

The background of the cover features a close-up of a person's hands holding a smartphone. The phone screen displays a "Recents" call log with a numeric keypad at the bottom. Below the phone, several financial documents, including a check and a receipt, are visible. The documents contain various numbers, dates, and text, such as "06/2022" and "TOTAL". The overall scene is dimly lit, with the phone's screen and the documents providing the primary light source.

DIGITAL FINANCIAL SERVICES FOR FINANCIAL INCLUSION: TOOLS FOR SUPERVISORS

ACKNOWLEDGMENTS

The authors would like to thank the following CGAP colleagues: Gerhard Coetzee for overseeing this effort and Peter Zetterli for peer review. We also thank World Bank colleagues Sérgio José de Mesquita Gomes, Danilo Queiroz Palermo, Gynedi Srinivas, and Yaewon Yoon for peer review. We thank the financial supervisory authorities from El Salvador, Ghana, Jordan, Myanmar, and Pakistan for working with us and sharing their experience. And we thank the Toronto Centre and Digital Frontiers Institute for early feedback on the content of this guide, as part of the development of the Digital Financial Inclusion Supervision training program.

Consultative Group to Assist the Poor

1818 H Street, NW, MSN F3K-306

Washington, DC 20433

Internet: www.cgap.org

Email: cgap@worldbank.org

Telephone: +1 202 473 9594

Cover photo by Arete/Mamadou Diop/World Bank.

© CGAP/World Bank, 2023.

RIGHTS AND PERMISSIONS

This work is available under the Creative Commons Attribution 4.0 International Public License (<https://creativecommons.org/licenses/by/4.0/>). Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

Attribution—Cite the work as follows: Attribution: Dias, Denise, Juan Carlos Izaguirre, Mehmet Kerse, and Stefan Staschen. 2023. “Digital Financial Services for Financial Inclusion: Tools for Supervisors.” Washington, D.C.: CGAP. <https://www.cgap.org/research/publication/digital-financial-services-for-financial-inclusion-tools-for-supervisors>

Translations—If you create a translation of this work, add the following disclaimer along with the attribution: This translation was not created by CGAP/World Bank and should not be considered an official translation. CGAP/World Bank shall not be liable for any content or error in this translation.

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: This is an adaptation of an original work by CGAP/World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by CGAP/World Bank.

All queries on rights and licenses should be addressed to CGAP Publications, 1818 H Street, NW, MSN F3K-306, Washington, DC 20433 USA; e-mail: cgap@worldbank.org.

CONTENTS

| | |
|--|-----------|
| CHAPTER 1: Introduction | 1 |
| CHAPTER 2: Approach of this Technical Guide | 3 |
| CHAPTER 3: Designing the DFS supervisory framework | 5 |
| 3.1: Creating a risk-based approach to supervision | 5 |
| 3.1.1: Step 1. Map supervisory objectives and risks to policy goals | 6 |
| 3.1.2: Step 2. Identify impact indicators and classify DFS providers | 8 |
| 3.1.3: Step 3. Develop a risk assessment methodology | 8 |
| 3.2: Defining an organizational structure | 10 |
| 3.2.1: National institutional setup | 12 |
| 3.2.2: Internal organization for DFS supervision | 12 |
| CHAPTER 4: Implementing the DFS supervisory framework | 17 |
| 4.1: Conducting an initial risk assessment | 17 |
| 4.2: Developing the supervision plan | 18 |
| 4.3: Using a mix of supervisory tools | 20 |
| 4.4: Ensuring effective licensing | 20 |
| 4.4.1: Building a strong licensing framework | 20 |
| 4.4.2: Establishing clear and efficient licensing procedures | 22 |
| 4.4.3: Increasing proportionality and flexibility of licensing | 23 |
| 4.5: Optimizing offsite supervision | 24 |
| 4.5.1: Types of offsite activities | 25 |
| 4.5.2: Improving the effectiveness of ongoing offsite monitoring | 26 |
| 4.6: Improving supervisory data | 27 |
| 4.6.1: Step 1. Identify data quality shortcomings | 27 |
| 4.6.2: Step 2. Assess quality of data collection mechanisms | 28 |
| 4.6.3: Step 3. Assess the level of data granularity | 28 |
| 4.6.4: Step 4. Improve data collection | 30 |
| 4.6.5: Step 5. Improve data analytics | 31 |
| 4.7: Optimizing inspections | 33 |
| 4.7.1: Step 1. Prepare as much as possible offsite | 34 |
| 4.7.2: Step 2. Collect sufficient information prior to inspection | 34 |
| 4.7.3: Step 3. Develop tailored questions for inspection meetings and interviews | 34 |
| 4.7.4: Step 4. Produce inspection documents based on internal guidance | 35 |
| 4.7.5: Step 5. Corrective measures, enforcement, and follow-up | 35 |

| | |
|---|-----------|
| 4.8: Resolution of DFS providers | 36 |
| 4.8.1: Resolving DFS providers | 36 |
| 4.8.2: Deposit insurance applied to e-money | 38 |
| 4.9: Improving coordination and collaboration | 39 |
| CHAPTER 5: Overcoming implementation challenges | 41 |
| 5.1: Structural challenges | 41 |
| 5.2: Internal challenges | 42 |
| 5.2.1: Ramping up supervisory capacity | 43 |
| CHAPTER 6: Addressing emerging issues in DFS supervision | 45 |
| 6.1: Cloud computing | 45 |
| 6.1.1: Why does it matter? | 45 |
| 6.1.2: Supervisory implications | 45 |
| 6.2: Modularization | 48 |
| 6.2.1: Why does it matter? | 48 |
| 6.2.2: Supervisory implications | 49 |
| 6.3: Open finance | 50 |
| 6.3.1: Why does it matter? | 50 |
| 6.3.2: Supervisory implications | 50 |
| 6.4: The use of artificial intelligence and machine learning | 52 |
| 6.4.1: Why does it matter? | 52 |
| 6.4.2: Supervisory implications | 52 |
| Glossary | 56 |
| References | 60 |
| Additional Reading | 66 |

| | |
|---|----|
| FIGURES | |
| FIGURE 1: Initial steps to set the foundation for risk-based supervision | 6 |
| FIGURE 2: Example of goals and objectives mapping for payment services | 7 |
| FIGURE 3: Generic risk matrix for risk-based supervision | 9 |
| FIGURE 4: The supervisory cycle: from design to feedback | 18 |
| FIGURE 5: Types of supervisory activities | 19 |
| FIGURE 6: Core principles for effective banking supervision relevant to licensing and authorizations | 21 |
| FIGURE 7: Components of a strong licensing framework | 21 |
| FIGURE 8: Increasing flexibility of licensing procedures | 24 |
| FIGURE 9: Five steps to make DFS supervision more data-driven | 27 |
| FIGURE 10: The U.K.'s priorities for data reform | 32 |
| FIGURE 11: Common challenges faced by supervisors in EMDEs | 41 |
| FIGURE 12: Supervisory capacity depends on adequate budget | 43 |
| FIGURE 13: Unweighted average API availability of account providers' open banking APIs (September 2020–September 2022) | 51 |
| FIGURE 14: Successful API calls made by third parties using account providers' open banking APIs (September 2020–September 2022) | 51 |
| TABLES | |
| TABLE 1: Functions, activities, expertise, and skills for DFS supervision | 15 |
| TABLE 2: Sample questions to avoid and to ask during inspections | 35 |
| BOXES | |
| BOX 1: Example of prioritization based on impact and net risk | 11 |
| BOX 2: The national institutional setup for DFS supervision | 13 |
| BOX 3: Examples of internal organization for DFS supervision | 14 |
| BOX 4: Types of offsite supervisory activities | 25 |
| BOX 5: Reforming the EBA's reporting system | 29 |
| BOX 6: Example of reporting an aggregated indicator | 30 |
| BOX 7: Using technology to improve data collection mechanisms | 31 |
| BOX 8: Reforming data collection in the U.K. | 32 |
| BOX 9: Examples of supotech initiatives | 33 |
| BOX 10: The case of Wirecard | 37 |
| BOX 11: The FCA and insolvency in EMIs | 38 |
| BOX 12: Performance indicators of open banking in the U.K. | 51 |
| BOX 13: Examples of rules and principles for the responsible use of AI | 53 |
| BOX 14: ECB oversight of the use of third-party AI providers | 54 |
| BOX 15: Requirements for the algorithmic decision-making process in the United States | 54 |

ADDITIONAL EXAMPLES AND GUIDANCE

- 1: Supervisory objectives and risks mapped to policy goals
- 2: Examples of impact indicators
- 3: A risk assessment methodology for EMIs
- 4: A simplified annual supervision plan
- 5: Analyzing an EMI's licensing application
- 6: Financial analyses of EMIs
- 7: Data collection template for EMIs
- 8: Reporting guidance for EMIs
- 9: Anonymized data collection plan for EMIs

CHAPTER 1

INTRODUCTION

REGULATORS IN EMERGING MARKETS and developing economies (EMDEs) have made substantial progress toward putting in place the basic regulatory enablers for inclusive digital financial services (DFS).¹ While a positive development, enabling regulation is not enough. Effective supervision is needed to ensure that regulations are adequately applied. Without it, regulated nonbanks providing DFS (referred to as “DFS providers” throughout) may take excessive risks or adopt practices that could jeopardize financial inclusion, consumer protection, competition, integrity, and stability. Two aspects of effective DFS supervision take center stage:

- **Proportionality.** Supervision and regulation must be scaled in line with the DFS provider’s business model, size, complexity, and risk profile—all of which determine the impact DFS providers have on the policy goals pursued. Lack of proportionality could impose excessive compliance costs that impact the provider’s ability to cater to underserved populations. It could also leave risks unchecked. Proportionality demands that supervisors have a solid knowledge of DFS business models, along with their benefits and risks. It should be applied in all phases—from regulation and licensing to supervision and enforcement.²

- **Risk-based supervision.** Risk-based supervision (RBS) is closely related to proportionality. It requires using a methodology that systematically assesses risks and allocates supervisory resources. Financial supervisors worldwide broadly acknowledge that the risk-based supervisory approach helps them to achieve proportionality and effectiveness. Supervisory procedures and intensity should be adapted to the risks posed by DFS providers following systematic assessment of risks and the application of a balanced mix of supervisory tools. The risk-based approach helps authorities in EMDEs to optimize the use of scarce resources and overcome some of the challenges they face in supervising a burgeoning DFS market.

Creating an effective supervisory framework is a complex task that takes effort and time. However, supervisors in EMDEs often face competing priorities and challenges to implementation and may lack the experience, time, or resources to make significant improvements in their supervisory approach (Newbury and Izaguirre 2019). Building on CGAP’s work in several jurisdictions, our extensive previous research, and our work with partner development organizations, we created this Technical Guide to provide practical guidance and set strong

1 The basic regulatory enablers are discussed in Staschen and Meagher (2018) and further developed in Kerse and Staschen (2018), Dias and Staschen (2019), Dias and Kerse (2021), and Izaguirre et al. (2019).

2 For more on the application of proportionality to supervision, see BCBS (2016 and 2019). Additionally, Borio et al. (2022) advocates for the principle of “same business, same risks, same rules,” where regulation and supervision are not only focused on institutions and regulated institutional types, but similarly apply to institutions of different types that perform similar functions. Market conduct supervision is an example of such a “functional approach” to regulation and supervision, covering all types of regulated entities that offer similar services.

foundations for DFS supervision.³ It also offers a range of additional examples and guidance, such as step-by-step guides and data templates. The guide is divided into four chapters:

- A. Designing the DFS supervisory framework.** This chapter guides supervisors on how to design an effective DFS supervisory framework.
- B. Implementing the DFS supervisory framework.** This chapter offers guidance on implementing the supervisory framework, from licensing and offsite supervision to onsite inspections and resolution for DFS providers. It also discusses how to improve intra- and inter-agency coordination.
- C. Overcoming implementation challenges.** This chapter offers basic guidance on how to overcome the challenges commonly faced by EMDE supervisors aiming to implement effective DFS supervision, including challenges with data quality.
- D. Addressing emerging issues in DFS supervision.** This chapter offers an outlook on relevant emerging developments in DFS and their potential supervisory implications.

Key references are cited throughout the paper and links to additional examples and guidance are embedded in each chapter. The full list of additional examples and guidance can be found in the table of contents.

³ CGAP recently supported the work of supervisors conducting supervision of some DFS providers in several jurisdictions, including El Salvador, Ghana, Jordan, Myanmar, and Pakistan.

CHAPTER 2

APPROACH OF THIS TECHNICAL GUIDE

THIS TECHNICAL GUIDE AIMS TO help supervisors in EMDEs design and implement effective supervision of DFS and DFS providers. Its general approach is as follows:

- DFS includes a range of financial services delivered through digital channels, such as payments, credit, savings, insurance, and remittances. While most of the guide can apply to any type of service, some sections focus on specific types of DFS, such as electronic money (e-money).
- Providers offering DFS in EMDEs include banks and nonbanks. While most of this document's guidance could apply to supervision of banks providing DFS, the focus is on nonbank DFS providers for three reasons. First, a well-established body of international guidance and standards for prudential bank supervision already exists.⁴ Second, we take into consideration the fact that in most EMDEs, bank and nonbank supervision is separate (i.e., placed in different departments) and the main audience is the latter. Finally, the main driver for producing this guide is the emergence of innovative DFS providers in EMDEs—nonbank e-money issuers in particular. Such market development has rarely been matched by the development of a comprehensive RBS framework, let alone a framework that covers nonbanks offering innovative DFS to large numbers of customers.

The guide intends to help supervisors in EMDEs that face this particular scenario.

