Some EMDE supervisors send only one documentation request before the onsite visit.

Flexibility in preparing for an examination that includes onsite visits allows supervisors to make several requests to EMIs and organize preliminary findings for onsite follow up. This increases efficiency and saves time for both the supervisor and the EMI.

In addition, SupTech could help increase efficiency and effectiveness of data analysis, system audits, penetration tests, and so forth. Machine learning applications, which are widely available, can identify patterns and correlations that could indicate, for instance, unauthorized changes to customer records, attempted intrusions, and suspicious transactions.[12] However, the quality of SupTech outputs depends on the quality of the data used, so supervisors may need to improve their data first.[13]

Data include the standardized data regularly reported by EMIs and nonstandardized (unstructured) data, such as previous inspection reports, licensing applications, EMI management reports, thematic reviews, agent agreements, consumer contracts, etc. Supervision is more effective when these types of data are used, but they are not always easy to gather.

[10] See Kerse and Staschen (2018) for more on concentration risk.
[11] "Examination" is used in this paper to refer to an assessment focused on a single EMI. An examination often includes both offsite and onsite procedures and can vary substantially in its scope. Different countries use other terms to refer to assessments at individual institutions.
[12] See Dias (2018) and FSI (2018) for more examples.
[13] See Dias and Staschen (2017) for more on digital financial services supervisory data and data collection mechanisms.

EMDE supervisors face challenges in using unstructured, nonstandardized data. They spend long hours reading documents where information is presented in narratives or unstructured numerical-based data, in formats like PDFs, and even in hard-copy, printed versions.

SupTech solutions include using analytics software to integrate a variety of data formats and make them usable.[14] For example, analytics software can allow users to search for and analyze a large array of digitized documents automatically and to cross-analyze structured and unstructured data from a range of sources to generate insights for supervisory inquiry. SupTech can make it significantly easier to sort and analyze text-heavy documents like policies and procedures manuals.

2.5 Implementing risk-based EMI supervision

Supervisors can use a risk-based methodology to develop a proportional approach to EMIs. This type of methodology provides a systematized view of risks and their relative

Box 2. Risk-based supervision

In a risk-based approach, supervisory effort focuses on the greatest risks of regulated markets.[a] The approach provides formal guidance on supervisory priorities, how supervision is to be conducted, and how supervisory decisions are to be made.

Risk-based methodologies are often summarized in risk matrices. A risk matrix presents all risks inherent to a type of business—according to the activities permitted by regulation for the type of institution—and the risk factors for each risk category. It assigns weights to risk factors and categories according to their relative importance to the business type. Based on actual risk assessments of individual institutions, supervisors indicate how well or badly an institution mitigates inherent risks through governance, risk management, and internal controls. This methodology culminates in a risk rating assigned to each institution that is comparable across institutions. The matrix allows for better supervisory planning and use of resources. The more risk areas exist in a type of regulated institution, the more useful the matrix is for identifying supervisory priorities and summarizing the results of examinations.

[a] For further guidance on risk-based supervision, see Wright (2018).

[14] See Bauguess (2018) for more on machine-readable supervisory data (data in a format that can be used by analytical software).

importance within and across EMIs and can help to standardize supervisory procedures. It also helps supervisors to increase or reduce the intensity of supervision of different EMIs over time, in a structured manner, according to past assessments of EMIs. In a risk-based approach, supervisory procedures, such as the ones described in this paper, are deployed according to an initial risk assessment based on a comprehensive data analysis. A risk matrix is commonly used to summarize the risk profile of a regulated institution.

There is no single risk-based methodology and risk matrix model that would work for all EMI supervisors. Supervisors often define risks differently and choose different risk categories, risk factors, and respective relative weights for their risk matrices. They also create different risk rating and trend assessment methods. A risk matrix that is generally designed for banks will not fit the risk profile of EMIs and will need to be adapted.

While all supervisors interviewed report using a risk-based approach to supervise banks, only a few have adapted their methodology to EMIs.

2.6 Organizational arrangements for EMI supervision

Although there is no single approach on where EMI supervision should be located, e-money is a financial service, and as such, it should be the responsibility of financial sector authorities (e.g., the central bank), not telecommunication authorities, even when EMIs are owned by mobile network operators (MNOs).[15] Within a financial sector authority, the internal arrangement for EMI supervision may vary.

Financial sector authorities in all the countries researched assign the responsibility of EMI supervision to a financial supervisory authority—typically the central bank—rather than other financial sector authorities such as the Ministry of Finance. In a few countries, an independent supervisory authority (e.g., a banking superintendence) took on this responsibility. In most of these cases, the central bank continues to be responsible for payments regulation and payment systems oversight (with a focus on infrastructure, safety, and efficiency).

In the United Kingdom, an independent regulator—the Payment Services Regulator (PSR)—was created in 2015. PSR regulates payment services providers and payment system operators, while the Financial Conduct Authority supervises payment services providers, including EMIs. Oversight of the national payment system for stability purposes and the operation of key payment systems are done by the Bank of England.

[15] In at least one country, Kenya, the central bank can authorize MNOs to become an EMI, in which case the MNO's e-money line of business is regulated by the central bank and is subject to supervision. However, in most countries, the EMI must be a separate legal entity that is dedicated to e-money issuing.

Different approaches are used internally at supervisory authorities as well. In most of the African countries studied (e.g., in Ghana, Kenya, Rwanda, Tanzania), the central bank's payments department—which primarily focuses on payment system oversight—has become the EMI supervisor. In most cases, oversight and supervision are separated from central banking operations (e.g., real-time gross settlement systems, check clearing, market operations). In Hong Kong and Singapore, where the EMI supervisor is also the central bank, EMI supervision is done by the bank supervision department. In countries with an independent financial supervisor separate from the central bank (e.g., Austria, France, Luxembourg, Mexico, the United Kingdom), this often includes a team specialized in payment service providers.

The experience among the supervisors interviewed indicates that there is value in creating a specialist team for operational and IT risks that covers all types of regulated entities, including EMIs. Examples of this can be found in Austria, Brazil, France, Hong Kong, Luxembourg, Malaysia, Mexico, Peru, the Philippines, and Singapore. Some of these countries also have specialist teams for AML/CFT and market conduct, and some have a specialist cybersecurity team (e.g., the United Kingdom's Financial Conduct Authority).

All organizational arrangements require some degree of coordination. Interagency coordination is useful for both regulation (e.g., MNO regulation on access to channels such as USSD) and supervision (e.g., monitoring by data protection authorities, assessing the impact of e-money business on the MNO's business and vice-versa, monitoring mobile insurance by the insurance supervisor, etc.). Interdepartmental coordination is needed, for instance, between payments oversight and EMI supervision, EMI supervision and bank supervision (e.g., to draw on experience with bank examinations, check compliance with e-float limits on a bank, and coordinate in case of EMI resolution), and EMI supervision and specialist teams (e.g., operational risk).

3. Licensing EMIs: Analyzing the business plan

In many countries, EMIs are required to have a license to operate.[16] Supervisory authorities conduct a range of analyses on licensing applications to ensure the EMI, its owners, and management meet minimum criteria, such as capital and fit-and-proper requirements. Some supervisors also inspect EMIs before they begin operations and do background checks on significant shareholders, board members, senior management, and other key positions in the EMI.

This section does not cover all issues addressed during licensing. Rather, it provides basic guidance for analysis of EMI business plans.

A business plan (and financial projections) is required by all supervisors interviewed where EMIs are subject to licensing, and some (e.g., Luxembourg's CSSF and Bank Indonesia) also require periodic updates of the business plan after the license is granted.

Business plans can be analyzed from two perspectives: their quality as a planning tool and the strength of the plan itself.

A low-quality business plan could signal poor planning skills or unwillingness to share information with the supervisor. A poor plan in terms of its content could signal strategic risk based on poor business acumen. These perspectives apply to business plans of both new and already established EMIs. EMIs may update their business plans periodically to adapt strategies and projections to changing market conditions and past performance.

When assessing the quality of a business plan, supervisors should keep the following in mind:

- The plan needs to be complete and comprehensive.
- The sum of the parts of a plan needs to be cogent, with little inconsistency.

Although there is no standard approach to organizing and labeling sections of a business plan, in general, a complete business plan (of any type of organization) describes the overall strategy, its operations, and its financial projections. Table 2 provides an exemplary structure of an EMI business plan.

[16] The term "licensing" is used broadly to refer to any mandatory authorization process to which EMIs are subject before being allowed to start operating or to continue operating after a new EMI regulation is passed. Countries may use other terms such as "registration" and "authorization."