- As the guide focuses on nonbanks, it does not advocate for differentiation of bank and nonbank supervision. Since the definition of DFS is so broad and because banks can (and do) provide DFS, it is important to align the supervisory approaches applied when banks and nonbanks carry out similar activities—the “same business, same risks, same rules” approach advocated by Borio et al. (2022).
- Most of this document's guidance could apply to supervision of any service type, not just DFS. That is because the guidance focuses on a foundational element—the establishment of a risk-based supervisory framework—as a prerequisite for effectiveness. Such a foundation is necessary for every type of supervision, including supervision of DFS and their providers. The focus is justified because RBS is still underdeveloped in many EMDEs.
- Although most of the guidance generally applies to any DFS or DFS provider, some sections (e.g., [Additional examples and guidance 5: Analyzing an EMI's licensing application](#)) focus on e-money issuers given their prominent role in financial inclusion in EMDEs. The guide does not address specificities of all types of DFS. CGAP continues to explore supervisory issues in

⁴ Nonetheless, the supervisory approach to some innovations relevant to banks, those discussed in [Chapter 6](#) in particular, is still under development even in advanced economies. Further research and experience are required before guidance can be issued on such innovations.

innovations relevant to financial inclusion in order to identify the need to issue specific guidance.

- The guide does not advocate for special supervisory procedures to advance financial inclusion. Its focus is on establishing effective supervision of services and providers that are relevant to financial inclusion in EMDEs.⁵ Financial inclusion monitoring is not addressed as a supervisory concern. The assumption is that financial inclusion and other policy goals such as competition are supported by effective prudential and market conduct supervision.
- Although the guide emphasizes the importance of building a risk-based framework for DFS supervision, it is not a comprehensive manual. Extensive guidance is already available in the existing literature and international standards for setting up RBS (see the [References](#) and [Additional Reading](#) sections for lists of key sources).
- The guide intends to help supervisors as they work on a framework for DFS supervision in their country context. Each chapter cites references that can assist supervisors in improving their current framework. Moreover, links to additional examples and guidance throughout provide illustrations and further guidance. The additional examples and guidance are not intended as standalone pieces but are rather meant to be read in conjunction with the main guide.
- Due to the above considerations, the guide should be adapted to each context, including stage of RBS development, quality of supervisory data, availability of resources and skills, and types and number of DFS providers subject to supervision. Supervisors that have already fully implemented the risk-based approach may pick and choose guidance and resources from the guide's various sections, for example, if they intend to address a particular implementation challenge (e.g., data quality). Supervisors at the beginning of the journey to RBS implementation may find many parts helpful and supportive of their own planning and implementation strategies.

⁵ The approach was also adopted by BCBS (2016) when discussing the application of the Basel Core Principles for Effective Bank Supervision to institutions relevant to financial inclusion.

CHAPTER 3

DESIGNING THE DFS SUPERVISORY FRAMEWORK

T HIS CHAPTER PROVIDES GUIDANCE

on how to establish a solid foundation for DFS supervision. While supervision is shaped by existing legal frameworks and regulations, certain design issues need to be considered regardless of the regulations in place. Good planning is essential in all contexts, including deciding upon an organizational structure and which data collection mechanism will support a risk-based approach to supervision. This type of foundation allows supervisors to continuously adjust their supervisory practices to evolving DFS issues and respective regulatory responses.

Supervisors may find it useful to plan and make incremental improvements toward a stated vision of RBS rather than strive to establish a perfect supervisory framework from day one. RBS requires supervisors to develop a methodology to systematically assess the risk profile of individual DFS providers and identify system-wide risks. RBS allows them to tailor the intensity, frequency, and focus of supervisory activities in proportion to relative risks and to optimize the use of scarce supervisory resources.

This chapter contributes to the implementation of a risk-based approach to DFS supervision. Its guidance can be applied either partially or in total, depending on the supervisor's needs and capacity and the specific country context, including whether RBS is already conducted on

other regulated sectors by different departments or by the department currently in charge of DFS providers. The following areas are addressed:

- Creating a risk-based approach to supervision
- Defining an organizational structure

While designed for supervisors at the beginning of the journey to apply RBS to DFS providers, this chapter also contributes to the ongoing work of EMDE supervisors striving to improve an existing risk-based approach.

3.1 **Creating a risk-based approach to supervision**

Risk-based supervision is the key to supervisors achieving statutory policy goals, assuming that resources, capacity, and skills are limited. The RBS methodology allocates supervisory attention and time (i.e., intensity of supervisory activities and enforcement measures) according to a systematic evaluation and risk prioritization. The intent is to rationalize efforts to achieve greater effectiveness and efficiency. This makes it easier for supervisors to strike a balance among the policy objectives of financial inclusion, stability, integrity, competition, and consumer protection.⁶

⁶ See Tomilova and Valenzuela (2018) for a toolkit that focuses on how to identify and manage links among the following policy objectives: financial inclusion, stability, integrity, and consumer protection.

RBS requires supervisors to identify and measure the risks created by each provider’s DFS activities and to estimate the potential impact of such risks and the likelihood they will materialize.⁷ With an understanding of the relative importance of various providers (i.e., risk assessment at the market level) and the different risks within each provider (i.e., risk assessment at the provider level), supervisors can tailor the type, scope, and depth of their supervisory activities.

A first crucial question to ask is, “Which type of supervision is the risk-based approach being designed for?” The answer will determine the choice of policy goals, the supervisory objectives, and the risks involved. Two main types of supervision can be identified: prudential supervision and market conduct supervision. The former focuses on provider safety and soundness, the latter on provider business conduct, usually with the aim to protect consumers. In some countries (only a few of which are EMDEs),⁸ different authorities perform prudential and market conduct supervision. This institutional model is known as “twin peaks.” In many EMDEs the two types of supervision fall under the same authority, such as the central bank, even though they may be conducted by different departments (i.e., internal twin peaks). Regardless of institutional setup, both market conduct and prudential supervision require a risk-based approach. The broad concepts described in this chapter will be the same but the methodologies will differ in the details.⁹ In cases of a specialized department for market conduct supervision, this department should also cover DFS providers, and the department in charge of prudential supervision should not consider consumer protection in its risk-based methodology.

After defining which type of supervision will be conducted, supervisors can set the foundation for risk-based supervision by following the three initial steps detailed in [Figure 1](#) below.

The outputs of these steps are not static, especially since the DFS industry is quickly evolving. Over time, supervisors may refine their understanding of the relative importance of various risks and identify new ones. RBS is a dynamic, continuous, and adaptable cycle of planning, implementation, and feedback. Swift changes must be introduced when needed, including changes to the articulation of policy goals and supervisory objectives, the identification of indicators, and the risk assessment methodology itself. In the course of this adaptive process, the quality of data the supervisor collects and data analytics capabilities also play an important role.

3.1.1 STEP 1. MAP SUPERVISORY OBJECTIVES AND RISKS TO POLICY GOALS

Supervisors need to articulate their overarching policy goals and the specific objectives supervision will pursue under each. Policy goals vary in level of priority, and supervisory objectives need to be identified considering such variation. Supervisors should next identify the main risks DFS pose to achieving supervisory objectives. For example, national payments system (NPS) law could make the supervisor responsible for (i) ensuring trust in the NPS and (ii) ensuring NPS efficiency. Depending on how the supervisor prioritizes these goals, a set of supervisory objectives would be identified for each. To achieve trust, for instance, DFS supervision objectives could include ensuring safety and reliability. Several risks could be

FIGURE 1. Initial steps to set the foundation for risk-based supervision



7 See Wright (2018a and 2018b) for further guidance on how to implement risk-based supervision.

8 Examples include Mexico and South Africa but several other countries are currently considering adopting this institutional arrangement.

9 See Gomes et al. (2022) for a guide on how to implement risk-based market conduct supervision covering many types of providers, including DFS providers. See Chalwe-Mulenga et al. (2022) for a review of consumer protection risks posed by DFS.

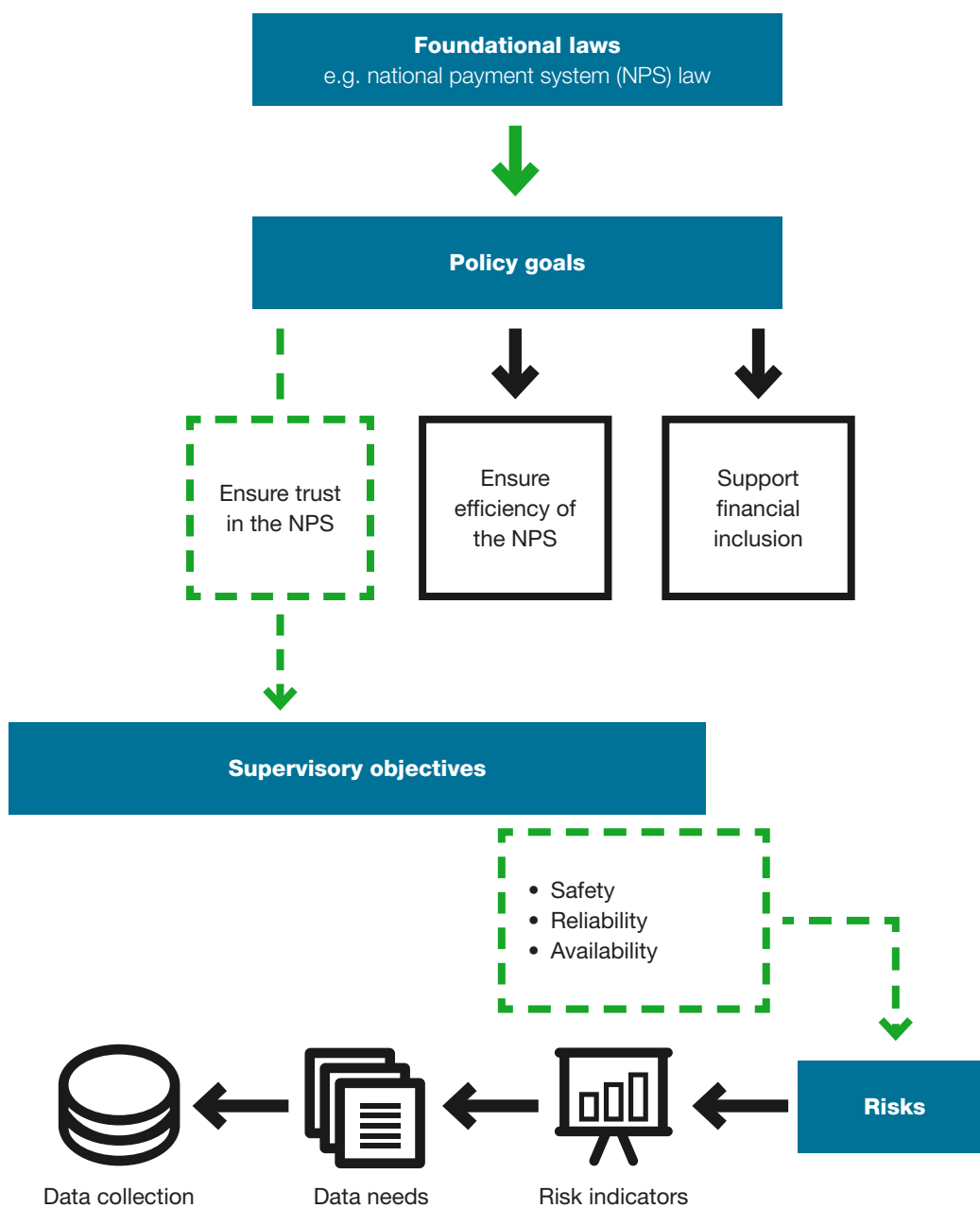
identified under each supervisory objective. [Figure 2](#) shows an example of mapping supervisory objectives and risks to policy goals.

Identified risks can be classified into two main types: (i) risks of the broader operating environment that affect all DFS providers and are usually beyond the supervisor’s and providers’ influence, such as high inflation or political turmoil (macro level, market, or systematic risks) and (ii) the micro level risks of each provider (idiosyncratic risk).

Additional examples and guidance

[1. Supervisory objectives and risks mapped to policy goals](#)

FIGURE 2. **Example of goals and objectives mapping for payment services**



3.1.2 STEP 2. IDENTIFY IMPACT INDICATORS AND CLASSIFY DFS PROVIDERS

Once supervisors have mapped supervisory objectives and risks to policy goals and before they develop their risk assessment methodology (Step 3), they are ready to start prioritizing.

When prioritizing risks to calibrate supervisory efforts, it is useful to examine risks at three levels: (i) the highest level, where risks determine the relative importance of different DFS activities across the market (e.g., e-money issuing, payments, digital lending); (ii) at the mid-level, where risks determine the relative importance of individual DFS providers involved in similar activities; and (iii) at the micro level, where different risks are of varying relative internal importance to each provider.

Once supervisors have reached an understanding of how much attention the different types of DFS activities deserve, the next step is to classify DFS providers according to their relative importance (risk) by estimating their potential impact on supervisory objectives.

Impact indicators estimate the potential harm that would result from the materialization of a provider's risks. With a list of impact indicators at hand, DFS providers can be ranked from highest to lowest impact. By nature, high-impact providers receive more supervisory attention. For example, the failure of a large DFS provider could impact trust in the entire DFS market. Provider size (measured, for instance, by number of customers) is a type of impact indicator. The identification of impact indicators is one of the first and most basic steps to start optimizing the use of supervisory resources.¹⁰

Additional examples and guidance

[2. Examples of impact indicators](#)



3.1.3 STEP 3. DEVELOP A RISK ASSESSMENT METHODOLOGY

RBS requires systematic risk assessment of individual DFS providers based on a standardized methodology. The methodology acts as a guide for supervisors to measure each provider's risk in order to prioritize supervisory efforts. In its written form, the methodology looks like a supervision manual, with instructions for analytical procedures.

At this stage, supervisors will have identified impact indicators (i.e., indicators of inherent risk). DFS providers undertaking similar activities will find a similar set of risks inherent to that activity. For instance, since virtually all DFS providers face cybersecurity risk, it is a risk that can be considered *inherent* to the DFS business. However, the actual level of cybersecurity risk varies according to each provider's risk management and mitigation practices. This actual level is known as net (residual) risk. The risk assessment methodology is the main guide to help supervisors estimate a provider's net risk. It could be, for instance, that a provider previously classified as high risk (because it has the largest customer base) is classified as low risk from a cybersecurity perspective because it has the best risk mitigation strategies among all providers.

The objective of conducting a risk assessment is to estimate the net risk of a particular DFS provider.¹¹ Risk assessment evaluates the internal controls, risk management, and governance measures the provider has put in place to mitigate the risks inherent to its business and the broader market risks that may exist. By comparing the net risk of different providers, supervisors can fine tune the provider prioritization that started with impact indicators analysis. Assessment also provides granular knowledge on how each provider deals with each risk so supervisors can prioritize each provider's most problematic areas of risk. This knowledge allows them to adapt the scope of subsequent assessments as it is not necessary to

10 The risk-based methodology combines measuring the impact risk materialization would have and the likelihood it will occur. Hence, it requires the use of likelihood indicators, in other words, indicators that show whether a risk has a higher or lower chance of materializing. While this Technical Guide focuses on impact indicators for the initial step mainly for simplicity's sake, it also recognizes that in practice, many supervisors in EMDEs mix impact and likelihood indicators in the initial phase. Complexity of products is an example of a likelihood indicator. Focusing on impact in this phase does not mean this Technical Guide proposes a risk-based methodology that ignores likelihood. The likelihood element becomes more apparent when supervisors undertake risk assessments of individual providers. For example, a provider with weaker governance and internal controls would be placed higher on the likelihood scale than a provider with strong risk mitigants.

11 Since only a fine line exists between inherent and net risk, risk assessments can also help supervisors adjust their initial estimation of inherent risk.



Additional examples and guidance

[3. A risk assessment methodology for EMIs](#)

carry out a comprehensive scope of risk assessment for all DFS providers each year.

The first step in designing a risk assessment methodology is to identify all relevant risks, also known as risk factors, risk components, or risk categories. For example, ineffective fund safeguarding would be a risk for a nonbank e-money issuer (EMI). In assessing nonbank digital credit providers, credit risk would be a major risk. The methodology used would explain how each risk is to be assessed and the specific indicators and risk mitigants the assessment would analyze. In the EMI example, effective reconciliation between total e-money issued and funds set aside in float (trust) accounts could be a mitigant for the fund safeguarding risk.

Estimating the net risk of a specific DFS provider requires supervisory resources, including staff time and human resources with the right expertise and skills. If conducting a full risk assessment of priority DFS providers is initially not possible, supervisors can scale down their workplan to undertake what is possible given available resources and data. If the initial assessment cannot cover some priority DFS providers, supervisors may consider including them in the next supervisory cycle based on the plan and available resources.

3.1.3.1 Risk matrix

The elements of a risk assessment methodology can be summarized in a risk matrix like the example shown in [Figure 3](#).

A risk matrix is a visual representation of each type of inherent risk for an individual DFS provider. Within the matrix, “area” can be a business line, a type of DFS product, or a combination of the two. It is often referred to as “significant activity.” Less complex DFS providers may not require different significant activities to be identified. Each type of risk inherent in each significant activity is assigned a degree of significance (i.e., a weight) that impacts the DFS provider’s total inherent risk. For example, in the case of an EMI, the e-money product carries the highest weight among all products (if the EMI offers others). Within the e-money product, the inherent risk of fund safeguarding could be assigned a higher weight than, for instance, liquidity risk. Assigning relative weights is not an exact science as the process is heavily

FIGURE 3. **Generic risk matrix for risk-based supervision**

| Areas/Activities | Level of significance | Inherent risks | | | | Control and management | | | Net risk | Risk direction |
|---|-----------------------|----------------------------------|---|------------------------------|---------------------|------------------------|-----------------|------------|----------|----------------|
| | | Risk 1 (e.g., fund safeguarding) | Risk 2 (e.g., credit risk—partnerships) | Risk 3 (e.g., cyber attacks) | Total inherent risk | Internal controls | Risk management | Governance | | |
| Area 1 (e.g., e-wallet) | High | | | | | | | | | |
| Area 2 (e.g., mobile insurance) | Low | | | | | | | | | |
| Area 3 (e.g., outsourcing arrangements) | Medium | | | | | | | | | |
| Area 4 | | | | | | | | | | |

influenced by supervisory judgment and experience. Weights can also be fine-tuned as experience grows with supervision of different types of DFS providers.

After evaluating the quality of a provider's internal controls, risk management process, and governance, the use of weights for risks and significant activities within the provider allows supervisors to calculate net risk: the sum of all weighted risks. Net risk is represented by a rate or score (i.e., a single number or letter, a short expression) chosen from a predetermined rating or scoring scale (e.g., risk levels 1–4, low to high).¹² With the rate at hand, supervisors can more easily and consistently compare providers. Supervisors should additionally make a judgment call on the expected direction of risk for the DFS provider (i.e., increase, maintain stability, reduce).

A risk assessment methodology and risk matrix can be developed for virtually any type of DFS provider. It applies the same ideas as the more well-known risk matrices for prudential banking supervision. However, the methodology and risk matrix for most DFS providers is much simpler than those used for banks. Since banks perform a broader range of activities, their inherent risk profile and assessment of their net risk is much more complex.

It is important to note that conducting risk assessments to determine the net risk of a DFS provider carries a cost for supervisors. Supervisors need to prioritize DFS providers for the purpose of conducting risk assessments (or not), according to previously identified impact indicators in line with existing supervisory capacity and human and financial resources. It is unlikely that all providers will ever be subject to a full risk assessment covering all risk areas.

3.1.3.2 Learning from peers

Supervisors may benefit from engaging with peers in other countries to learn more about how they developed their risk assessment methodology, including the risk matrix, and what they considered when assigning relative risk weights. Peer engagement may be helpful for jurisdictions at the beginning of the risk-based supervision journey. However, due caution must be exercised given the differences between countries. Some elements of

methodology and, specifically, the risk matrix, must fit each country's legal framework, market characteristics, availability and quality of data, institutional arrangements, and supervisory experience.¹³ There is no unique or best recipe for a risk matrix. For instance, the risk matrix for mobile lenders in one country could use customer vulnerability as a risk category—and at a high weight due to local circumstances. These parameters would not apply in all contexts or even be feasible if the supervisor lacked indicators of customer vulnerability.

Also, designing a risk matrix with weights assigned to different risks and risk mitigants may not currently be the highest priority for all supervisors. A risk matrix and its risk score are useful for systematizing the prioritization process and results of risk assessments, particularly with a large number of providers. For example, suppose a country's DFS market is in its infancy and only includes a few types of relatively simple DFS providers. The supervisor could begin the RBS journey by using impact indicators (see [section 3.1.2](#)) to prioritize DFS providers and develop a risk assessment methodology while leaving the matrix and rating system for later. These actions would already make supervision immensely more effective. The supervisor could have other more pressing needs than designing a matrix, such as improving the quality of data collected through regulatory reporting (see [section 4.6](#)).

3.2 Defining an organizational structure

Two components of an organizational structure for DFS supervision require clarity: (i) national institutional setup and (ii) the internal organizational arrangement of each authority involved. While there are no standard formulas for the organizational arrangement of DFS supervision, this section highlights important aspects to consider.

¹² A risk assessment methodology must describe, in sum, what each level or rate of the rating scale looks like in practice.

¹³ See Taylor et al. (2020) for a discussion on institutional arrangements for the regulation and supervision of certain types of DFS providers.

BOX 1. Example of prioritization based on impact and net risk

For those not fully versed in RBS, using a single risk score to compare and prioritize DFS providers after prioritizing them by impact indicators can be a confusing task. Which prioritization is more important? Does the risk score substitute for the impact indicators? What is the relationship between risk weights and impact indicators?

The following hypothetical example uses two DFS providers to clarify these questions. The table shows an impact indicator (number of accounts), the assessment of two risks (one with high weight in the risk-scoring methodology and one with low), and final risk score (net risk).

| | DFS Provider X | DFS Provider Z |
|---|--------------------|----------------------|
| Impact indicator (number of accounts) | 5 million accounts | 1.5 million accounts |
| Fund safeguarding risk (high risk weight) | Low | Medium-high |
| Credit risk (low risk weight) | Medium | Low |
| Risk score (net risk) | Low (stable) | High (upwards) |

Which DFS provider should the supervisor prioritize? The short answer is Provider X because the potential impact of its risks is higher. It will, therefore, always be a higher priority provider. A provider with a much lower impact indicator may not even be subject to a full risk assessment.

Assuming a risk assessment was conducted on Provider Z, findings could include that Provider Z has poorer internal controls, risk management, or governance; is scored at a higher risk level (with an upward trend) than Provider X; and that particular concern exists in the important area of risk (fund

safeguarding). Still, Provider Z is much smaller than Provider X. The supervisor’s decision on what to include in the supervision plan for the next year will depend on specific circumstances, such as staff availability. However, by using the impact indicator and assessing risks in the two providers, the supervisor is able to make a few decisions to optimize staff time. For instance, she may decide to include in the annual supervision plan:

- Remote follow up on Provider X’s credit risk issue
- Ongoing remote monitoring of a set of key indicators for both providers (e.g., transaction levels, account numbers, total e-money issued, etc.)
- A special onsite inspection to follow up on improvements to Provider Z’s fund safeguarding practices, as agreed upon in the time-bound action plan the provider delivered

This example shows that the RBS methodology is not a zero sum game. It is not about “this or that” provider. It is a method to identify priority activities to be performed based on the knowledge of the risks of different providers. Designing a risk assessment methodology, including assigning relative levels of importance to different risks (risk weights) and identifying level of importance of their risk mitigants (e.g., internal controls), helps supervisors calibrate the scope and type of supervisory activities to perform. They may otherwise be tempted to plan full scope inspections (assessments) that cover all risk areas every year—at least on large providers.

A key takeaway from this example is what the supervisor’s annual plan does *not* include. She will not repeat a full risk assessment on both providers. That is one of the most important contributions of the RBS methodology: there is no need to perform a full scope risk assessment on all providers, let alone every year.

3.2.1 NATIONAL INSTITUTIONAL SETUP

National institutional setup for DFS supervision varies by the existing capacity and resources across different authorities, their respective legal mandate and experience with financial supervision, the structure of the country's financial sector and its foundational legislation, and the types of DFS providers operating in the market.

On principle, a DFS provider should be regulated and supervised by a financial supervisory authority rather than an authority that covers another economic sector (BCBS 2016). In most countries, DFS supervision is conducted by the central bank, an independent financial supervisory authority such as the financial superintendencies in Latin America, or both.

The main responsibility for supervising DFS providers—with respect to their financial soundness and safety—should lie with financial authorities, even in the case where a provider is involved in economic activities other than financial services provision. For example, when mobile network operators (MNOs) are allowed to issue e-money, the telecommunications authority regulates the core activity (telecommunications services). However, since their e-money operations are in the realm of financial sector regulation, most often payments regulation, a financial sector authority needs to supervise that part of the business.¹⁴ The same applies to DFS activities in platform-based finance.¹⁵

Another consideration in the institutional setup for DFS supervision is the growing fragmentation of the financial services value chain, also known as modularization.¹⁶ DFS providers increasingly adopt models that rely on a range of third parties through outsourcing arrangements and/or partnerships. Modularization, especially in digital banking,¹⁷ is becoming central to innovative DFS and raises difficult questions for the national institutional setup for financial supervision. For instance, the majority of innovative DFS providers use cloud computing

infrastructure provided by third parties—usually the same ones that provide cloud services to the banking sector. Large cloud computing providers could become pivotal players in DFS and even in the traditional financial sector by providing critical services to multiple supervised entities. Should they also be regulated and supervised?¹⁸ Many DFS providers also partner with banks in banking-as-a-service (BaaS) arrangements¹⁹ and, in this way, offer banking services to end users without having a banking license. Such models also give rise to competition, concentration, and market conduct risks, which may involve different authorities in some countries.

Finally, it is possible for countries to go through transition periods where they adopt temporary institutional arrangements for DFS supervision. One authority may assume initial responsibility for supervision of some types of DFS providers then later shift responsibility to another authority. A certain type of provider may be unregulated and unsupervised for a period of time while a legal reform is finalized. To reduce regulatory uncertainty, however, transition periods for institutional arrangements should be limited and the intended final arrangement clearly communicated to the industry. In any case, as DFS providers adopt business, governance, or shareholding models that blur the lines between different economic sectors and the traditional divisions within the financial sector, DFS supervision increasingly requires interagency coordination (see [section 4.9](#)).

3.2.2 INTERNAL ORGANIZATION FOR DFS SUPERVISION

The internal organization for DFS supervision—that is, how a supervisory authority internally organizes its DFS supervision—varies widely across countries. The decision about how to organize the different functions and activities involved in DFS supervision (see [section 3.2.2.1](#)) depends on various factors, such as adoption by the supervisory authority of a matrix organizational

14 The DFS business of such nonfinancial entities should ideally be under a separate legal entity, as preconized by BCBS (2016).

15 For a discussion of regulatory issues in platform-based finance, see Staschen and Meagher (2022).

16 See Zetterli (2021) for a discussion on modularization.

17 See Jenik and Zetterli (2020) for a discussion on digital banking.

18 [Chapter 6](#) discusses this and other evolving regulatory and supervisory issues.

19 In such an arrangement, the nonbank offers banking services to the public by using the bank's platform and accounting; all banking operations remain in the bank's books. See [section 6.2](#).

BOX 2. The national institutional setup for DFS supervision

In **Kenya**, subject to prior authorization by the Central Bank of Kenya, nonfinancial companies such as MNOs are allowed to conduct e-money business without having to establish a separate legal entity to act as EMI. They only need to have a separate business unit with separate management and accounting. Kenya's major EMIs include MNOs such as Safaricom, which are regulated and supervised in relation to their core activity by the Communications Authority of Kenya. MNO e-money activities are regulated and supervised by the Central Bank of Kenya, which is the payments regulator.

WeChat Pay is one of the largest EMIs in **Malaysia**. It is owned by the big tech firm, Tencent. Similarly, Razer Pay and GPay, owned respectively by Razer (a gaming company) and Grab (a ride-hailing/food delivery company), have EMI licenses in Malaysia and the **Philippines**. In 2020, the consortium of Singtel (a telecommunications company) and Grab was awarded a digital bank license in **Singapore**. In

Myanmar, EMIs known as mobile FSPs are wholly owned by MNOs, large retailers, or technology companies. In each case the country's central bank supervises DFS providers (e.g., EMIs), regardless of their holding company.