Table 2. Potential structure of an EMI business plan

Risk	Description
The strategic plan	i. Mission, vision, objective ii. Market analysis a. Market overview, total size, and growth potential b. Market trends, competitive landscape c. Market segments and target segments d. Positioning (what needs of the target segments will be met) e. Products/services to be offered f. Projected market share g. Success factors (e.g., agent network, product design, shareholder commitment, regulation, partnerships, technology, infrastructure) iii. Analysis of strengths, weaknesses, opportunities, and threats iv. Summary of business strategy
The operational plan	i. Products and services ii. Business model and partnerships iii. Growth and investment strategy iv. Marketing strategy v. Governance, organizational structure, and staffing vi. Systems, controls, and risk management vii. Implementation roadmap (timeline)
Financial plan (also called financial projections or viability plan)	i. Basic assumptions (e.g., inflation rate, cost of funds, GDP growth) ii. Initial capital, investment and capital injection plan, source of funds iii. Forecasted revenues, capital expenditures, operating expenses, profit/loss iv. Key financial performance indicators v. Projected financial statements

In a poor business plan, important components may not be addressed or they may be poorly developed. Even if these components are present and fully developed, there may be inconsistencies. For instance, an EMI may project an unrealistic growth in the number of customers and transactions without a supporting strategy to address competitors, without an aggressive plan to grow the agent network, and with insufficient resources to cover marketing expenses. Other potential inconsistencies include misalignment between projected revenues and a small target market segment (e.g., only farmers in rural areas), high capital expenditures (e.g., furniture, IT infrastructure, risk management software) against a low budget, and discrepancies in the plan's narrative and the financial projections.

Supervisors need to have knowledge about the EMI business, in general, and local market conditions, in particular, to assess whether the assumptions underpinning financial projections are reasonable. For instance, the EMI's market analysis (e.g., description of competitors and their strategy, market size, access to infrastructure such as switching services and specialized labor) may be inaccurate, and other assumptions (e.g., GDP growth, cost of funding, socioeconomic and demographic indicators, size of target market segment, customer adoption rate, growth in revenues, etc.) may be too optimistic. The objective is to judge the reasonability of the projections; no plans will be foolproof.

If financial planning and analysis expertise are available, the calculations in the financial projections could be probed. To do this, the financial projections need to be in a digital format (e.g., Excel or other) that allows the formulas to be scrutinized. The next section outlines basic guidance for analyzing key performance indicators for licensing.

To assess the business plans of EMIs (particularly mobile money providers), supervisors should consider the EMIs' typical growth trajectory, according to patterns seen with mobile money that uses extensive agent networks. (Such a trajectory may not hold for other business models.) The following are three phases of growth:[17]

- Start-up—high CAPEX, OPEX growth, probable loss
- High-growth—OPEX growth, revenue growth, modest profit, investment in customer acquisition through sales force and marketing
- Mature—potential additional revenue sources through product diversity and partnerships, solid profit

[17] Almazán and Vonthron (2014) note that the largest operating expenses for EMIs in the first years of operation are investments in the e-money platform and the creation of the agent network, which includes fee expenses and commercial efforts. A small profit may appear in the second or third year, while expenses with agent acquisition and fees continue to be high relative to the revenues.

4. Offsite monitoring (surveillance) of EMIs

Continuous offsite monitoring—or surveillance—is fundamental to risk-based EMI supervision. Continuous monitoring helps supervisors identify (and compare over time) variations in the risk profiles of different EMIs. It also helps them spot indications of risks that could preempt supervisory (including remedial/corrective) action (e.g., an inspection on fund safeguarding, fraud, or strategic risk). Monitoring involves analyzing the EMI market (e.g., market development) and individual EMIs, thus, monitoring is an integral part of supervisory planning, EMI examinations, and the regulatory process.

Only a few of the EMDE supervisors interviewed conduct comprehensive market monitoring (surveillance or oversight) on an ongoing basis, while this is a common practice among supervisors of developed economies.

Offsite monitoring may involve analyzing internal standardized and unstructured data from the supervisory authority (e.g., reports submitted by EMIs) and external data (e.g., government statistics and MNO data). It may use financial data (e.g., key indicators) and nonfinancial data (e.g., consumer complaints, transaction volume).[18] In general, the analyses follow a standardized methodology and uniform criteria defined by the supervisory authority according to its objectives (see Table 3 for a few examples). Given the objectives, the depth and frequency of the analyses will depend on the data, the technology, the supervisor's skills, and the priorities set by the risk-based methodology.

Although assessing the financial performance of all EMIs may not be the top concern of supervisors, efficiently monitoring key financial indicators and other business metrics on an ongoing basis can help to establish supervisory priorities.

All supervisors interviewed indicated that financial statements (balance sheet, income statement), prudential indicators (e.g., capital and liquidity ratios), and key performance indicators (e.g., ROA, ROE, CAPEX, etc.) are required to varying degrees and with varying frequencies.

Table 4 provides some financial and business metrics. The type and number of indicators used will depend on the supervisor's preferences and analytical skills and on

[18] See Dias and Staschen (2017) for an overview of the data collected by EMI supervisors.

Table 3. Examples of objectives pursued with offsite monitoring and related data

Objectives	Examples of data used
Measure systemic risk and relative importance of EMIs	Volume and value of total EMI transactions relative to bank transactions or transactions in the RTGS or other payment systems, size of e-float and number of customers, in relation to total bank deposits and bank clients. Number and type of large fund flows (e.g., government salaries and social transfers), total value of transactions relative to GDP or total bank payments in the RTGS, operational disruptions in EMIs considered systemic, etc.
Monitor market development and financial inclusion[a]	Number and location of agents; overlap of agent points with MNO coverage (towers) and other official demographic and socioeconomic indicators (e.g., schools, health clinics, total population); number of agents per adult or total population by population segment (e.g., rural x urban); number and value of total EMI transactions by type of transaction (e.g., check whether digital means are increasing in importance, versus cash); number of inter-EMI and EMI-bank transactions (interoperable transactions); number of shared/exclusive agents, etc. Percentage of adults within a certain radius of an agent or other access points; account penetration in urban and rural areas; per total adult population and by certain breakdowns such as by gender, age, or income level; number of EMI customers with bank account, insurance or credit, percentage of active EMI accounts, etc.
Assess individual and relative performance of EMIs, and set benchmarks	Key performance indicators (see Table 4)
Check compliance with regulatory requirements	Minimum capital ratio relative to total e-money issued, minimum liquidity ratio, regulatory limits to account balances or deposits, total e-money issued versus balance in the float account, balance in the float account relative to total deposits of banks holding the float accounts, etc.
AML/CFT	Patterns of transactions volume and values by type, agent, location (including locations considered riskier such as border cities), statistics of suspicious transaction reports, etc.
Consumer protection and competition	Number of complaints by type of complaint and status, fees by type of transaction; location and duration of MNO and EMI disruptions; number of failed (not completed) transactions; duration, location, and frequency of system downtime; fraud volumes, types, and location; etc. Interchange fees on interoperable transactions, market share of EMIs, fee revenue in relation to transaction volume, fees on specific transaction types (person-to-person transfer, deposits, withdrawals), number and location of exclusive agents, agent fees, etc.

[a] See CPMI (2017) for standards for retail payment statistics to measure market development and CPMI (2016, p. 59–62) for indicators for financial inclusion monitoring.

the availability of SupTech and input data. Many indicators can be extracted from the financial statements periodically reported by EMIs, while others require additional data (e.g., total e-money issued; number of accounts/clients; fees paid to agents; fees from partnerships with third parties, such as lenders; and fees by type of product) to be collected.

All supervisors interviewed meet with EMIs outside of specific examinations, but only a few have incorporated this intelligence gathering opportunity into their formal supervisory risk-based methodology. For instance, some supervisors organize annual outreach meetings or schedule meetings with individual institutions, while others meet EMIs on an ad-hoc basis, as needed or as requested by the EMIs.

Table 4. Examples of financial and business metrics for EMI supervision

Business metrics
Total e-money issued (e-float)
Number of e-money accounts
Number of e-money clients
Number and value of transactions
Financial metrics
EBITDA: Net income before interest, taxes, depreciation, and amortization
EBITDA margin (net margin): EBITDA as % of gross revenue
OPEX ratio: Operating expenses (OPEX) as % of gross revenue
CAPEX ratio: Capital expenditure (CAPEX) as % of gross revenue
ROE: Return on Equity is net income as % of equity
ROA: Return on Assets is net income as % of assets
Gross revenue: Total income from commercial activities (e.g., provision of payment, withdrawal and transfer transactions to customers against fees)
Revenue streams
• Transaction fees from customers by type of product/service
• Fees collected from partners (e.g., insurers, lenders)
• Other income sources (interest income and investments)
Fee income as % of gross revenue
Fee income as % of number of transactions
Fee income as % of number of e-money customers
OPEX: Operating expenses, by type of expense (e.g., agent fees)
OPEX per number of staff members
Total agent fee and fees to agent network managers
Total agent fee as % of number of agents
Total agent fee as % of number of transactions
CAPEX: Capital expenditure (e.g., update of e-money platform)
Capital: Money reserved in form of capital (e.g., equity)
Capital (solvency) ratio: Regardless of whether the regulation requires EMIs to maintain a minimum level of capital or equity in relation to the assets or the e-float, it's useful to monitor EMIs' solvency.
Liquidity ratio: Short-term assets (cash and other highly liquid asset, such as government bonds) as % of short-term liabilities (e.g., salaries, rent, accounts payable)

Supervisors also gather market intelligence as part of ongoing market monitoring. They meet with EMIs, industry associations, and knowledgeable third parties.[19] Supervisors can discuss their expectations on compliance, current concerns, and broad supervisory findings when they meet with the EMIs.

[19] See BCBS (2016b) for guidance on market intelligence.