In **Mexico**, EMIs known as electronic payment funds institutions (IFPE) are regulated and supervised by both the National Banking and Securities Commission (CNBV) and the central bank (Banco de México). Banco de México conducts payments oversight while CNBV conducts prudential supervision. Separately, consumer protection issues are under the responsibility of Condusef, the financial consumer protection agency. In **Peru**, EMIs known as e-money issuing companies (EEDÉ) are also regulated and supervised by both the central bank (Banco Central de Reserva del Perú) and the Superintendency of Banking, Insurance, and Pensions (SBS).

structure where specialized teams are dedicated to certain core or support functions that work across the whole organization (Asana 2021) and cover DFS providers. Cross-support units may include teams specialized in certain risks or topics, such as operational and IT risks (e.g., Malaysia, Mexico, Philippines), anti-money laundering and combating the financing of terrorism (AML/CFT), market conduct and consumer protection, and cybersecurity (e.g., Monetary Authority of Singapore).

The core function of DFS supervision (i.e., implementing risk-based supervision) can be configured in many ways. For example, the payments department may be responsible for overseeing the NPS and supervising individual payment services providers (PSPs), including a range of DFS providers. Alternatively, a DFS provider may be prudentially supervised by a specialized team within the financial supervision department (e.g., EMIs are supervised by a specialist team of the prudential supervision department of the Hong Kong Monetary Authority). Other departments, such as payments, market conduct, and financial integrity, may also supervise the

same EMI from their particular perspective and using their own prioritization methodology. Some authorities have created units with a broader mandate to cover all types of fintech developments, including innovation facilities, monitoring of new developments, licensing of new fintechs, institution-focused supervision, and publication of statistics. This is the case in Ghana, which is discussed in [Box 3](#).

Some authorities in EMDEs (e.g., Ethiopia, India, Malaysia, Nigeria, Pakistan) have departments dedicated to promoting specific segments of the financial sector. For example, one task handled by the Reserve Bank of India's Financial Inclusion and Development Department is to make credit available to productive sectors of the economy, including rural and micro, small, and medium enterprise (MSME) sectors. An objective of the State Bank of Pakistan's Digital Innovation and Settlements Department provides another example: to ensure digital payments market development. As a rule, in order to avoid conflicts of interest and optimize the use of specialized and scarce supervisory skills, the

BOX 3. Examples of internal organization for DFS supervision

The **Central Bank of Jordan's** Oversight and Supervision on National Payment System Department has two separate teams to internally organize DFS supervision: one responsible for NPS oversight and one for prudential supervision of payment providers. In **Mexico, CNBV** conducts institution-focused prudential supervision. Its specialized unit is responsible for supervising both payment networks (e.g., ATMs, POS networks) and PSPs, including EMLs and other DFS providers. These providers are also subject to specialized supervision by the operational risk supervision department. The **Monetary Authority of Singapore (MAS)** is the sole regulatory and supervisory authority for Singapore's entire financial sector, including all DFS providers. It is also the central bank. While MAS's bank supervision department handles EML supervision, its payments department conducts oversight of the whole NPS, including e-money.

In 2020, the **Bank of Ghana** created the Fintech and Innovation Office for the purpose of supervising DFS providers, including EMLs, and all types of

fintech companies that may fall under the 2019 Payment Systems and Services Act. The office took over DFS supervisory activities that were previously the responsibility of the Payment Systems Department. That department currently oversees market infrastructure, such as the Real-time Gross Settlement (RTGS) System and payment services provided by banks. It also approves DFS products offered by fintechs.

At **Bangladesh Bank**, several departments (e.g., banking supervision, offsite surveillance) are involved in the supervision of mobile financial services. A similar case can be observed in Brazil, where some institutions are regulated by the **Central Bank of Brazil**. There, DFS providers focused on retail payment services are typically covered by four departments: the Credit Unions and Nonbanks Supervision Department, the NPS Oversight Department, the Conduct Supervision Department, and the Department of Competition and Financial Market Structure. Licensing is conducted by yet another centralized licensing department.

responsibility for promotion and development should remain separate from supervisory responsibilities.

Finally, temporary arrangements could be made for the internal organization of DFS supervision. In its initial stages, for instance, a team inside a preexisting department (e.g., banking supervision) may become responsible for prudential DFS supervision (see [section 3.2.2.1](#)). The arrangement may persist until a team with adequate skills and expertise is formed, a unit head appointed, and the organizational chart adjusted. In any case, it is important that DFS supervision (both prudential and market conduct) receives the required level of attention and resources necessary according to the growing importance and sophistication of the country's DFS markets.

3.2.2.1 Key functions and activities of DFS supervision

Clarifying the functions, activities, expertise, and skills that DFS supervision requires is a key step in defining the best internal organization. A range of core and support tasks work to keep the risk profile of individual supervised DFS providers in check (institution-focused activities) and monitor the risks of the DFS market as a whole (market-focused activities). [Table 1](#) provides a possible set of functions for DFS supervision and its related skills and expertise. These functions are usually not all performed by a single department. Multiple departments, teams in the same department, or even different authorities may take on different functions.²⁰ The variations are even greater with support functions such as training and planning.

20 See AFI (2020) for a case study that illustrates how several Bangladesh Bank departments are involved in supervising digital financial services.

TABLE 1. **Functions, activities, expertise, and skills for DFS supervision**

| Core functions and activities | | Expertise | Skills |
|--|---|---|---|
| Market-focused activities | Market monitoring (including thematic reviews) | <ul style="list-style-type: none"> • DFS business models, products, and services | <ul style="list-style-type: none"> • Data analytics • Research and writing |
| Institution-focused activities | Remote/onsite inspections <ul style="list-style-type: none"> • Strategy and governance • Financial risk (e.g., fund safeguarding, liquidity, credit, settlement) • Conduct risk • Operational and IT risk (IT infrastructure, business continuity, operational resilience, data security, cyber security, third-party management, other operational risks) | <ul style="list-style-type: none"> • Financial analysis • Supervision tools and techniques • Risk-based supervision • Financial market functioning and structure • Competition in financial markets • Relevant DFS laws and regulations • Consumer protection laws and regulations • AML/CFT laws and regulations | <ul style="list-style-type: none"> • Auditing • Interview • Communication and persuasion |
| Support functions and activities | | Expertise | Skills |
| Supervisory capacity building | Supervisory planning | <ul style="list-style-type: none"> • Supervision tools and techniques • Risk-based supervision | <ul style="list-style-type: none"> • Management and leadership • Communication |
| | Training | <ul style="list-style-type: none"> • Capacity building and training | <ul style="list-style-type: none"> • Organizational and logistics • Planning and resource management • Negotiation |
| Supervisory policy and guidance development | Internal guidance development | <ul style="list-style-type: none"> • DFS regulation and business models | |
| | Guidance to DFS providers and policy statements | <ul style="list-style-type: none"> • Supervision tools and techniques • Risk-based supervision | <ul style="list-style-type: none"> • Research and writing • Legal and regulatory drafting • Communication and persuasion |
| | Regulatory change proposals | <ul style="list-style-type: none"> • Relevant DFS laws and regulations • DFS products and services • DFS business models | <ul style="list-style-type: none"> • Stakeholder management |
| Regulatory reporting | Submissions management | <ul style="list-style-type: none"> • Regulatory reporting requirements | <ul style="list-style-type: none"> • Data engineering |
| | Data validation | <ul style="list-style-type: none"> • Data science | <ul style="list-style-type: none"> • Data analytics • Organizational |

3.2.2.2 Payments oversight or payments supervision?

The terms “oversight” and “supervision” may cause confusion among supervisors when defining an internal organization and determining related functions and responsibilities. The two terms may also get mixed up in reference to PSP supervision.

Exclusively for the purpose of this guide, we define the terms as follows:²¹

- **Payments system oversight.** Payments system oversight focuses on the stability, safety, security, and reliability of a country’s NPS. It includes activities such as round-the-clock monitoring of large value payments systems (e.g., real-time gross

²¹ These definitions are not aligned with the definitions used in all countries. In some countries, for instance, the definition of oversight covers prudential supervision (e.g., India) or even market conduct supervision (e.g., Georgia) of PSPs.

settlement [RTGS]), licensing, and inspections and risk assessments of financial market infrastructure (FMI).²² The Principles for Financial Market Infrastructures issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) provide guidance for addressing risks and efficiency in FMI. The Principles also outline the general responsibilities of central banks, market regulators, and other relevant FMI authorities in implementing these principles.²³

- **Payments supervision.** Payments supervision focuses on the viability, safety, and business conduct of individual PSPs. It is similar in function to bank/ other nonbank supervision and uses a mix of offsite and onsite supervisory techniques. In cases where the supervisory authority has a consumer protection mandate, the goal could be both prudential and market conduct. The skills and expertise needed to conduct institution-focused supervision are slightly different from those needed to conduct NPS oversight, although overlap may exist—especially regarding the inspections NPS oversight may require in financial market infrastructure. The supervisory function usually deals with a much greater number of entities compared to FMI oversight. It therefore needs to rationalize the use of supervisory resources by adopting a risk-based approach.

Separating the functions discussed above has become more common practice.²⁴ The recent entry of a large variety and number of DFS providers in the retail payments market is one of the reasons for separation. This phenomenon has at times pushed supervision to create a specialized supervision team inside the same department (e.g., Jordan) or to shift the supervisory function to another department (e.g., Brazil). In some countries (e.g., Colombia, Mexico, Peru), different authorities perform NPS oversight and retail payments supervision. When these functions are separate, coordination and collaboration are required.

22 CPMI (2005) defines oversight with a focus on payments systems.

23 Most central banks in EMDEs also operate FMI, such as the RTGS system and clearinghouses. To avoid conflicts of interest, different departments should be responsible for operational and supervisory functions. See CPMI and IOSCO (2012).

24 See Delort and Garcia Luna (2022) for a discussion on the impact of payments innovations on the central bank as NPS overseer, PSPs supervisor, and payments systems operator.

CHAPTER 4

IMPLEMENTING THE DFS SUPERVISORY FRAMEWORK

ONCE THE FOUNDATION FOR DFS supervision has been established, it can be operationalized. Effective implementation of RBS involves conducting an ongoing range of supervisory activities based on careful periodic (annual) planning. This chapter provides guidance related to some important implementing aspects. With the exception of sections [4.1](#) and [4.2](#), it is not meant to be sequential. Some sections are more relevant to institution-focused DFS supervision than to market monitoring.²⁵ For instance, the discussion about licensing in [section 4.4](#) is institution-focused. Also, some guidance may not be specific to DFS supervision but more generally apply to efforts to improve risk-based supervision. Finally, the intent is not to provide an exhaustive step-by-step guide on how to conduct each type of activity. Instead, this chapter provides guidance and resources to help supervisors address some common implementation issues toward improved DFS supervision.

4.1 Conducting an initial risk assessment

[Section 3.1.3](#) highlighted the importance of developing a risk assessment methodology for DFS providers. The next step is to put that methodology into practice in an ongoing cycle of assessing risks, taking supervisory measures and following up on them, providing feedback

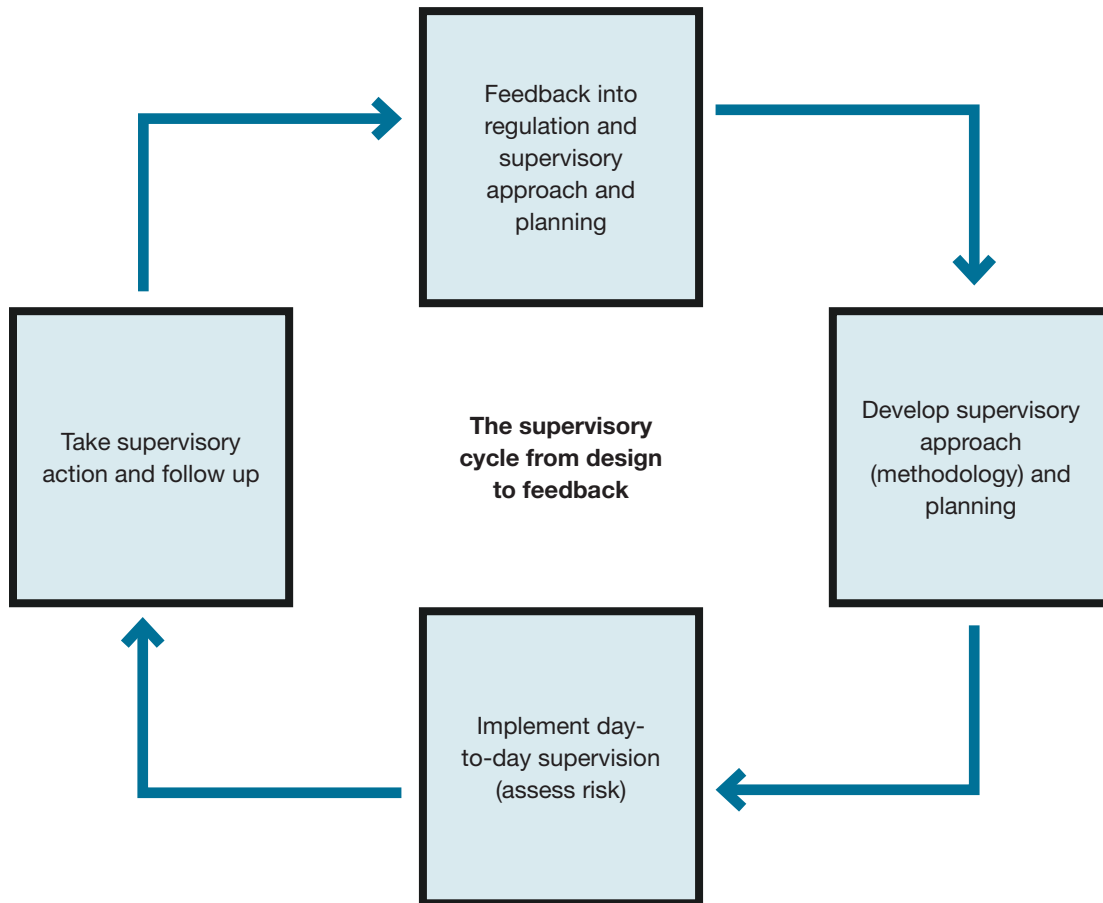
to adjust the supervisory approach and regulations, and planning for the next year. [Figure 4](#) illustrates the supervisory cycle.

If resources were infinite, all DFS providers would be subject to an initial risk assessment that covers the whole risk assessment methodology—every risk and analytical procedure described in the methodology. Supervisors would be able to repeat the full assessment every year or once per supervisory cycle: the period of strategic planning that covers the whole regulated market, which, in some countries, coincides with the calendar year. In reality, supervisory resources are almost always scarce. Careful implementation of risk-based supervision, including risk assessment methodology, means prioritizing which risks and DFS providers receive greater attention.

To begin, supervisors need to choose which providers will receive a full initial risk assessment. For priority providers at the beginning of the RBS journey, the assessment needs to be as comprehensive as possible. For other, lower priority providers, the supervisor needs to assess as many issues as possible based on prioritization of those identified in previously collected data. The objective is to set the widest possible assessment scope for selected providers (in terms of number of areas of the risk assessment methodology). In large markets, a good part of the market will be excluded from the initial assessment. Previously collected impact indicators are the main source

²⁵ Market monitoring tools—albeit with a focus on consumer protection—are discussed in depth in Izaguirre et al. (2022) and Gomes et al. (2022).

FIGURE 4. **The supervisory cycle: from design to feedback**



of information for identifying priority providers and issues for initial assessment (see [section 3.1.2](#)). For example, even basic indicators such as number of customers, number and value of outstanding digital loans, or number of total accounts may help supervisors decide which DFS providers and risk areas to include in the initial risk assessment. Additional sources of information can come from meetings with other departments to discuss risks in the DFS market.²⁶

4.2 Developing the supervision plan

The initial assessment is the basis for each DFS provider’s relative risk profile, which can periodically be updated through subsequent risk assessments (e.g., remote or onsite inspections, other types of supervisory activities). Supervisors need to document the initial assessment’s results and compile takeaways that inform the next planning period. The assessment should also be used to fine tune the assessment methodology itself, which may even trigger recommendations to improve regulations. Finally, the assessment becomes the basis for filling in the risk matrix of assessed DFS providers, including direction of risk.

Supervisors are rarely able to continuously assess, via inspections, all risks covered in an initial risk assessment.

Additional examples and guidance

[2. Examples of impact indicators](#)

[3. A risk assessment methodology for EMIs](#)



26 For more information on types of DFS risks, see Chalwe-Mulenga et al. (2022), USAID (2010), and IFC and the MasterCard Foundation (2016).

In fact, this inability is what requires risk-based supervision to focus on certain risk areas. The subsequent DFS supervision plans will include, for instance, targeted inspections on individual providers that cover only a few aspects of the risk assessment methodology. In many EMDEs where supervisors have already created a risk assessment methodology and a risk matrix (e.g., for prudential bank supervision), it is still common practice to conduct a full scope inspection that covers the whole methodology for the same institutions in every cycle—an extended effort that unnecessarily absorbs limited supervisory capacity. A better practice is to adjust the scope of inspections and other activities according to the information gathered throughout the supervisory cycle. Otherwise, supervisors cannot say they have indeed implemented risk-based supervision.

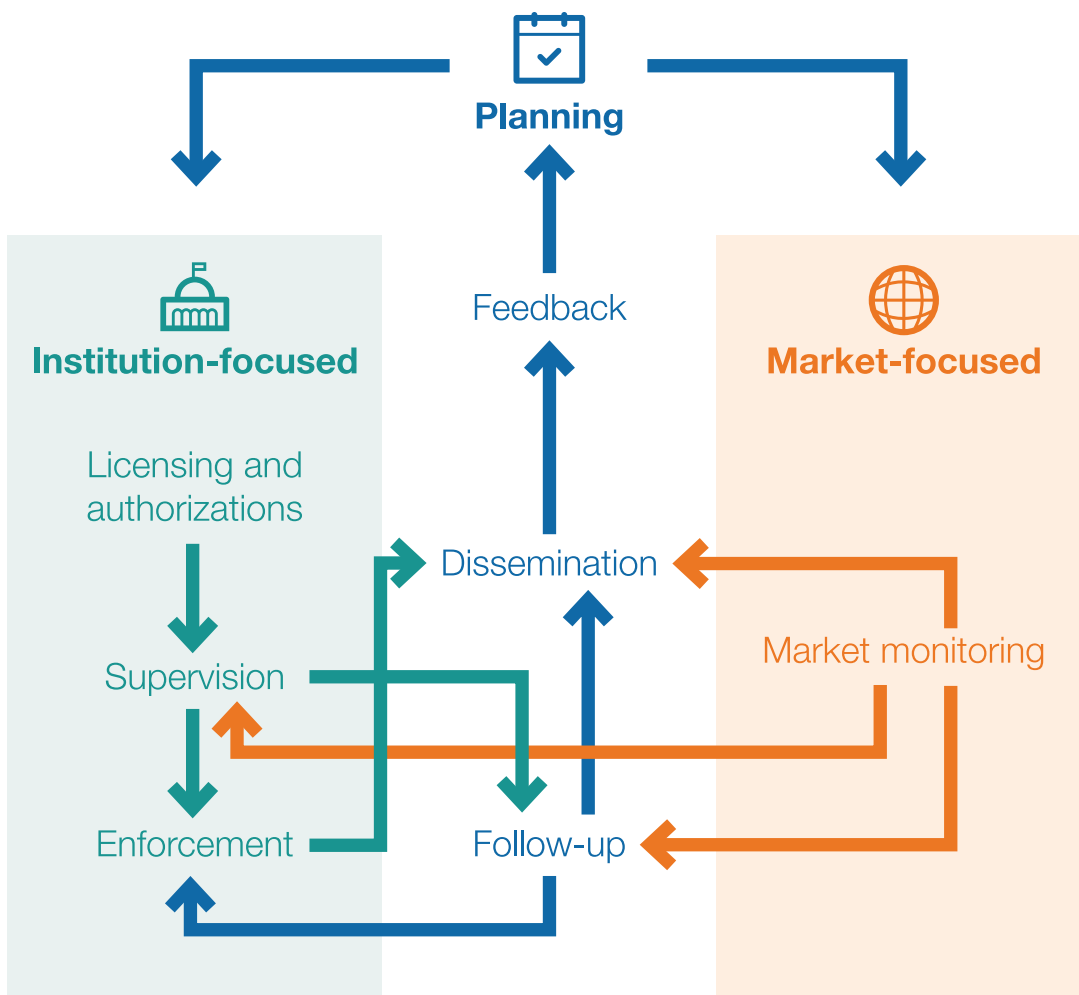
To identify which areas supervision should focus on, it is critical to use impact indicators together with updated risk profiles. The next point to consider is existing capacity, especially in terms of number of staff, their availability, and their expertise. Priorities at the market level may also shift throughout the supervisory cycle due to factors such as entry of new providers and emerging new risks and DFS products. Finally, it is advisable to leave some free staff time in the plan to accommodate unexpected activities and projects related to shifts and external/internal demands.

Additional examples and guidance

[4. A simplified annual supervision plan](#)



FIGURE 5. **Types of supervisory activities**



Source: Izaguirre et al. 2022.

4.3 Using a mix of supervisory tools

Supervisors carry out a range of supervisory activities. A range of offsite and onsite tools can be deployed for each (see [Figure 5](#)).

A mix of supervisory tools is important for effective RBS. The combination of tools should be based on the objectives pursued, existing capacity to deploy the tools, and the need to proportionately use resources according to the risk profile of each DFS provider. For instance, institution-focused supervision should not rely on onsite inspections alone. Other potential tools include offsite (remote) inspections, whistleblower investigations, and mystery shopping. Follow-up tools include requiring course correction by DFS providers, providing guidance to the market, referring cases to a criminal authority, and proposing regulatory change. Enforcement tools include fines, product withdrawal, suspension of operations, and the requirement to increase capital. Tools for dissemination include publishing statistical reports, reports on supervisory activities, and a summary of enforcement actions. Effective licensing is also important. In addition to keeping unqualified applicants out of the market, it provides supervisors with a wealth of useful information about DFS providers.

Market-focused activities are fundamental to effective RBS. They include thematic reviews, surveys, mystery shopping and, most importantly, ongoing market monitoring (see sections [3.2.2.1](#) and [4.5](#)). Market monitoring tools include analysis of regulatory returns, social media monitoring, customer interviews and surveys, mystery shopping, and thematic reviews (Izaguirre et al. 2022). Market-focused activities feed into institution-focused supervision and vice versa. However, most supervisors in EMDEs tend to focus DFS supervision on providers, especially in the initial supervisory cycles. One reason may be low quality data (see [section 4.6](#)) and the tendency to prioritize onsite inspections.

There is also the need to balance institution- and market-focused activities. Internal organization can play a role in achieving such a balance (see [section 3.2.2.1](#)). Supervisors should prioritize improved market monitoring by improving internal organization, data collection, and data analytics (see [section 4.6](#)).

4.4 Ensuring effective licensing

4.4.1 BUILDING A STRONG LICENSING FRAMEWORK

Most countries accept applications for new DFS providers on a rolling basis (i.e., prospective applicants may apply for a license at any time). As a gatekeeping function, licensing facilitates the work of supervisors by staving off unfit DFS providers, indicating minimum compliance and risk management requirements to each applicant, and producing useful information about applicants that supervisors can use. In addition to new licenses, authorization procedures can cover a range of situations depending on the country's regulatory framework:


- Transfer of significant ownership of DFS providers
- Mergers or acquisitions of DFS providers
- New products from or activities by DFS providers
- Opening or closing new channels or service points by DFS providers
- Increasing or reducing DFS provider capital
- Hiring or dismissing DFS provider executives
- Changes in DFS provider bylaws
- Cancellation (or withdrawal) of operating license

Although international standards do not exist for regulating and supervising DFS providers, the existing financial sector standards for banks offer a good framework for DFS provider licensing. The most relevant international standards related to licensing that could apply to DFS providers are the Core Principles for Effective Banking Supervision (BCBS 2019a), those listed in [Figure 6](#) in particular.


Several elements make up a strong licensing framework by allowing supervisors to conduct thorough analyses of applications while increasing transparency, accountability, and certainty: legal basis, framework for rejection, clear procedures, clear communication, and timeliness—as [Figure 7](#) further elaborates.

The supervisor should lawfully be given the power to establish licensing and rejection criteria for DFS providers. Minimum initial capital is one of the most common licensing criteria. But many others exist, such as governance


FIGURE 6. **Core principles for effective banking supervision relevant to licensing and authorizations**




CORE PRINCIPLE 4
Permissible activities: The permissible activities of institutions that are licensed and subject to supervision as banks are clearly defined and the use of the word “bank” in names is controlled.



CORE PRINCIPLE 5
Licensing criteria: The licensing authority has the power to set criteria and reject applications for establishments that do not meet the criteria. At a minimum, the licensing process consists of an assessment of the ownership structure and governance (including the fitness and propriety of Board members and senior management) of the bank and its wider group, and its strategic and operating plan, internal controls, risk management and projected financial condition (including capital base). Where the proposed owner or parent organisation is a foreign bank, the prior consent of its home supervisor is obtained.




CORE PRINCIPLE 6
Transfer of significant ownership: Transfer of significant ownership: The supervisor has the power to review, reject and impose prudential conditions on any proposals to transfer significant ownership or controlling interests held directly or indirectly in existing banks to other parties.



CORE PRINCIPLE 7
Major acquisitions: The supervisor has the power to approve or reject (or recommend to the responsible authority the approval or rejection of), and impose prudential conditions on, major acquisitions or investments by a bank, against prescribed criteria, including the establishment of cross-border operations, and to determine that corporate affiliations or structures do not expose the bank to undue risks or hinder effective supervision.


Source: BCBS 2019a.

FIGURE 7. **Components of a strong licensing framework**




LEGAL BASIS

- Licensing powers, requirements and procedures in regulation
- Entities and situations subject to license/authorization
- Unrestricted right to request additional information and interviews with applicants




FRAMEWORK FOR REJECTION

- Formal powers and willingness to reject applications
- Criteria for rejection, including broader policy goals




CLEAR PROCEDURES

- Formal, clear, timely and efficient procedures
- Internal guidance for analysis
- External guidance for clarity



CLEAR COMMUNICATION

- Timely communication of the licensing decision to the applicant, with reasoning in the case of rejection or imposition of conditions



TIMELINESS

- Time to process an application clearly established. Time starts counting when application is considered complete. Additional information requests interrupt the countdown

structure and transparency of ownership, proof of origin of funds used by investors, quality and strength of the business plan, fit and proper requirements for investors and executives of the DFS provider, and consumer protection requirements. The supervisor should have the power to reject applications when licensing criteria are not fully met and issue licenses that are conditional upon the implementation of certain measures.²⁷

4.4.2 ESTABLISHING CLEAR AND EFFICIENT LICENSING PROCEDURES

It is important to provide potential DFS providers and the general public with clear guidance about the licensing process and its requirements, including explanations about when licensing/authorization is required. The supervisor should also communicate the time it takes to process license applications. Inadequate communication about how existing regulations apply to DFS, especially those designed for traditional businesses, could lead to less interest by potential applicants.

The supervisor should create clear licensing procedures that include the following steps:

- **Step 1: Identify licensing phase.** In the case of applications for becoming a new DFS provider, many—if not most—countries divide the licensing process into two phases: initial authorization and final authorization. The process and requirements of each phase should be made clear to applicants.
- **Step 2: Determine relevant licensing category.** Most countries require that different types of DFS providers obtain a license prior to starting operations. Different types of businesses fall into different licensing categories (e.g., EMI, PSP, payment initiation service provider, account information service provider, crowdfunding platform operator, robo-advisory service provider, virtual asset service provider, peer-to-peer [P2P] lending platform operator). The licensing requirements for each licensing category should be made clear to applicants.