5. EMI examinations (offsite and onsite procedures)

5.1 Introduction

In addition to conducting offsite monitoring on an ongoing basis, supervisors often conduct examinations of individual EMIs that focus on one, a few, or every risk area. Different approaches are used for different EMIs and across countries. For instance, a supervisor may conduct examinations on all EMIs at a point in time solely to check how EMIs implement fund-safeguarding requirements, while subsequent examinations on this or other issues (e.g., consumer protection) would be triggered by the findings of offsite monitoring. Generally, when fund safeguarding is effective, the supervisory scope and depth can be more limited, at least for nonsystemic EMIs. For large EMIs, supervisors may increase the depth of fund safeguarding analyses and expand the scope of examinations by including other risk areas, such as operational risk and AML/CFT controls.

Despite using different supervisory practices, all supervisors interviewed agreed that the most important area of EMI supervision is customer fund safeguarding. Other priorities included operational risk, AML/CFT controls, and consumer protection. Not all supervisors cover all of these (a few do not even check fund safeguarding), while others (none in EMDE) cover these and many additional areas, such as strategic risk.

This section does not provide guidance for examinations of all risk areas that supervisors can cover for large or small EMIs (see Table 1). It is limited to describing potential procedures for assessing three important areas of EMI supervision: fund safeguarding (Section 5.2), operational risk (Section 5.3), and AML/CFT controls (Section 5.4). For each of these, we summarize common regulatory requirements, suggest the scope of an examination, and finally, illustrate offsite and onsite procedures. The procedures may be adopted in their totality or partially, in combination or separately, as part of full EMI examinations or of thematic reviews.[20]

[20] In addition to offsite monitoring and EMI-focused examinations, thematic reviews can be useful, particularly in the initial years of EMI supervision. Thematic reviews give in-depth insight into specific issues, thus helping the supervisor compare good/bad practices and communicate its expectations to EMIs. The reviews can also help the regulatory authority improve regulations. Thematic reviews focus on one or a limited number of topics (e.g., fund safeguarding) but cover several EMIs. They may comprise offsite and onsite procedures like those described in this section. Among the supervisors interviewed, only a few conduct thematic reviews on the EMI industry.

Box 3. Review policies and procedures manuals—a key examination technique

The risk management practices and operations of EMIs are expected to be described in written policies and procedures manuals endorsed by the EMI's board and enforced across the EMI by senior management, with board oversight. This type of documentation is commonly reviewed by supervisors to (a) assess their completeness, reasonability, and alignment with regulations and international standards and (b) to partially guide the supervisor's follow-up inquiries during offsite and onsite examinations. Supervisors may request and analyze policies and procedures manuals for all areas covered in this section. An EMI that lacks or does not update policies and procedures manuals should raise supervisory concerns.

Many examinations include a review of policies and procedures manuals. The following is a three-step approach on how to do this: (i) analyze the manuals and policies offsite, (ii) gather evidence about their implementation (offsite and onsite), and (iii) probe the information through observation, interviews, and system audits (onsite).

5.2 Fund safeguarding

5.2.1 Key regulatory requirements

Most EMI regulations include fund safeguarding requirements that have two elements:

- **Segregation.** EMIs are required to set aside a minimum amount of money to back the e-money issued or e-money liabilities (***e-float)***. Typically, they must back 100 percent of the e-float, by depositing the equivalent amount into an account (***float account***) separate from the EMI accounts used for running daily operations (e.g., paying bills, paying/receiving fees, etc.). There may be one or several float accounts.[21]
  - ***Liquidity requirement***. Regulations require that the e-float be invested (if any investment is permitted) only in liquid and low-risk assets, such as government bonds, or simply in an account with a commercial bank (that may or may not pay interest).
  - ***Diversification requirement.*** Some regulations require EMIs to spread the e-float into different banks, to protect against the risk of bank failure.[22]

[21] This section considers the most common approach EMIs use to safeguard float: depositing it into an account at a commercial bank and/or holding it in safe investments. Other approaches, which could affect the legal, operational, and supervisory issues discussed in this paper, are described in Mehmet and Staschen (2018).
[22] From a bank supervision perspective, this requirement limits the risk of large depositors at individual banks. See Kerse and Staschen (2018).

- **Ring-fencing.** Ring-fencing arrangements protect the e-float against EMI creditors (e.g., lenders, investors, suppliers, employees, government). This can be done by requiring the float account to be a special type of account, such as a trust or escrow account.[23]
  - ***Unencumbered e-float.*** Regulations may prohibit EMIs from encumbering the e-float (e.g., pledging them as guarantee for loans) and/or may state that the funds in the float account are not assets of the EMI.[24]

Effectively safeguarding funds by EMIs does not depend only on whether the e-float is safe, but also on whether individual customer claims can be clearly identified and the information in the claim has not been altered. Thus, safeguarding funds is affected by how operational risks (e.g., the risk of fraud, errors and mistakes, business continuity, IT, and cybersecurity) are managed. Some operational issues in fund safeguarding are addressed in this section, while others are addressed in Section 5.3. Also, supervisors should assess whether the use of several float accounts in several banks makes fund safeguarding less effective. Finally, safeguarding focuses on ensuring liquidity to meet customer claims in two scenarios: (i) over the course of the EMI's life (covered in this section) and (ii) in the event the EMI goes under.

5.2.2 Scope of examinations

Checking the float account balance is the most basic way to verify that the EMI is complying with the fund-safeguarding requirement. However, supervisors will need to use additional examination procedures if they want to assess the quality of the policies, procedures, and systems behind the balances reported by EMIs (e.g., to validate the accuracy of such numbers and to assess the EMI's risk management and internal controls that affect fund safeguarding). A comprehensive examination on fund safeguarding could cover the following:[25]

- Existence and sufficiency of funds in the float account
- Terms and legal status of the float account
- Procedures to ensure the required balance (i.e., reconciliation)
- Float account governance and management
- Liquidity of the float (i.e., investment types and no pledges)
- Accurate control and reporting of e-float and client balances

[23] See Staschen and Meagher (2018) and Greenacre and Buckley (2014).
[24] Depending on the country's law for trust or escrow accounts, pledges on the float are invalid.
[25] Several EMDE supervisors interviewed check only that there are sufficient funds in the float account.

5.2.3 Examination procedures

5.2.3.1 EXISTENCE AND SUFFICIENCY OF FUNDS IN THE FLOAT ACCOUNT

Supervisors can compare reports on the e-float with reports on the float account balance. To confirm the veracity of these reports, supervisors can analyze bank statements of the float account to do the following:

- Check the float account identification data (e.g., number, branch, account holder) against the float account agreement/contract and the periodic reports sent.
- Check the balance of the float account at several cut-off dates and compare with total reported e-float on the same dates to test consistency.[26]
- If interest and investment profits are paid in the float account and used by the EMI (including to distribute to customers), check whether the total balance reported excludes these amounts because there may be a separate claim over them in addition to the claim on the e-float.[27]
- Check whether credits and debits are concentrated around the reporting dates, which could raise suspicion of weak reconciliation or intentional mismatching and its cover up.

These procedures assume that the reported e-float is accurate. Supervisors can test the accuracy of the reported e-float by following the procedures in 5.2.3.6.

5.2.3.2 THE TERMS AND LEGAL STATUS OF THE FLOAT ACCOUNT

Float accounts are usually opened at banks. If a trust, escrow, or some other special type of account is required, the supervisor can review its formality (e.g., if it follows legal requirements for trust/escrow accounts) and its terms and conditions (which may vary according to the bank holding the float account). This is done by analyzing the trust or escrow (or similar) account agreement between the EMI/trustee and the bank to check whether it complies with any specific requirements, such as those in the country's trust laws or other applicable law. In the case of trusts, some countries require a trustee (which, in some countries, can be the bank holding the trust account) to be created to manage the funds on behalf of the e-money customers, while other countries allow the float account to be managed by the EMI, and the agreements will vary accordingly.

[26] Mismatches could mean ineffective controls, intentional mismatch, or even fraud.
[27] If the profits from investments and interest are not distributed or used otherwise, then there is no obvious reason for not counting them toward compliance with the minimum required balance unless this is prohibited in regulation.

The trust agreement may contain information about whether and how the account can be accessed and how funds can be withdrawn from it, including to be invested in other assets, etc. The agreement might detail the trustee's powers and responsibilities, compared tothe EMI's responsibilities, and the role of the supervisor, including the supervisor's prerogative, if allowed by law, to inspect the trustee. Similar restrictions on the use of funds and how they can be accessed may exist in the case of escrow accounts.[28]

5.2.3.3 EFFECTIVE RECONCILIATION PROCEDURES

Understanding how the EMI reconciles the float account with the e-float is key to probing the effectiveness of fund safeguarding. The EMI must ensure there is always sufficient balance in the float account, and many regulations require reconciliation by the end of each business day.

Among the EMDE supervisors interviewed, there was limited knowledge about how EMIs reconcile the float account with the e-float. There is wide variation in reconciliation procedures across EMIs, from highly manual (e.g., an EMI staff calls the bank at the end of each day to increase/reduce the balance in the float account) to entirely automated (e.g., the float account is adjusted automatically once [i.e., batch] or several times [i.e., real time] through integrated EMI and the bank systems).

The first step is to study the relevant policies and procedures, which should describe the reconciliation process and assign staff responsibilities. Lack of formal policies and procedures could lead to insufficient fund safeguarding. Also, it is useful to understand how e-money is created (i.e., situations that increase the e-float) and destroyed (e.g., situations that decrease the e-float). E-money creation/destruction can vary across EMIs. For instance, in EMIs working with intermediaries that buy large quantities of e-money (often called super/master agents or distributors) for distribution (sale) to individual agents (which in turn sell e-money to retail customers), the e-float may be affected only when such intermediaries buy e-money, but not when agents and customers make transactions (buy/sell e-money).

It is also important to know whether reconciliation is done once or several times a day or if transfers are done immediately when e-money is created/destroyed (real time) or otherwise. For instance, some EMIs permit certain intermediaries, agents, and merchants to pay for e-money by transferring funds directly into the float account. In other cases, there is a single daily reconciliation immediately before the bank's closing time to reflect the net creation/destruction of e-money throughout the day. Finally, transfers to/from

[28] Some supervisors interviewed in Africa check the terms of interest payment and fees imposed by the bank, in part because banks have created obstacles to EMIs by offering poor terms or refusing service.

the float account can be automated or manually initiated. Supervisors need to identify whether different types of reconciliation are used in the same EMI and assess their risk.

From a supervisory standpoint, effective automated reconciliation (whether real time or in batch[es]) is expected to reduce errors and delays. If data security and integrity controls exist, they should reduce the risk of fraud and unauthorized access to the float account. Even in the case of automated procedures, it is worth reviewing how the system is set up, by (i) asking about the rules encoded in it to trigger the transfers between the EMI bank account(s)[29] and the float account and (ii) identifying steps that require manual intervention to assess their risk. Also, supervisors need to assess how reconciliation happens when a trustee is involved in the management of the float account.[30]

With detailed knowledge of the whole process, supervisors can assess the risk of deficiency in the float account from failure of internal control or tampering by employees at the EMI, bank, or trustee. In the case of automated reconciliation, supervisors may conduct system tests simulating variations in the e-float, unauthorized access to and alteration of the e-float information, and purchases or sales by agents and master/super agents. Other potential techniques include observing a full reconciliation process (when manual) and reviewing audit trails of reconciliations (when automated). If the review in Section 5.2.3.1 reveals mismatches, the supervisor can look at the records of the reconciliation on the mismatch dates and ask for an explanation.[31]

If an EMI uses several banks to hold portions of the float, supervisors can ask how the EMI divides the e-float (e.g., whether it will depend on the banks where the master/super agents have accounts). The EMI should be able to ensure that the reconciliation is similarly effective for all banks. Supervisors should identify whether there are differences in reconciliation across banks and assess their effectiveness.[32]

5.2.3.4 FLOAT ACCOUNT GOVERNANCE AND MANAGEMENT

Float account governance and management play an important role in the reconciliation and the safety of the funds. EMIs must have written policies and operational proce-

[29] These are the bank account(s) used by the EMI to run its business, including to receive fees and deposits from consumers and to pay expenses such as salaries. The funds to be deposited in the float account will come out of these accounts (unless buyers of e-money can pay for e-money by depositing directly into the float account).
[30] Depending on the arrangement, the examination procedures may need to be performed at the trustee.
[31] Supervisors may investigate mismatches further by checking if there is any internal management or audit report about the mismatches and whether and how mismatches are regularly reported to the board, risk committee, or audit committee, if any.
[32] Depending on the regulation, EMIs may be required to spread the e-float across several banks according to certain criteria (e.g., maximum portion of the total e-money issued per bank). In such a case, the supervisor may add procedures to check compliance with the specific requirements and criteria.

dures that govern access to and operation of the float account. In most cases, only a few designated employees are authorized to access and make transactions in the float account. In addition, the EMI needs to have a contingency plan that ensures reconciliation continues as expected when the principal operator is unavailable.

The access and escalation rules must be commensurate with the EMI's structure, size, and complexity (e.g., in large EMIs, lower-level staff may have access to the float account) and the type of reconciliation mechanism (e.g., fully automated versus manual). Rules should be documented, and they should define the transactions permitted for each user profile. Supervisors can analyze the list of employees and their relevant user profiles to decide who they should interview to learn more about adherence to EMI policies and the instances in which the policies were broken. Similar controls should be in place if a trustee operates the float account.

In addition to access rules and user profiles, there should be formal rules for managing the funds (e.g., transferring to/from the float account). This is related to reconciliation, but it also includes other situations, such as responsibilities and procedures for periodically checking interest or other income flowing into the float account and their withdrawal or distribution and dealing with errors, such as transfers resulting from glitches in IT codes. Supervisors can test EMI policies through system audits.

5.2.3.5 LIQUIDITY OF THE E-FLOAT

Supervisors also can conduct checks to ensure EMI compliance with liquidity requirements (i.e., permitted investments of the e-float). Most country regulations are strict. They either prohibit investment (e.g., require funds to be in demand deposits) or allow investments only in assets prescribed/authorized by the supervisor. Others allow (and some may require) a percentage of the e-float to be invested in low-risk government bonds. Only a few (e.g., the Central Bank of West African States) allow risky investments such as securities.[33]

Supervisors can start by asking about the investment policy/strategy (e.g., risk profile, target return, assets), any recent changes (and their reasons) to the policy, and how decisions are made. Generally, the board should approve the investment strategy and the risk management functions, and the risk committee, if any, should monitor the results. Supervisors may also ask whether the investment strategy varies across float accounts and request and analyze evidence of the investments made (e.g., statements of investment accounts, statements of the float account showing transfers to investment

[33] See Kerse and Staschen (2018).

accounts), assess their performance and level of risk, and confirm the information with investment managers.

Another area of interest is the regulatory prohibition of pledging the e-float as a guarantee for loans or other type of encumbrance. Supervisors can interview senior management and ask them about areas of concern that came up in separate interviews with staff responsible for EMI borrowings. For additional clarify, supervisors may analyze the EMI's borrowings (loan contracts).[34]

5.2.3.6 ACCURATE CONTROL AND REPORTING OF E-FLOAT AND CLIENT BALANCES

Keeping accurate control of customers' account balances is one of the most basic obligations of an EMI. The EMI should report to the supervisor the correct e-float (sum of all customer account balances), which is central for supervision. To assess this, supervisors can do the following:

- **Assess if there is accurate control of client balances:**[35]
  - Review complaints data to check for complaints about insufficient or incorrect balances.
  - Review the EMI's dormant account activity and management practices.
  - Review the EMI's practices for settling offline transactions.[36]
  - Check the rules that allow access to the e-money platform and whether there are profiles that are authorized to alter client balances and under which situations. Probe rules by conducting system tests (e.g., unauthorized alteration of client balances).
  - If weak controls are a concern, conduct transaction simulations to check whether the system correctly updates a client account balance for each type of transaction offered.
  - Ask about the rules around the amounts kept temporarily in settlement or suspense accounts and how they affect client balances on the sending and receiving end.[37]

[34] In countries where the trust (or other) law recognizes customers' ownership of the float account balance, encumbrance of such nature is usually legally null (i.e., the EMI lender would not have a claim even if the float is pledged in the loan contract between the EMI and the lender).
[35] The controls should be the same for any type of client, including agents.
[36] Most EMI regulations in EMDEs require e-money transactions to be conducted in real time (i.e., immediately affecting customer account balances), but there are exceptions. When offline transactions are permitted, customer account balances will be outdated temporarily before the transaction is finally settled. These and other issues in operational risk (e.g., data security, disaster recovery) are important to enable continuous access to updated client balance information.
[37] These accounts are designed to hold funds temporarily, while transactions or unclassified and disputed funds (e.g., when a customer sends money to the wrong mobile number and reports it to the EMI before the transaction is settled) are being settled.

- Assess if there is accurate reporting of the e-float:
  - Compare previously reported e-float on several cut-off dates with reports generated upon the supervisor's request and in the presence of the supervisor (onsite) directly from the EMI e-money platform (account system).
  - Ask how periodic regulatory reports on the e-float are produced, who the responsible staff are, and whether manual procedures are used to generate the report. Ask staff responsible for the reports about weaknesses (e.g., whether the EMI system is not able to automatically report the total e-money issued or any other field in the regulatory report). If concerns arise, require staff to simulate the production of a report in front of supervisors and ask about the steps taken when errors have been found in the reports.
  - Ask whether pending transactions (i.e., amounts temporarily registered in suspense or settlement accounts) are included in the total e-money issued reported to the supervisor and are considered for replenishing the float account. Probe rules by conducting system tests.

5.3 Operational risk

5.3.1 Key regulatory requirements

Operational risk is defined as the risk of loss resulting from (i) failed internal processes, people, and systems or (ii) external events (BCBS 2011, p. 3). EMI regulations may contain general requirements for EMIs to manage their operational risk, including risks related to agents, frauds, cyber-threats, IT systems, and business continuity. These regulations typically require a minimum risk governance and management structure, such as board oversight and an internal auditor, and senior management responsibilities, including establishing written policies and procedures, internal controls and risk management, and compliance functions. In some countries, a separate outsourcing regulation may apply to EMIs and impose rules such as for data storage (e.g., outsourced cloud computing) and the supervisor's access to the outsourced parties (BCBS 2016a, p. 28 [EC 8]). There also may be regulation on data security and business continuity.