- **Step 3: Analyze business plans.** DFS providers should be required to present a business plan covering a minimum number of years. At least two aspects should be assessed by supervisors during licensing review: quality (completeness, coherence, and whether the plan is realistic) and the feasibility and viability of the proposed business.



Additional examples and guidance

[5. Analyzing an EMI's licensing application](#)

- **Step 4: Carry out an initial meeting.** It is good practice for supervisors to call at least one meeting with the DFS provider applicant so their representatives can explain the applicant's background; intentions; overall strategy to enter, grow, and compete in the market; target clientele; and other business plan highlights. The DFS provider may also be required to perform a product demonstration.
- **Step 5: Adopt a licensing decision.** Supervisors should not grant a license simply because an application is complete. Granting a license means being satisfied with all the aspects analyzed during the licensing process. In granting a license or rejecting a licensing application, supervisors may also consider broader policy goals such as financial inclusion, competition, consumer protection, and financial system efficiency and safety.

In addition to increasing transparency, other improvements to licensing procedures that could be considered include:

- Setting up a mechanism to gather feedback about licensing procedures from DFS providers
- Gathering internal feedback about licensing procedures
- Establishing objectives and procedures for seeking the opinion or approval of other departments on specific licensing applications

²⁷ Another issue that arises in licensing new DFS providers is how to apply or adapt existing licensing categories (types of regulated institutions) to new business models. For instance, the Central Bank of Brazil has gradually allowed nonbank DFS to use the “LEGO approach,” whereby licenses (e.g., PSP and lender licenses) are combined.

- Improving internal guidance for licensing staff to support the practice of adapting regulatory requirements in proportion to DFS provider size, complexity, and business model
- Maintaining an information system to record the particulars of each licensing application, related documentation, and interactions with applicants; making the information accessible to various licensing, supervisory, and regulatory departments
- Consider setting up an interface to digitally receive applications, communicate with applicants, and store all related documentation to improve agility, reduce costs, and increase convenience for both DFS providers and supervisors

Some financial authorities in EMDEs lack written guidance for staff that analyzes DFS applications. This can lead to delays, inefficiency, and lack of consistency in licensing decisions. For instance, in a case where internal guidance is lacking, an application may be halted due to a minor weakness in the information provided. However, if the issue is minor, a conditional license could be considered and the issue flagged for follow-up when the DFS provider becomes operational. In some cases a brief inspection by the supervisor may be required before a newly licensed applicant starts operations. This could be useful in understanding the severity of issues spotted during licensing and whether those problems have been addressed. Another common issue is untimely, unclear, or lack of feedback, including long periods where the applicant gets little to no information on the status of their application. Silence could be related to, for instance, a lack of clarity about the need to seek concurrence from other departments or simply their opinion, which could lead to a standoff in the case of divergent opinions. These situations affect process efficiency and the supervisory authority’s credibility.

4.4.3 INCREASING PROPORTIONALITY AND FLEXIBILITY OF LICENSING

Gatekeeping is fundamental to achieving policy goals such as financial inclusion, consumer protection, stability, safety and soundness, market integrity, and competition.

However, these objectives are not always easy to balance and supervisors may run the risk of overemphasizing one or another (Tomilova and Valenzuela 2018). For instance, applying requirements designed for complex banks to DFS providers with a limited scope of activities could create undue barriers to entry. On the other hand, excessively permissive licensing to foster financial inclusion may attract DFS providers that lack the capacity or willingness to safely provide services. There are many reasons supervisors may impose disproportionate (too lax or too strict) requirements on DFS providers during licensing, including limited knowledge about DFS and business models (see [section 5.2.1.2](#)) and the absence of guidance for licensing staff on how to interpret regulations.

In addition, swift developments in DFS markets—the modularization of value chains, in particular—require greater licensing flexibility.²⁸ Existing licensing frameworks may be on the way to becoming outdated. Some questions supervisors should ask themselves include: Are current licensing categories adequate? Does the licensing framework limit innovation? Does it cover innovation that should be covered? Newer approaches to licensing can introduce agility and accommodate new business models but they require greater flexibility in the use of licensing categories and their respective requirements. In practice, this means better adjustment of entry and operating requirements to each applicant. In some countries, introducing flexibility in licensing may require legal and regulatory reforms. In most cases it will also require a cultural shift by supervisory staff. [Figure 8](#) describes a few examples of emerging licensing approaches.

Some EMDEs have taken steps to improve flexibility in licensing to accommodate innovation and new types of players, including fintechs and digital banks (Dias 2020b). For instance, many run innovation facilitators such as regulatory sandboxes. In some cases DFS providers that participated in sandboxes have been licensed.

28 For a discussion on modularization and relevant cases, see [section 6.2](#), Zetterli (2021), Mdluli et al. (2022), and Mitha et al. (2022).

FIGURE 8. Increasing flexibility of licensing procedures



4.5 Optimizing offsite supervision

In our work we have observed that in many EMDEs, supervisors tend to conduct inspections without the proper support of offsite analysis. An excessive or exclusive focus on onsite inspections could lead to ineffectiveness

and drain limited supervisory capacity. This section provides guidance to enhance offsite supervision, with the purpose of increasing effectiveness and supporting other supervisory activities, including onsite inspections.

Offsite supervision includes offsite analysis of both the market as a whole and specific providers. It plays a central

role in risk-based supervision as it helps identify providers and risks that warrant greater supervisory attention and resources during institution-focused inspection work (onsite or remote). High quality data and analytics capabilities are essential (see [section 4.6](#)).

4.5.1 TYPES OF OFFSITE ACTIVITIES

Although there is not an internationally agreed-upon classification of offsite supervisory activities, for the purposes of this Technical Guide we use the following classification (further developed in [Box 4](#)):

- i) Offsite analyses as part of ongoing monitoring/surveillance
- ii) Offsite analyses to support inspections or thematic reviews

A fine line exists between offsite institution-focused monitoring and offsite analyses to support an inspection. The main differences are in the data and skills needed:

- **Differences in the data.** Monitoring primarily uses data that are regularly collected through regulatory reports and other regular sources (e.g., data reported by other departments or agencies, collected from social media and websites of DFS providers). Offsite analyses to support inspections use the same regularly collected data complemented by a range of additional information collected for the specific purpose of the inspection or thematic review. It could include, for example:



Additional examples and guidance

[6. Financial analyses of EMIs](#)

[7. Data collection template for EMIs](#)

[8. Reporting guidance for EMIs](#)

BOX 4. Types of offsite supervisory activities

Offsite analyses as part of ongoing monitoring or surveillance. In many countries, ongoing (repeated, periodic) analyses are known as offsite supervision or offsite surveillance. It could but does not need to be in the hands of a dedicated team. This type of monitoring can be split into

two focus areas: (i) market-focused monitoring and (ii) institution-focused monitoring. The two complementary activities feed each other. For instance, a set of indicators originally produced for institution-focused monitoring may also be useful in market-focused monitoring.

Market-focused monitoring

Analyses that look at the whole market to identify and measure risks and market trends across all DFS providers and peer groups of DFS providers. Examples: monitoring for consumer protection purposes by looking at indicators such as volume and nature of complaints; monitoring of growth trends in the e-money industry by looking at indicators such as total e-money issued compared to total retail deposits.

Institution-focused monitoring

Analyses that focus on key aspects of individual DFS providers. Examples: monitoring compliance with specific regulatory requirements such as the equivalence between total e-money issued and the balance in float accounts; monitoring financial performance of DFS providers by looking at indicators such as profitability and operational efficiency.

Offsite analyses to support inspections and thematic reviews. Supervisors should make a significant effort offsite prior to departing for an onsite inspection or before they start a remote inspection. The better the offsite inspection preparations, which

are institution-focused by nature, the more efficient and effective the onsite or remote inspection. Thematic reviews may also partially or entirely rely on offsite analyses.

- Information requested directly from the DFS provider (e.g., operations manual, business continuity plan, internal audit reports)
- Information collected internally by the DFS supervision department and other departments (e.g., licensing data, previous inspection reports, follow-ups, communications with the DFS provider)
- Information collected externally, such as from other authorities (e.g., ombuds, competition authority, foreign authorities)
- **Differences in skills.** Expertise and skills also differ between the two types of institution-focused offsite work. Those performing offsite analysis to support inspections often need to engage directly with providers. This requires good communication and persuasion skills in addition to the self-confidence supervisors involved with inspections ideally possess. Monitoring requires data management and analytical skills that may be less important for those performing inspections.

Taking the above into consideration, an array of possible internal arrangements can be made for offsite supervision and onsite inspections, as discussed in [section 3.2.2](#).

4.5.2 IMPROVING THE EFFECTIVENESS OF ONGOING OFFSITE MONITORING

Supervisors should ensure that ongoing market- and institution-focused monitoring are both comprehensive and of high quality to fully support annual supervisory planning and timely adjustments. However, supervisors in EMDEs rarely conduct offsite monitoring on an ongoing basis. Getting reports sent by DFS providers is not enough; supervisors need to analyze the reports and act upon their analysis. Few EMDEs have a structured ongoing monitoring framework, particularly for market monitoring. Supervisors looking to become more data-driven need to improve offsite monitoring (see [section 4.6](#) for specific guidance). Supervisors may consider the following aspects:

1. Periodically assess the quality of offsite monitoring.

- a. Does ongoing monitoring include both market- and institution-focused monitoring?
 - b. Is ongoing monitoring based on a written framework that describes objectives, monitoring strategy, indicators monitored, content and audience of periodic monitoring reports (e.g., ongoing, quarterly, annually), and staff responsibilities?
 - c. Is staff conducting offsite monitoring adequate in terms of number and expertise?
 - d. Is the organizational arrangement adequate enough to support effective offsite monitoring?
 - e. Are the periodic monitoring reports of high quality and used to shape the annual supervision plan, along with the scope and depth of inspections and thematic reviews?
 - f. Is coordination between departments adequate?
2. Periodically assess the data used in ongoing monitoring.
 - a. Is the set of indicators used sufficient and of high quality (accurate, timely, comprehensive)?
 - b. Are shortcomings in monitoring reports due to low data quality or weaknesses in data analytics?²⁹
 - c. If shortcomings are related to data analytics and visualization, are analytics and visualization tools adequate or is the problem related to expertise, guidance, or both? What are the possible solutions? Invest in new software? Invest in training? Hire new staff with expertise in data science, data engineering, statistics, machine learning?

If resources are available, it is good practice to set up a team to undertake offsite market monitoring and ongoing institution-focused monitoring. This is the case with the Central Bank of Brazil where the monitoring team supports the teams responsible for prudential, market conduct, and AML/CFT supervision with their monitoring activities. The dedicated team covering market-focused and institution-focused monitoring may also be responsible for conducting

²⁹ See [section 4.6](#) for guidance on shortcomings related to data quality.

thematic reviews, as is the case with the Financial Conduct Authority in the U.K. However, this type of internal arrangement may not be the most common in EMDEs where the team responsible for conducting inspections conducts institution-focused ongoing monitoring (e.g., Ghana). Despite its importance, market-focused monitoring does not exist as a function in many EMDEs.

4.6 Improving supervisory data

Since supervisors ground their actions and decisions in information and data, becoming data-driven is a necessary step for most. It means improving the quality of supervisory data and data analytics capabilities. Without quality data, it is virtually impossible to implement risk-based supervision—the cornerstone of effective DFS supervision (see [Chapter 3](#)). Yet low-quality data is possibly one of the most common challenges EMDEs face. Others are discussed in [Chapter 5](#).

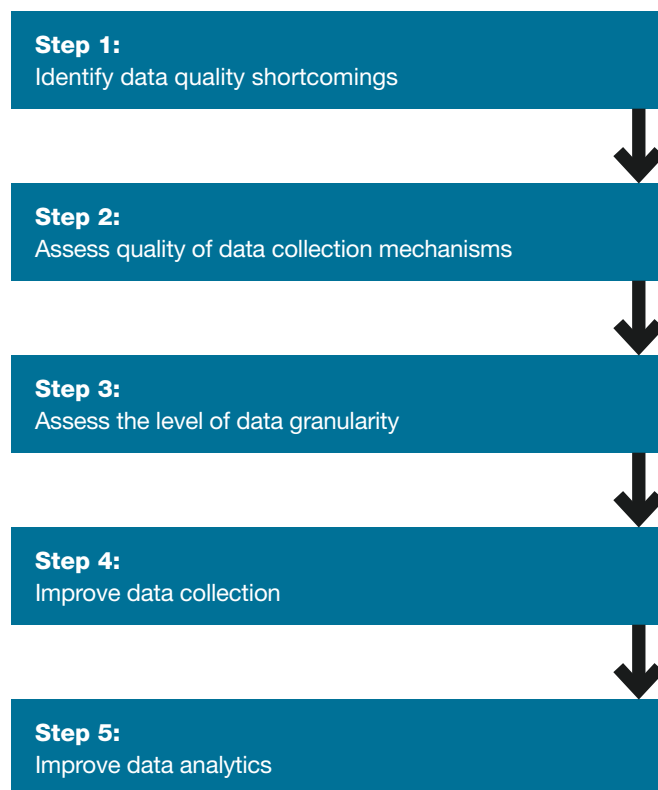
It is worth highlighting that while data quality is a precondition for effective RBS, a lack of quality data does not mean supervisors cannot begin to implement the foundations of the risk-based approach described in [Chapter 3](#). RBS can start prior to resolving all data quality issues. In terms of data, most supervisors in EMDEs start off with what is available then work to improve data over time. Making DFS supervision more data-driven means harnessing the power of data and technology to strengthen ongoing market monitoring and other supervisory functions. This section presents five steps to help supervisors become more data-driven (see [Figure 9](#)).

Additional examples and guidance

[2. Examples of impact indicators](#)



FIGURE 9. **Five steps to make DFS supervision more data-driven**



4.6.1 STEP 1. IDENTIFY DATA QUALITY SHORTCOMINGS

Supervisors looking to ensure they have the quality and quantity of data they need may ask the following questions: Which data are needed? How frequently? In what format and at what level of granularity? How does that compare with existing data? What are the shortcomings of the existing data?