5.3.2 Scope of examinations

Operational risk is complex and involves interdependencies with other areas, such as fund safeguarding, AML/CFT, and consumer protection. A comprehensive operational risk examination can be burdensome and may not be justifiable for all EMIs. Supervisors need to determine to what extent and how often, according to their risk-based approach, each EMI will be covered for operational risk and adjust this coverage over time.

This section does not address all aspects of operational risk nor does it provide a structure for a comprehensive assessment. Rather, it gives high-level guidance for the following:[38]

- Risk governance
- Overarching operational risk management framework
- Fraud prevention and management
- Data security (including cyber-security)
- Business continuity and disaster recovery

While most procedures can be conducted by generalists, other procedures may require specialized inspections (e.g., to assess the robustness of the IT infrastructure, test cyber-security defenses, etc.). Supervisors who do not have in-house expertise may hire external auditors, when permitted by law (BCBS 2016a, p. 14 [EC 11]). In addition, SupTech tools can help supervisors partly overcome capacity constraints, for instance, to analyze large transaction datasets.

5.3.3 Examination procedures

5.3.3.1 RISK GOVERNANCE

Every EMI must have a formal framework for managing operational risk, including IT risk. A risk management framework needs to be customized to the EMI business. And there must be clear lines of governance and responsibilities—enshrined in formal agreements—between an EMI and its parent company.[39]

Many EMIs in our research are owned by MNOs and "use" the risk management framework (and key infrastructure) of their parent company, even though an MNOs' risk management focuses on the risks of the telecommunication business, not on the e-money business.

Like banks, large EMIs should formalize three lines of defense: (i) business line or management controls, (ii) risk management and compliance functions, and (iii) independent internal and external auditors. Small EMIs can apply the same concept to a less formal structure, but the internal auditor must always be independent from business

[38] See Annex 4 for more guidance. Important issues related to reliability of payment services, including finality of payments and completion of transactions in the event of loss of communication or other problem, are not specifically addressed in this paper.

[39] It is good practice for EMIs to hire risk management staff that have experience in financial services. In at least one country in our research, MNOs can be authorized as EMIs (instead of being required to create a subsidiary). This can expose the EMI to MNO risks and vice-versa, delay the adoption of good risk management practices, and pose constraints to supervisory examinations.

units, risk management, and compliance, and it must report directly to the board. Most EMI regulations require EMIs of all sizes to hire external auditors. Risk committees at the board level should be required for large EMIs (alternatively, risk oversight could be done by an audit committee), while the board of small EMIs should have at least one member familiar with risk management.

5.3.3.2 OVERARCHING OPERATIONAL RISK MANAGEMENT FRAMEWORK

Supervisors can assess the existence, quality, and implementation of a framework for operational risk. The framework should identify all sources of operational risk, such as IT failures, frauds, data security breaches, service disruptions, theft, and others. It should be approved by the board and be commensurate with the EMI's size and complexity. In general, a good framework does the following:

- Defines the risk governance structure.
- Outlines a repeating cycle of risk management activities (i.e., routine processes and systems used to identify, measure, monitor, report, and mitigate risks).
- Covers three dimensions: (i) avoiding risks, (ii) dealing with risk materialization, and (iii) avoiding recurrence by improving the risk management and controls processes.
- Establishes procedures and systems to estimate and monitor losses.
- Sets the EMI's risk appetite and countermeasures when higher risk is tolerated (e.g., capital buffer, insurance).[40]
- Establishes an independent internal audit function that reports directly to the board.
- Provides frameworks for hiring, monitoring, and exiting from third-party agreements, such as outsourcing and partnerships, and for initial and periodic due diligence of third parties.
- Is subject to regular reviews.

The examination starts with the offsite analysis of relevant documentation, which includes policies and procedures manuals, risk reports, internal and external auditor's reports, and reports of incidents (e.g., frauds, disruptions).[41] Onsite verification, which can include observation, interviews and system tests, are based on offsite analyses. The core of onsite work is to probe whether the risk management framework is effectively implemented and to follow up on findings from the offsite preparation. For instance, the

[40] This is important for EMIs in a fast growth phase because the quality of operational controls and risk management may drop during this time.
[41] The supervisor should try to assess the internal auditor's independence. If the auditor's independence is compromised, the reports will have little value. The external auditor's reports can also provide relevant information.

supervisor may look into whether internal controls are embedded in the EMI's day-to-day activities and whether the IT systems provide a good tool for identifying, monitoring, and reporting risk, including data on estimated and incurred losses (e.g., reversals to customers because of unauthorized transactions, payment of insurance deductibles when claiming coverage, loss of equipment because of a power outage, etc.).[42]

Supervisors may review how the operational risk reports they receive are generated and whether the data in these reports match the information in the EMI's risk management IT system (i.e., whether it is accurate and complete). If discrepancies are found, the supervisor can require internal operational risk management reports instead of the standard report template.

5.3.3.3 FRAUD PREVENTION AND MANAGEMENT

Several different fraud types can affect EMIs.[43] The EMI needs to catalog these and include them in the operational risk management framework and in its fraud detection software. Informal, incomplete, or lax fraud management at EMIs (e.g., no investigation of fraud cases) should raise supervisory concerns.

The risk of fraud such as unauthorized access to customer funds by EMI staff is a major concern among EMDE authorities interviewed. Internal fraud is particularly worthy of attention—most of the fraud cases in newspaper headlines in the EMDEs studied were perpetrated by staff, sometimes in collusion with agents.

Supervisors can do the following:[44]

- Check (offsite) that there are adequate policies and procedures to avoid, identify, and respond to frauds; that fraud typologies are identified; and that responsibilities are clear.
- Assess how effectively the EMI internally communicates its policy for identifying and penalizing internal and agent fraudsters.
- Review the history of fraud cases (offsite) over a long timeframe to identify the types of frauds, growth of fraud rates, areas affected, and losses incurred. This review will have to assess adherence to the EMI's policies, the effectiveness of fraud risk management, and the impact of the losses on the EMI's financial health. Compare results with that of other EMIs.

[42] Although targeted at complex, large banks, BCBS's (2013) "Principles for Effective Risk Data Aggregation and Risk Reporting" provides guidance that could be customized for less complex institutions such as EMIs.
[43] See fraud typologies in Buku and Mazer (2017).
[44] Given the high incidence of frauds in some types of e-money transactions (e.g., mobile money in Sub-Saharan Africa), supervisors may want to do a thematic review of fraud prevention and management.

- Equire why frauds happened and what was done to avoid recurrence. Pay special attention to re-occurrences.
- If analytical capacity or software are available, request and audit (offsite) granular datasets to probe the information provided by the EMI with respect to frauds, such as to identify unusual patterns in transaction behavior (e.g., concentration of large withdrawals in a short time frame and geographic location).[45]
- Probe information provided by the EMI on its history of red flags from the fraud detection system and about the parameters used to issue flags.
- Check access rights to the e-money account system and enquire which staff can delete and alter data, transfer funds, etc. Ask about the controls to limit access to the platform and protect customers' login details and about exceptions to the rules. Use enquiries and system tests to assess whether staff are able to manually create/destruct e-money.
- Analyze audit trails to, for instance, search for unusual or attempted unauthorized logs by staff and agents (e.g., nighttime activity by staff) and simulate unauthorized actions.
- Ask about the frequency of updates to the fraud detection system and patch management (acquiring, testing, installing, and keeping track of code changes).
- Assess how settlement accounts (temporary or suspense accounts) are managed. Poor reconciliation can be an opening for fraudsters.[46]

5.3.3.4 DATA SECURITY (INCLUDING CYBER-SECURITY)

Data security is important for risk management in EMIs given their reliance on digital data, widely spread agent networks, and increasing connectivity with third parties. EMIs of any size need effective data security strategies formalized in a **data security program**. A good data security program does the following:[47]

- Is approved by and is the responsibility of the EMI board.
- Appoints an executive (e.g., information security officer) to be responsible.
- Is based on risk assessment(s) conducted by the EMI or external experts.

[45] Despite the potential benefits of conducting audits of large sets of granular data to assess how an EMI manages and reports its operational risk, including the risk of fraud, most EMDE supervisors interviewed did not have the expertise and analytical software required.
[46] An example of this is a high-profile fraud case in mobile money in Uganda related to the unauthorized transfer of funds to/from these accounts. See Morawczynski (2015).
[47] Data security and data privacy are related, but they are different areas of supervisory review. This section does not address data privacy (e.g., whether the EMI seeks customer consent before sharing data for marketing purposes).

- Identifies and classifies data according to their sensitivity.
- Covers all facilities and systems used to access, collect, store, use, transfer, secure, and dispose of data.
- Classifies risks to data security into internal and external, and identifies their sources, likelihood, and impact.
- Covers administrative, technical, and physical safeguards to ensure security, confidentiality, and integrity of data to (i) avoid risk (**prevention**), (ii) identify risk (**detection**), and (iii) respond to risk materialization (**treatment**). See Box 4 for examples of safeguards.
- Frames the ongoing and periodic evaluation of the program's effectiveness and consequent improvement.