The current data could have many types of shortcomings:

- **Gaps.** Data that are needed but not collected
- **Duplication.** Same or very similar data being collected in different reports
- **Inaccuracy.** Data that do not reflect reality due to false reporting or failure in integrity
- **Inconsistency.** With duplication, there could be inconsistency across different indicators due to the formulas used to calculate them in different templates, use of different terminology or different formats, or failures in the data aggregation process at DFS providers

- **Delay.** The time-to-report (period between cutoff date and actual reporting date) may be long, which could be related to factors such as lag allowed by reporting requirements, the inability of DFS providers to quickly transform data into required formats, or a combination of these factors

Supervisors need to identify the root causes of shortcomings prior to finding solutions. It is unadvisable to rush into technical solutions (e.g., buying new software or data warehouse) prior to identifying the causes. This way, supervisors avoid investments or reforms that do not fully resolve shortcomings or those that create new problems.

4.6.2 STEP 2. ASSESS QUALITY OF DATA COLLECTION MECHANISMS

Many underlying causes for weaknesses in supervisory data are related to the mechanisms supervisors use to collect the data and those DFS providers use to report data in the required formats. In this context, “data collection mechanism” covers the end-to-end process of regulatory reporting. Supervisors have to assess which parts of the process are generating data quality problems:³⁰

- **Design and imposition of reporting requirements.** Dias and Staschen (2017) shows that although most supervisors use report templates to impose data standardization, only a few offer comprehensive guidance to reporting institutions and consult with the industry before imposing requirements. Detailed guidance to reporting institutions (including data dictionaries and taxonomies) helps ensure a high level of standardization and, hence, comparability.
- **Data aggregation, validation, and reporting processes at DFS providers.** Even large internationally active banks may use manual procedures for data gathering, validation, and reporting, as European Banking Authority/EBA (2017) describes. These issues almost always affect DFS providers in EMDEs.
- **Interface for data transfer.** When not well designed, the interface between a DFS provider and the supervisor, such

as a file transfer system, email, or application programming interface (API), can be the source of problems.

- **Supervisor’s validation of regulatory reporting data** submitted by DFS providers, in addition to the validation checks DFS providers conduct before remitting data.
- **Supervisor’s management of regulatory reporting submissions** by DFS providers, particularly when performed manually (e.g., controlling the timely submission of a large number of reports using spreadsheets).
- **Data storage and retrieval used by the supervisor** can be outdated, inconvenient, and lack storage capacity.

Many financial supervisors in EMDEs and advanced economies alike have recently reformed or are currently revamping their data collection mechanisms ([Box 5](#) describes the EBA as an example). Goals include achieving higher data quality via greater automation, higher levels of data granularity (see [section 4.6.3](#)), and lower compliance costs in the long run.

4.6.3 STEP 3. ASSESS THE LEVEL OF DATA GRANULARITY

One key decision supervisors need to make when considering improvements to their data relates to level of data granularity. Granular data are closer to the raw business data DFS providers produce as part of their operations on an ongoing basis. The standards (scope, format, and definitions) of such raw data vary widely across providers according to their respective information systems. Supervisors cannot readily use raw data to compare providers. Data need to be standardized first, that is, the raw data need to be “transformed” into common standards set by the supervisor. The level of standardization detail depends on whether the supervisor wants to collect granular or aggregate data. Collecting granular data means collecting many more data points than those collected with aggregate data. Hence, it is also more complex to standardize granular data because more data points must be standardized. The prevalent practice

³⁰ Data collection mechanisms have a direct impact on compliance costs imposed on DFS providers and on the effectiveness and efficiency of DFS supervision. Hence, a good data collection mechanism should also be a priority for supervisors assessing compliance costs imposed on providers.

BOX 5. Reforming the EBA's reporting system

In 2017 the European Banking Authority (EBA) published a report describing a range of shortcomings in reporting procedures at reporting institutions. More recently it was complemented by a study of the effectiveness of supervisory data (EBA 2021a). The EBA, which establishes a pan-European supervisory reporting framework for national (country-level) and European authorities, is currently working toward more efficient and proportionate supervisory reporting, taking into consideration the need to improve data quality, reduce compliance costs imposed on reporting institutions, and address the shortcomings of current data collection mechanisms. To this end, the EBA studied compliance costs and practical challenges currently faced by reporting institutions and put forward 25 recommendations in the following areas:

1. Changes to the development process for the EBA reporting framework
2. Changes to the design of EBA supervisory reporting requirements and reporting content
3. Coordination and integration of data requests and reporting requirements
4. Changes to the reporting process, including the wider use of technology

In tandem, the EBA has studied the viability of integrating its systems with reporting institution systems (EBA 2021b) based on clearly stated

objectives and principles (e.g., the “report once” principle, the principle to eliminate multiple reporting of the same data). Among other expected results, the new system would reduce the overall scope of reporting requirements, introduce a higher level of granularity and automation in reporting, and integrate all the data needs of different EBA departments (e.g., prudential supervision, statistics for monetary policy, data needed for resolution of regulated institutions). Next steps for implementing the envisioned reforms include:

1. Defining a common data dictionary for prudential, statistical, and resolution data
2. Further exploring the possibility of increasing granularity or reporting requirements
3. Investigating the need for a common solution to the reporting institution compliance process
4. Further investigating the desired target scenario based on a cost–benefit assessment
5. Setting up strong governance arrangements
6. Providing an estimate of costs and resources needed

In a dedicated online page, the EBA (2022) provides extensive guidance to reporting institutions with its Single Rulebook Q&A on Supervisory Reporting, Technical Standards, Guidelines and Recommendations, and other resources.

among supervisors in EMDEs is to collect aggregated indicators rather than granular data (see [Box 6](#) for an example of reporting an aggregated indicator).

There are benefits and challenges to collecting granular data but the central question remains whether the collection mechanism is adequate enough to handle granular reporting without jeopardizing data quality, increasing compliance costs for DFS providers, or overwhelming supervisors with manual validations and

complex data retrieval. Traditional mechanisms, such as Excel templates uploaded by DFS providers onto a web portal or via email, are inadequate for granular data. Supervisors moving toward granular data need to reevaluate their data collection mechanism. Otherwise, increasing granularity will most certainly lead to poor data quality.³¹

31 Compatibility between legacy and new data is another issue supervisors need to address when implementing a new collection mechanism for granular data. They must consider whether to require that some historical data be reported at the new level of granularity and establish a reasonable cutoff date that considers the practical challenges such reporting imposes on both DFS providers and supervisors.

BOX 6. Example of reporting an aggregated indicator

Supervisors commonly collect the aggregated indicator that encompasses total number of transactions by different types of DFS providers (e.g., EMIs). The most granular version of the indicator would instead collect the whole transaction database for a certain period, including every transaction, with all of its attributes determined by the information system each DFS provider uses (e.g., client number; transaction type, date, time, amount, and location). When reporting the indicator “total number/value of transactions,” the DFS provider must sum up all

transactions in the system and report the aggregated result to the supervisor.

Aggregation is often automated or semi-automated because DFS providers configure their systems to run the necessary calculations to arrive at the required indicator. Full automation is not always possible, particularly when data need to be collected and aggregated from different information systems, and even more so when dealing with legacy systems that use outdated infrastructure and data management architecture.

Additional examples and guidance

[9. Anonymized data collection plan for EMIs](#)



4.6.4 STEP 4. IMPROVE DATA COLLECTION

Supervisors may consider investing in better data collection mechanisms that allow high quality granular data and timely reporting. These mechanisms could be based on IT solutions that expedite the shift away from traditional reporting templates that need to be filled out by DFS providers (e.g., Excel files) and toward greater automation. The need for automation is not one-sided, as both the supervisor and DFS providers need to automate procedures on their end. Even if the supervisor installs an excellent interface for data transfer, validation, storage, and retrieval, it will still produce low-quality data if DFS providers continue to use manual processes to gather, transform, and validate data. One alternative is for the supervisor’s systems to collect data directly from providers’ systems and transform the data to common standards at the desired level of aggregation (see EBA plans in [section 4.6.2](#)). This approach to data collection is called “data pull.” However, it does not automatically lead to higher

data quality in the absence of excellent standardization and validation.³²

While many IT solutions have been used to automate reporting in banking supervision over the past decades, newer types of supervisory technology (suptech) are creating opportunities for supervisors to significantly improve data collection without the need to make the prohibitively expensive investments previously required (see [Box 7](#) for two country examples).

The examples above and the EBA example in [Box 5](#) are not specific to DFS but could apply to any supervisory data, including those used by supervisors of DFS providers. Data collection for DFS supervision is part of an ecosystem of functions performed by different departments of a supervisory authority. DFS data collection does not occur in isolation and is rarely planned and reformed in isolation. Depending on the case, revamping DFS data collection mechanisms could require revamping an authority’s whole data collection mechanism. It could also involve other financial authorities. In most cases, revamping the entire mechanism requires a significant amount of time and effort. These types of projects are usually long-term, multi-year, and based on careful planning (see [Box 8](#) on the joint initiative between the FCA and the Bank of England to transform data collection).

32 One mistake supervisors in EMDEs may make is to leave the definition of standardization and validation rules almost entirely in the hands of the technical vendor and internal IT professionals. While their contribution is crucial, as subject matter experts and the main users of such data, the supervisory staff needs to lead the standardization process.

BOX 7. Using technology to improve data collection mechanisms

AUSTRIA

In the case of Austria, Turner (2015) illustrates the kinds of improvements countries can achieve in supervisory reporting with good planning and attention to implementation challenges. Austria's central bank, OeNB, led a multi-year project to revamp the banking sector's data collection mechanism, integrating all main reporting requirements from within OeNB and other authorities, including the Financial Market Authority. Its main objectives were to integrate requirements and eliminate duplication and inconsistency of data across reports. To do so, granular data were needed. The project involved extensive consultations with the industry to define and standardize each granular data point collected.

Currently, raw business data go through a first phase of standardization. Then, large batches of such granular data are input into a central database held at a company called AuRep. This can be considered a "push" approach, with the use of a centralized

structure for data storage. OeNB accesses the data from AuRep after it is again transformed according to the rules OeNB defined in consultation with the banks. Despite the initial investment banks made in order for granular data reporting to become feasible and to set up AuRep, the use of a common reporting platform means that banks may be saving on reporting costs over the years. Importantly, due to the granularity of the data sitting at AuRep, OeNB can change reporting requirements (the second level of "transformation" mentioned above) at virtually no cost to banks.

PHILIPPINES

di Castri et al. (2018) illustrates how the Central Bank of the Philippines (BSP) conducted a pilot to use API-based data architecture for prudential reporting. The prototype delivered a greater volume of data at shorter intervals (hourly) and with fewer duplications, errors, and omissions. Staff time dedicated to validation was also significantly reduced.

Not all data collection reforms for DFS supervision need such ambitious goals from the start. They may, for instance, start with a pilot project that only covers one type of DFS provider (e.g., EMIs). A pilot may also only cover certain data types. Pilots can later inform all-encompassing reforms.

4.6.5 STEP 5. IMPROVE DATA ANALYTICS

Supervisors need adequate capacity to take full advantage of the data collected. If data collection mechanisms shift toward larger volumes of frequent granular data, the need for analytical capacity increases and new skills and more staff may be required. Suptech can offer value for supervisors in improving data analytics but it does not substitute for the need to invest in analytical skills and expertise.

Investments in suptech to revamp data collection and analytics could create greater opportunities for supervisors in EMDEs to leapfrog the gradual evolution seen in advanced economies (Dias and Staschen 2018b).

To achieve this, a well-defined suptech strategy is essential. It should support prioritized policy goals and help supervisors assign the right resources for effective implementation of suptech solutions. Designing a suptech strategy requires the engagement of different stakeholders within the authority, including IT and legal units, as well as key external stakeholders (Appaya et al. 2020).

Use cases for suptech in data analytics include:

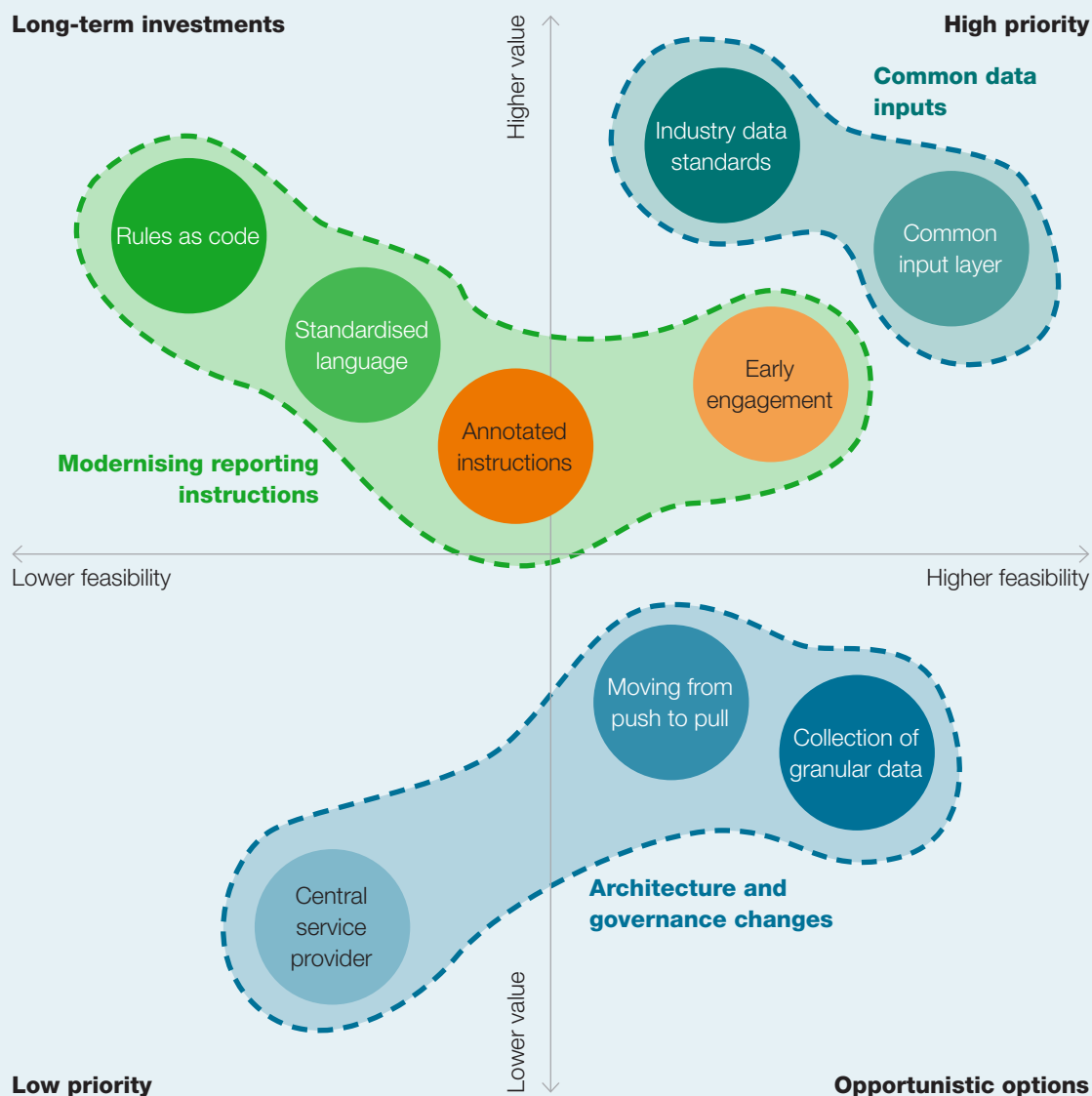
- Automated compliance checks with certain regulatory requirements like capital requirements, transaction thresholds, and fund safeguarding requirements
- Automated search and preliminary analysis of information publicly available on the internet (web scraping and web crawling)
- Augmented analytical capacity with the use of technologies such as network analysis, topic modeling, and pattern recognition
- Better visualization of analyses of individual DFS providers or the entire DFS market

BOX 8. Reforming data collection in the U.K.