Depending on the EMI and the expertise available, an examination can mix document review, interviews, observation, and system tests. It may do the following:[48]

- Gather evidence that the security program is protecting the EMI against risks and will continue to do so given the EMI's business and growth strategy.
- Analyze and further enquire about the results of risk assessments.
- Analyze auditors' reports and implementation of their recommendations.
- Analyze data security in outsourcing agreements, including cloud computing, transaction processing, API development, and others.[49]
- Analyze risk data (e.g., reported data security breaches, hacks, virus injections, etc.).
- Assess the physical security of sensitive facilities (e.g., data storage/processing).
- Test key controls, including by doing a vulnerability scan, penetration tests, audit trail analysis, etc.

An EMI's security program is only as strong as its weakest link. For instance, many EMIs in Africa and Asia use Unstructured Supplementary Service Data (USSD), which is considered a low-security channel for carrying customer data. Also, EMIs often rely on personal identification numbers (PINs) to authenticate customers, but many customers disclose their PINs to EMI agents. Although many countries use USSD and agents to facilitate financial inclusion, supervisors should assess how EMIs reduce the related data se-

[48] See Annex 4 for additional resources.
[49] All EMDE supervisors interviewed were concerned about the outsourcing of cloud computing by EMIs, particularly across borders, because this could make accessing data and data storage facilities for supervisory purposes difficult. For example, India has recently issued a directive that requires payment system providers to store all data related to their operations exclusively in India, thus effectively prohibiting them from using cross-border cloud computing (see Baur-Yazbeck [2018]).

Box 4. Examples of EMI data security measures

As part of its data security program, an EMI may do the following:

- Implement a dual control system and segregate duties.
- Do background checks of and provide specialized training to critical staff.
- Immediately revoke access rights of departing employees.
- Maintain an inventory of technology resources (e.g., physical devices, network connections).
- Do periodic system updates and manage code changes (patch management).
- Use up-to-date monitoring tools to detect frauds and intrusions.
- Have a cyber-security program that provides a framework for risk identification, protections, detection, response and recovery, testing, and reporting. The security measure should include (i) encryption of data in transit and in storage (CGAP 2018), (ii) firewalls and virus controls, and (iii) vulnerability scans and penetration tests.
- Participate in information sharing groups and take measures for continuous learning.
- Control access to systems and critical facilities, do resilience testing on manual controls, and have physical security.
- Have measures to protect against and react to destruction, loss, or damage of data from hazards such as fire and floods.
- Have a framework for data security in outsourcing and partner arrangements.

curity risks (e.g., through biometric authentication, one-time password tokens, anomaly detection, or gradual shift away from USSD).

5.3.3.5 BUSINESS CONTINUITY

Business continuity management is important for operational risk management and should be well developed in large EMIs.[50] Business continuity arrangements should enable the EMI to rapidly resume critical operations and restore key IT infrastructure in the event of both minor and severe disruptions (e.g., disruption in telecommunications, power outages, natural disasters). Business continuity management enables companies to respond to and reduce the impact of crises.

[50] See Annex 4 for more guidance.

Supervisors should assess the EMI's business continuity plan to ensure the following:

- The plan identifies crisis scenarios and analyzes their potential impact.[51]
- There are contingency and recovery strategies that identify critical facilities, people, processes, IT systems, data, and alternative data-processing capabilities.
- Staff are adequately trained (including through simulations) to execute the plan.
- The plan is periodically tested and reviewed (supervisors can analyze the tests results).
- The EMI's critical systems undergo stress tests.
- Policies, manual and automated controls, and risk-sharing arrangements with third parties are in place and ensure transactions are eventually finalized, even if communication is disrupted before completion or in case of third-party failure (e.g., payment initiation services).[52]

The EMDEs in the study reported that failures of telecommunications and electricity infrastructure, which led to operational disruptions in EMI services, were common. These types of third-party dependencies generate risk. There seems to be little investment in contingency arrangements and little supervisory pressure for improvement. Other reported disruptions are due to unexpected or even planned interruptions of the EMI's systems. The African countries researched had cases of major disruptions because of upgrades in the e-money platform. One case was the approximately 12-hour disruption of M-PESA in Kenya because of a system upgrade in 2017 (Capital Business 2017).

The supervisor may coordinate with the telco regulator to access data or analytics that could provide a broader picture of telco service disruptions. These could be compared with EMI disruptions to determine how to improve contingency arrangements. Many EMIs in EMDEs depend on a single MNO and usually do not seek redundancy with other MNOs, which further exposes them to operational disruptions.

As part of the offsite examination, the supervisor can analyze data on frequency, location, and duration of disruptions; failed or incomplete transactions; and system downtime and their reasons (and remedies) and follow up on previous commitments of improvement. Supervisors with expertise may request and audit granular transaction datasets and system logs to identify unusual patterns that could mean failure in contingency arrangements and to spot disruptions that were not reported to the supervisor.

[51] Conducting a comprehensive business impact analysis and risk assessment to base the design of contingency strategy is good practice.
[52] Many payment system laws and regulations have relevant requirements covering these situations, but there is limited enforcement within EMDEs in this research, which leaves customers vulnerable.

5.4 AML/CFT

5.4.1 Key regulatory requirements

EMIs are often covered by AML/CFT laws and, therefore, are responsible for sending suspicious transaction reports to the financial intelligence unit and putting in place systems and controls to reduce the risk of ML/FT. EMI regulations focus on imposing balance and transaction limits to client and agent e-money accounts, such as limits to monthly balances, individual transaction value or volume of total monthly transactions, and at times, restrictions on the number of accounts each customer can have. If EMIs comply with these regulations, ML/FT risk could be reduced considerably. In addition, regulation requires EMIs to conduct customer due diligence (CDD) by verifying the identity of their customers and agents (including collection and storage of account opening information transaction data), and to monitor transactions to identify deviations from expected behavior according to customer and agent profiles.

Most EMDE supervisors interviewed for this research do not conduct specialized supervisory procedures (offsite or onsite) to assess how well EMIs manage ML/FT risks. A few, however, have established specialist teams dedicated to AML/CFT assessments. Industry practice suggests that ML/FT transaction monitoring and CDD are not always adequate. In Africa, for example, there are instances of customers self-registering for several e-money accounts with the same EMI and across EMIs and evading transaction limits, thus exposing flaws in risk management systems and controls.

5.4.2 Scope of examinations

Transaction and balance limits work only if account-opening procedures comply with the rules and if transaction monitoring is effective. Otherwise, clients can have several accounts, collude with agents and other clients, and evade the limits for criminal purposes. Controls must be embedded (encoded) in the EMI's systems, and effective monitoring requires specialized software. An AML/CFT examination should cover at least the following:

1. Compliance with regulatory limits
2. Account opening procedures (customer and agent)
3. Product, customer, and agent profiling
4. Transaction monitoring

5.4.3 Examination procedures

As in other areas, supervisors can analyze (offsite) the EMI's written policies and procedures manuals describing the EMI's internal controls, risk management policy, staff responsibilities and IT systems related to AML/CFT.[53] At a minimum, the policies and procedures manuals should be aligned with the applicable regulation; however, it is better to provide much greater detail. The examination can focus on:

- Whether the written rules are observed in practice and whether there is significant room for breaching them.
- How effective communication is throughout the organization regarding AML/CFT obligations and controls and changes to them.
- Whether there are reasonable ML typologies incorporated into the risk management program.
- How the detection, confirmation, and reporting of suspicious transaction is done, and how the EMI acts on them.
- Whether (and why) a lot of suspicious transactions have been detected by the system or operational level staff/agent but have not been reported to the financial intelligence unit.
- Offsite analysis of internal and external audit reports and follow up onsite.

As with operational risk, supervisors can conduct automated or manual analyses of granular transaction data and reported events, such as account opening records, to identify suspicious situations and exceptions to the regulations and EMI policies. These data may be accessed onsite or collected before onsite procedures.[54]

5.4.3.1 COMPLIANCE WITH REGULATORY LIMITS

Supervisors can do the following:

- Analyze (offsite) related policies and procedures to comply with limits, assess their level of implementation (offsite and onsite), and evaluate the exceptions.
- Assess the effectiveness of the automated controls embedded in the systems to identify and treat and report suspicious transactions.

[53] However, several EMIs in the EMDEs researched do not have specialized AML/CFT units, staff, and software. Rather, they use the AML/CFT program of their parent company. Given the differences between e-money and MNO services, AML/CFT controls need to be fully customized to EMIs.

[54] A few of the EMDE supervisors interviewed have access to highly granular EMI transaction data but do not conduct sophisticated analyses (such as by using modern analytical software) to identify operational and ML/FT risks.

- Run system tests to simulate prohibited transactions.
- Ask about and require demonstration of automated controls and the criteria for alerts or flags.
- Analyze the log of limit breaches or attempted breaches, and enquire what caused these and what was done to solve them.
- Analyze granular datasets across time to probe the information provided by the EMI and check consistency of compliance with the regulatory limits.
- Check whether there is any control that attempts to identify clients with multiple accounts within an EMI and across different EMIs.
- Make further enquiries into the types of accounts that raise concern (e.g., self-registered accounts, accounts that have been repeatedly flagged).
- Request information on the employees who have permission to alter the limits or other system rules and ask whether alterations have been made in the past and how they are proposed and approved.

5.4.3.2 ACCOUNT OPENING PROCEDURES

To check whether account opening procedures comply with EMI policies and regulation, supervisors can do the following:

- Ask operational staff and agents about account opening (including remote) procedures (e.g., describe each step and rule), whether exceptions exist, whether they find it difficult to follow the procedures (e.g., examining IDs), and whether customers have been able to open several accounts.
- If granular transaction data are available, check whether there is a concentration of account opening volumes in certain periods/geographies or branches/agents and request and analyze documentation of a sample of accounts if there are any suspicions.
- Observe agents and/or staff opening accounts of actual customers.
- Conduct mystery shopping.[55]
- Assess risk management when using biometrics or other e-KYC/CDD procedures.
- Review procedures to identify and monitor politically exposed persons and the use of sanctions lists.
- Ask about and seek proof of repeated agent training covering all agent staff who conduct e-money transactions, through documentation and by interviewing agents.

[55] For guidance on mystery shopping, see Mazer et al. (2015).

5.4.3.3 PRODUCT, CUSTOMER, AND AGENT PROFILING

Supervisors may check and assess how EMIs define customer and agent profiles (e.g., retail customer, small agents, large agents, master agents, etc.), location (e.g., large urban center, border area, rural village, etc.), and other characteristics (e.g., income, date of account creation) whose combination may lead to different levels of ML/FT risk and respective expected transaction patterns. In most EMDEs researched, the regulation imposes account and transaction limits on all EMI customers and products, but EMIs may have lower limits for riskier customers (e.g., customers living in border areas) or products (e.g., remittances). Agents may have greater flexibility for limits because they require bigger transactions to serve end customers. It is important to understand how EMIs define client and agent profiles, because it is the foundation for identifying potentially risky behavior through transaction monitoring.

5.4.3.4 TRANSACTION MONITORING

EMIs may use specialized software to monitor transactions and compare suspicious behavior against expected behavior. While the sophistication of such systems should be commensurate with an EMI's size and complexity, all EMIs should have a fully automated system. The system should be able to identify attempts to transact above permitted limits, transactions not in line with the preset profiles, and other suspicious situations, such as high volume of transactions to/from few accounts, transaction surges, geographic concentration, multiple transactions by same customer, etc.

Fraud and AML/CFT risk identification systems are becoming more sophisticated and innovative. Some use complex machine-learning analysis of numerous factors and data in real time to identify suspicious behavior, which could, for instance, identify potential multiplicity of accounts being used by the same person using fake identification information or using relatives and friends. Such systems may automatically block certain accounts and trigger alerts to staff.

The quality of transaction monitoring depends on the quality and variety of the data used for the analytical software. An expensive and sophisticated system that uses machine learning will be as weak as any other system if the data are bad. The supervisor may ask about the data sources used and their quality to assess how well the monitoring system identifies and how quickly it reports risk, staff performance in reporting and treating situations flagged by the system, and whether confirmed risky situations have been reported to the supervisor.

Some EMDE supervisors want to collect highly granular transaction data to monitor ML/FT risk in real time, akin to what some of today's financial institutions do when using sophisticated monitoring systems. Although this is possible, the cost-benefit of doing so is not clear in all cases. Supervisors can collect granular data during an examination and conduct the desired analyses. Moreover, real-time monitoring by supervisors should never be a substitute for the EMI's obligation to do its own real-time monitoring. FSI (2018) and Dias (2018) describe a few examples of using highly granular data and sophisticated analytical software for AML/CFT monitoring by supervisors.

6. Conclusion

E-money issuers play a key role in advancing financial inclusion in many EMDEs. And supervisors are responsible for keeping e-money markets safe, through proportional supervision that balances priorities and focuses on the most significant risks. While a risk-based approach is a stepping stone for effective EMI supervision, SupTech can be used to alleviate the burden of labor-intensive supervisory tasks and improve in-depth analyses.

EMI supervision is simpler than bank supervision, because EMIs have, by regulation, a much more limited scope of activities. Hence, they usually pose limited risks compared to banks. In addition, typical EMI regulations impose fund-safeguarding requirements to back all funds owed to EMI customers with safe and liquid assets. If fund safeguarding is effectively implemented by EMIs, the risks of clients losing their money are curtailed significantly. Therefore, fund safeguarding is a central concern of EMI supervision.

There is no single recipe for the scope and depth of EMI supervision that would fit all countries. Supervisors need a risk-based approach that fits their context and focuses their assessments on the most important EMIs and their most important risks. In large EMIs, most supervisors will want to cover an array of risks, including operational risk, ML/FT risk, and consumer protection risk, in greater depth than they would in small EMIs. A good risk-based methodology depends on good data, starting with ongoing market monitoring that allows comparisons across EMIs and prepares supervisors for examinations of individual EMIs. The guidance given in this paper, particularly the detailed examination procedures, should be used wisely according to the specific risk-based approach to EMIs taken by each supervisor. Not all procedures will be applicable to all EMIs, and some EMIs may need more than what is described in this paper. Moreover, this paper does not cover important aspects such as corrective powers/measures and resolution of EMIs.

Finally, while there is no single model for where EMI supervision should be located within a financial supervisory authority, EMI supervisors must have experience with financial sector assessments and specific knowledge of EMI businesses.

Annex 1. Organizations interviewed

Country / region	Organizations
West Africa	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)
Austria	Oesterreichische National Bank
	Financial Markets Authority
Brazil	Banco Central do Brasil (BCB)
Colombia	Financial Superintendence
France	French Prudential Supervision and Resolution Authority (ACPR)
Ghana	Bank of Ghana
	MTN Mobile Money
	Airtel Money
	Tigo Cash
	Vodafone Ghana Mobile Financial Services
Hong Kong	Hong Kong Monetary Authority
India	India
Jordan	Jordan
Luxembourg	Luxembourg
Malaysia	Bank Negara Malaysia
Mexico	National Banking and Securities Commission (CBNV)
	National Pension System Commission (CONSAR)
Myanmar	Central Bank of Myanmar
	Wave Money
Nigeria	Central Bank of Nigeria
Pakistan	State Bank of Pakistan
Paraguay	Central Bank of Paraguay
Peru	Superintendence of Banks, Insurance and Pension Funds (SBS)
Philippines	Bangko Sentral ng Pilipinas (BSP)
Singapore	Monetary Authority of Singapore
Tanzania	Bank of Tanzania
	Tanzania Communications Regulatory Authority
	Tanzania Insurance Regulatory Authority
	Vodacom Tanzania
	Jumo
	Airtel Tanzania
Uganda	Bank of Uganda
United Kingdom	Financial Conduct Authority

Annex 2. References

Key References

Staschen, Stefan, and Patrick Meagher. 2018. "Basic Regulatory Enablers for Digital Financial Services." Focus Note 109. Washington, D.C.: CGAP. http://www.cgap.org/sites/default/files/Focus-Note-Basic-Regulatory-Enablers-for-DFS-May-2018.pdf

Dias, Denise, and Stefan Staschen. 2017. "Data Collection by Supervisors of DFS." Working Paper. Washington, D.C.: CGAP. http://www.cgap.org/sites/default/files/Working-Paper-Data-Collection-by-Supervisors-of-DFS-Dec-2017.pdf

———. 2015. "Supervision of Banks and Nonbanks Operating through Agents. Practice in Nine Countries and Insights for Supervisors." Working Paper. Washington, D.C.: CGAP. https://www.cgap.org/sites/default/files/Working-Paper-Supervision-of-Banks-and-Nonbanks-Operating-through-Agents-August-2015.pdf

Bibliography

Alliance for Financial Inclusion (AFI). 2014. "Supervision and Oversight of Mobile Financial Services." Guideline Note No. 12, February. http://www.afi-global.org/publications/1451/Guideline-Note-12-Mobile-Financial-Services-Supervision-and-Oversight-of-MFS

Almazán, Mireya, and Nicolas Vonthron. 2014. "Mobile Money Profitability: A Digital Ecosystem to Drive Healthy Margins." London: Mobile Money for the Unbanked, November. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/2014_Mobile-money-profitability-A-digital-ecosystem-to-drive-healthy-margins.pdf

APRA (Australian Prudential Regulatory Authority). 2015. "Outsourcing Involving Shared Computing Services (including Cloud)." Information Paper, July. https://www.apra.gov.au/sites/default/files/information-paper-outsourcing-involving-shared-computing-services.pdf

Bauguess, Scott W. 2018. "The Role of Machine Readability in an AO World." Key note address, Financial Information Management Conference, Boston, Mass., 3 May. https://www.sec.gov/news/speech/speech-bauguess-050318?utm_source=Master+List&utm_campaign=036e369e76-EMAIL_CAMPAIGN_2018_05_04&utm_medium=email&utm_term=0_da5920711b-036e369e76-183267633#_edn7

Buku, Mercy, and Rafe Mazer. 2017. "Fraud in Mobile Financial Services: Protecting Consumers, Providers and the System." Brief. Washington, D.C.: CGAP. http://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf

BCBS (Basel Committee on Banking Supervision). 2016a. "Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Basel: Bank of International Settlements, September. https://www.bis.org/bcbs/publ/d383.htm

———. 2016b. "Market Intelligence Gathering at Central Banks." Basel: Bank of International Settlements, December. https://www.bis.org/publ/mktc08.htm

———. 2013. "Principles for Effective Risk Data Aggregation and Risk Reporting." Basel: Bank of International Settlements, January. http://www.bis.org/publ/bcbs239.pdf

———. 2011. "Principles for Sound Management of Operational Risk." Basel: Bank of International Settlements, June. https://www.bis.org/publ/bcbs195.htm

———. 1998. "Risk Management for Electronic Banking and Electronic Money Activities." Basel: Bank of International Settlements, March, pp. 18–20. https://www.bis.org/publ/bcbsc215.pdf

Broeders, Dirk, and Jermy Prenio. 2018. "Innovative Technology in Financial Supervision (Suptech)—The Experience of Early Users." FSI Insights on policy implementation, No. 9. Geneva: Financial Stability Board. https://www.bis.org/fsi/publ/insights9.pdf

CPMI (Committee on Payments and Market Infrastructure). 2016. "Payment Aspects of Financial Inclusion." Basel: Bank of International Settlements, April. https://www.bis.org/cpmi/publ/d144.htm

———. 2014a. "Non-Banks in Retail Payments." Basel: Bank of International Settlements, September. https://www.bis.org/cpmi/publ/d118.pdf

———. 2014b. "Recovery of Financial Market Infrastructures." Basel: Bank of International Settlements, October. https://www.bis.org/cpmi/publ/d121.pdf

———. 2012. "Principles for Financial Market Infrastructures." Basel: Bank of International Settlements, April. https://www.bis.org/cpmi/publ/d101.htm

———. 2001. "Core Principles for Systemically Important Payment Systems." Basel: Bank of International Settlements, January. https://www.bis.org/cpmi/publ/d43.htm

———. 2000. "Clearing and Settlement Arrangements for Retail Payments in Selected Countries." Basel: Bank of International Settlements, September. https://www.bis.org/cpmi/publ/d40.pdf

Dias, Denise. 2018. "SupTech: Leveraging Technology for Better Supervision." Toronto: Toronto Centre, July. http://res.torontocentre.org/guidedocs/SupTech%20-%20Leveraging%20Technology%20for%20Better%20Supervision.pdf

ENISA (European Agency for Network and Information Security). 2009. "Cloud Computing Risk Assessment," November. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

FSB (Financial Stability Board). 2018. "Stocktake of Remittance Service Providers' Access to Banking Services." Geneva: FSB, March. https://www.g20.org/sites/default/files/documentos_producidos/stocktake_of_remittance_service_providers_access_to_banking_services_fsb_march_2018_2.pdf

———. 2014. "Key Attributes of Effective Resolution Regimes for Financial Institutions." Geneva: FSB, October. http://www.fsb.org/what-we-do/policy-development/effective-resolution-regimes-and-policies/key-attributes-of-effective-resolution-regimes-for-financial-institutions.

Greenacre, Jonathan, and Ross P. Buckley. 2014. "Using Trusts to Protect Mobile Money Customers." *Journal of Legal Studies*, 59–78.

G7. 2016. "G7 Fundamental Elements of Cybersecurity for the Financial Sector." https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Izaguirre, Juan Carlos, Timothy Lyman, Claire Mcguire, and Dave Grace. 2016. "Deposit Insurance and Digital Financial Inclusion." Brief. Washington, D.C.: CGAP. https://www.cgap.org/sites/default/files/Brief_Deposit_Insurance_and_Digital_Financial_Inclusion.pdf

Kemp, Katharine, and Ross P. Buckley. 2017. "Resolution Powers over E-Money Providers." UNSW Law Research Paper No. 49, December. http://classic.austlii.edu.au/au/journals/UNSWLRS/2017/49.html

Piechocki, M., and T. Dabringhausen. 2015. "Reforming Regulatory Reporting: From Templates to Cubes." The Irving Fischer Committee on Central Bank Statistics, "Combining Micro and Macro Financial Statistical Data for Financial Stability Analysis: Experiences, Opportunities and Challenges." Warsaw: BearingPoint, 14–15 December. http://www.bis.org/ifc/publ/ifcb41o.pdf

World Bank Group. 2018. "Financial Sector's Cybersecurity: Regulations and Supervision." Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

Wright, Paul. 2018. "Risk-Based Supervision." Toronto: Toronto Centre, March. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision.pdf

Annex 3. Reference Materials for Supervisors

Supervisory Guidance, Manuals, and Other

Association of Banks of Singapore. "Cloud Computing Implementation Guideline 1.1 for the Financial Industry in Singapore." Singapore: Association of Banks of Singapore, August. https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf

Central Bank of Ireland. 2016. "Cross Industry Guidance in Respect of Information Technology and Cybersecurity Risks." Dublin: Central Bank of Ireland. https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2

CPMI (Committee on Payments and Market Infrastructure). 2017. "Methodology of the Statistics on Payments and Financial Market Infrastructures in the CPMI Countries." Red Book Statistics. Geneva: Bank of International Settlements. https://www.bis.org/cpmi/publ/d168.htm

Dias, Denise. 2013. "Implementing Consumer Protection in Emerging Markets and Developing Economies. A Technical Guide for Bank Supervisors." Washington, D.C.: CGAP. http://www.cgap.org/sites/default/files/Technical-Guide-Implementing-Consumer-Protection-August-2013.pdf

ECB (European Central Bank). 2018. "Tiber-EU Framework. How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming." Frankfurt: ECB, May. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

HKMA (Hong Kong Monetary Authority). 2016. "Guideline on Supervision of Stored Value Facility Licensees." Hong Kong: HKMA. http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf.shtml

FFIEC (Federal Financial Institutions Examination Council). "Annex A. Examination Procedures" in *IT Examination Handbook, Retail Payments Systems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-a-examination-procedures.aspx

FFIEC (Federal Financial Institutions Examination Council). "Appendix E: Mobile Financial Services on e-mobile Services," in *IT Examination Handbook, Retail Payments Systems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx

———. "Business Continuity Planning" in *IT Examination Handbook, Retail Payments Systems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/operational-risk/business-continuity-planning.aspx

———. "Principles of the Business Continuity Testing Program" in *IT Examination Handbook, Business Continuity Planning*. https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program.aspx

U.S. Federal Reserve Board System, Board of Governors. "Interagency Guidelines Establishing Information Security Standards." https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

———. "Interagency Guidelines Establishing Information Security Standards." https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

FDIC (U.S. Federal Deposit Insurance Corporation). 2016. "Information Technology Risk Examination (InTREx) Information Technology Profile." IT risk examination template, July. https://www.fdic.gov/news/news/financial/2016/fil16043a.pdf

———. 2015. "Internal Routine and Controls" in *Security Safety Manual RMS Manual of Examination Policies*, March. https://www.fdic.gov/regulations/safety/manual/section4-2.pdf

Other guidance

CGAP. 2018. "Cybersecurity for Mobile Financial Services: FAQs for Regulators, Supervisory Authorities and Digital Financial Services Providers." http://www.cgap.org/events/cybersecurity-mobile-financial-services

CPMI (Committee on Payments and Market Infrastructure) and IOSCO (International Organization of Securities Commissions). 2016. "CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures." Basel: Bank of International Settlements. https://www.bis.org/cpmi/publ/d146.pdf

CPMI (Committee on Payments and Market Infrastructure). 2014. "Principles for Financial Market Infrastructures: Assessment Methodology for Oversight Expectations Applicable to Critical Service Providers." Basel: Bank of International Settlements, December. https://www.bis.org/cpmi/publ/d123.pdf

EBA (European Banking Authority). 2017. "Guidance for the Use of Cloud Service Providers." Frankfurt: EBA, December. https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions

FCA (Financial Conduct Authority). 2006. "Mystery Shopping Guide." London: FCA, November. https://www.fca.org.uk/publication/archive/fsa-mystery-shopping-guide.pdf

IFC (International Finance Corporate) and Mastercard Foundation. 2016. "Digital Financial Services and Risk Management Handbook." Washington, D.C.: IFC, pp. 28–39, 48–53, 68–86, 93, 95–108. https://www.ifc.org/wps/wcm/connect/06c7896a-47e1-40af-8213-af7f2672e68b/Digital+Financial+Services+and+Risk+Management+Handbook.pdf?MOD=AJPERES

Kerse, Mehmet, and Stefan Staschen. 2018. "Safeguarding Rules for Customer Funds Held by EMIs." Technical Note. Washington, D.C.: CGAP.

Mazer, Rafe, Xavier Gine, and Cristina Martinez. 2015. "Mystery Shopping for Financial Services." Washington, D.C.: CGAP. http://www.cgap.org/publications/mystery-shopping-financial-services

SEC (Securities and Exchange Commission). 2017. "Observations from Cybersecurity Examinations." *National Exam Program Risk Alert,* Volume VI, Issue 5, 7 August. https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

USAID (U.S. Agency for International Development) and Kenya School of Monetary Studies. 2010. "Mobile Financial Services Risk Matrix." Washington, D.C.: USAID and Kenya School of Monetary Studies, pp. 30–39. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf

Examples of thematic reviews

UK's Financial Conduct Authority

Mobile Phone Insurance: https://www.fca.org.uk/publication/thematic-reviews/mobile-phone-findings.pdf

Treatment of Consumers Who Suffer Unauthorized Transactions: https://www.fca.org.uk/publication/thematic-reviews/tr15-10.pdf