The U.K.'s Financial Conduct Authority (FCA) and the Bank of England are working together to revamp data collection in the financial sector to align with their respective long-term data strategies (FCA 2022a;

Bank of England 2021).^a The plan is informed by extensive industry consultation which, among other feedback, classified potential reforms into different levels of feasibility and value (see Figure 10).

FIGURE 10. The U.K.'s priorities for data reform



Prior to launching such broader data reform, the Bank of England and the FCA jointly ran a pilot on digital regulatory reporting that initially only covered part of the reporting requirements for mortgage operations. The joint initiative started in 2018 to pilot digital regulatory reporting (DRR), more specifically the use of machine executable regulation. The intent was to test the concept of DRR by initially using

only part of the reporting requirements imposed on mortgage operations to improve data quality and increase reporting efficiency. See FCA (2020) for details. The results of the DRR joint initiative have informed the broader data reform.

Source: Bank of England 2021.

a. Bank of England (2021) provides a detailed description of an incremental implementation plan that will span 10 years.

BOX 9. Examples of suptech initiatives

Some financial authorities have launched initiatives to explore suptech to improve data analytics. For example, De Nederlandsche Bank has a dedicated team to foster the development and use of suptech by supervisory and economic departments (Elderson 2020). The European Central Bank (ECB) created a SupTech Hub to explore suptech's potential (ECB 2022). Ghana's Digital Financial Services Policy identifies the creation of a "regtech strategy across regulators" as one of the necessary actions to achieve inclusive DFS in the country (Government of Ghana 2020).

In 2017, the Monetary Authority of Singapore also created a Data Analytics Group. Its three units include:

- The Data Governance and Architecture Office (DGA) formulates data management policies, manages data collection and quality, maintains MAS's data catalog, and publishes its official statistics.
- The Specialist Analytics and Visualisation Office (SAV) conducts data analyses in partnership with MAS departments, helps departments improve their data capabilities through reusable tools and code libraries, and partners with the MAS Academy to deliver data analytics training programs. Together with the MAS IT department, the team designs and implements the technical infrastructure needed to support data analytics work within MAS.
- The Supervisory Technology Office conducts data analyses on supervisory and financial sector data in partnership with MAS departments. It works with the Fintech and Innovation Group to promote data analytics capabilities within the financial industry and foster innovations that make regulatory compliance more efficient and effective (MAS 2017).

FSB (2020a) found that until very recently, over 50 percent of FSB members—many of whom are supervisors from advanced economies—relied solely on Excel for their data analytics for bank supervision and financial stability. In addition, the outputs from analyses were only descriptive. We may assume that this is also the reality of most supervisors in EMDEs. However, the increased availability and affordability of suptech is allowing supervisors to strengthen their analytical capacity to achieve results that would be impossible using only Excel. For instance, suptech tools enable them to go beyond a simple description of the current situation in their market to make diagnostics about the reasons for the situation, predict the future behavior of indicators, and potentially prescribe supervisory actions.

Larger data sets and the combination of different data types, sources, and formats to support supervisory findings and decisions require advanced analytics and specialized skills, but not every supervisor needs these skills, particularly in the early stages of DFS supervision. Supervisors must evaluate the required skill set and

technology that best supports their objectives, the characteristics of the market, and the data sets at hand.

4.7 Optimizing inspections

Onsite inspections enable supervisors to access DFS provider facilities, run audits and tests on their information systems, interview staff and customers, observe staff as they conduct activities, and use other supervisory techniques to arrive at a fair assessment of the level and direction of risks DFS providers face. However, onsite inspections are time consuming and expensive. They demand significant staff time and create additional expenses, such as transportation and accommodation costs, per diem, laptops, and remote online access to the supervisory authority's systems. To use onsite inspections most effectively, supervisors must step up their offsite preparations.

With the onset of the COVID-19 pandemic, many supervisors began taking steps to remotely perform many of the activities previously conducted onsite at headquarters, branches, and other provider locations.

Remote/offsite inspections have since become ever more common. This positive development pushes supervisors to seek opportunities to become more thorough and strategic in their offsite preparations for inspections, regardless of whether they are entirely or partially remote. For instance, some supervisors are used to requesting key documentation once onsite. However, by making requests for and analysis of most documentation and data prior to the start of remote or onsite meetings with DFS providers the rule rather than the exception, supervisors will achieve greater efficiency and ultimately increase supervisory effectiveness. This section highlights five steps to help supervisors optimize inspections.

4.7.1 STEP 1. PREPARE AS MUCH AS POSSIBLE OFFSITE

It is critical to ensure that the inspection team is well prepared. Organization and allocation of responsibilities among team members should be clear. Before inspection starts, all team members should be aware of what they need to acquire from the DFS provider and what they must produce and achieve. The team should also consider how best to use technology for effective remote and in-person provider interactions. With the right planning and mindset, many of the activities and analyses previously performed onsite can and should be done remotely (e.g., use APIs to connect to the DFS provider's systems). With APIs, the team can even partially or entirely conduct system audits.

The inspection team should start remote or in-person interactions (e.g., interviews, meetings, observation of routine procedures by operational staff) with the DFS provider only after thorough offsite preparation based on an initial information request and follow-ups. As part of the preparation, the supervisor needs to identify the most concerning issues at the highest level of specificity possible. They will be further investigated during interactions with the DFS provider; the team should also prepare for key meetings and interviews to discuss them. If serious and contentious issues are to be covered in meetings, supervisors may choose to rehearse responses to increase preparedness for potential reactions by the DFS provider.

4.7.2 STEP 2. COLLECT SUFFICIENT INFORMATION PRIOR TO INSPECTION

As a rule, supervisors should spend significantly more time on offsite preparations than on the inspection itself. They should exhaust efforts to remotely collect information prior to moving on with interactions with the DFS provider unless there is a specific reason for not doing so (e.g., probing into a certain issue needs to remain confidential until arrival onsite). A thorough preparation phase entails making one or likely several follow-ups on the initial request for information. In many countries, the initial request is the same document where the supervisor announces inspection date(s). It is important to remain flexible in terms of dates since preparations may take longer than expected. Rigidity on start date and number of information requests sent is not uncommon among supervisors in EMDEs but it reduces efficiency.

4.7.3 STEP 3. DEVELOP TAILORED QUESTIONS FOR INSPECTION MEETINGS AND INTERVIEWS

Optimizing inspections means more than conducting meetings via video conferencing or remotely accessing IT systems. It entails getting the most out of the time spent on inspections by maximizing preparatory analyses offsite. The inspection team should prepare guides or scripts for key interviews and meetings, including specifically how to raise sensitive questions or issues according to the supervisor's prior knowledge of DFS provider counterparts (e.g., a personality's tendency to confront, deny, or dismiss issues or to circumvent questions). Inspection meetings and interviews should not primarily be seen as fact-finding events but as techniques that allow supervisors to confirm, expand upon, and find causes for issues already identified during offsite preparations. For instance, rather than conducting interviews and meetings to review "yes" or "no" questions from a standard checklist, effective offsite preparation equips supervisors to ask more substantial questions about "why," "how," and "who."

Illustrative example. A supervisor is drafting a guide (talking points) for an interview with senior executives of a DFS provider as part of a special inspection of the complaints resolution mechanisms the provider has put

TABLE 2. **Sample questions to avoid and to ask during inspections**

| Examples of questions to avoid (get this information in advance instead) | Examples of questions to ask (confirm, deepen insight, probe, observe) |
|---|---|
| “Do you have a dedicated team to receive and solve consumer complaints?” | “Why don’t you have a dedicated team to receive and solve consumer complaints?” |
| “Does the Board discuss the effectiveness of complaints handling at your company?” | “Why hasn’t the Board discussed any issues related to the company’s complaints handling procedures, given that the internal auditor has flagged systematic failures for the last two years?” |
| “Is there a mechanism for reporting issues related to consumer complaints to the Board?” | “It seems that placing your complaints resolution unit under a business area that generates the largest volume of complaints (e.g., the credit card department) keeps the complaints handling team from solving complaints to the satisfaction of customers—most of whom escalate complaints to the external ombudsperson. It also seems to have restrained your company from analyzing complaints data to propose and implement changes to reduce incidents of the most common consumer issues generating complaints. What are your thoughts on this?” |
| “Where is the complaints resolution unit located in your organizational chart?” | |
| “Is this organizational structure the most effective way to achieve the objectives of your complaints resolution unit?” | |

in place. [Table 2](#) provides some sample questions the supervisor should avoid and some to ask.

Questions similar to those to “avoid” can instead be used as a probing technique. For instance, supervisors can use it when they already know an answer but want to probe a senior official’s knowledge of an observed weakness, issue, or policy the DFS provider has put in place. Supervisors can also use it to probe the official’s propensity to hide a weakness or knowledge of it.

The inspection team should always review answers with a critical eye toward whether misleading, incomplete, or false statements were given to dissuade the supervisor from pursuing an issue identified during offsite preparation. It is important for teams to adequately document key insights and information obtained during all meetings and interviews with the DFS provider.

4.7.4 **STEP 4. PRODUCE INSPECTION DOCUMENTS BASED ON INTERNAL GUIDANCE**

Supervisors should be given internal guidance and templates for preparing inspection documents. They are used to describe the main points covered in interviews and meetings with the DFS provider and respective outcomes. The same applies to the inspection report, which should describe the inspection’s objective, scope, techniques used, main findings, and recommendations or corrective measures. It is also good practice to conduct internal meetings with superiors and colleagues to discuss

weaknesses and other significant findings, especially those that would trigger enforcement procedures or corrective measures that could significantly impact the DFS provider. Prior to finalizing the report, the supervisor should conduct a dialogue with the DFS provider to clarify findings and potential recommendations. Without this interaction, the findings of the inspection report may catch the DFS provider off guard, which could lead to conflict, miscommunication, and delays in implementing corrective actions. The supervisor should seek to clarify issues and discuss potential corrective measures with the DFS provider’s senior management during the inspection’s exit meeting.

4.7.5 **STEP 5. CORRECTIVE MEASURES, ENFORCEMENT, AND FOLLOW-UP**

In the event an inspection identifies weaknesses, the supervisor can apply different tools to address them with the DFS provider. The most common outcome is an action plan that details the problem, the corrective measures to be implemented, and their respective timelines. The supervisor should follow up according to the specific timeline of each measure rather than wait for the next planned inspection. If weaknesses are serious or recurrent or if previous corrective measures have not been implemented, formal enforcement measures may be considered, such as fines, withholding approval of new products or acquisitions, suspending operations, imposing the requirement to hold additional capital, replacing or

restricting executives, limiting dividend payments, or referral to a criminal authority.³³ The supervisor may also require special external auditing or impose additional reporting obligations. Regardless of type, corrective and enforcement measures must be proportionate to the severity of each case.

4.8 Resolution of DFS providers

A financial safety net is a framework that includes several key functions to safeguard the stability of a country's financial system: prudential regulation and supervision, resolution, lender of last resort, and deposit insurance. The framework aims to reduce the probability of provider failure, and, in cases where failure does occur, reduce impact on individual consumers and the broader financial system. A strong risk-based prudential regulatory and supervisory framework is at the core of a financial safety net. It supports the safety and soundness of providers to ensure they are less likely to become insolvent.³⁴ However strong a framework may be, it does not guarantee zero failure of individual providers. That is why the financial safety net also includes a framework for minimizing the effects of eventual failures—in other words, the orderly wind down of all or part of a provider's operations, the reimbursement of consumer funds, and other measures.

Safety net frameworks are mostly designed to minimize and deal with the potential failure of large banks. However, fast and massive DFS adoption has changed the composition of financial sectors in EMDEs. These markets are experiencing increasing numbers and types of DFS providers, some that offer services akin to banking services to a large number of customers. A notable example in Brazil is Nubank, Latin America's largest fintech, which has nearly 65 million clients depositing funds in

its accounts. Nubank is the third largest “bank” in Brazil by number of customers. However, legally it is not a bank but a nonbank that combines an EMI license with a lender license. Innovation in business models and greater flexibility in licensing (see [section 4.4.3](#)) increase the urgency to discuss the application of safety net frameworks beyond prudential and market conduct supervision to nonbanks. While this section does not cover every element of the financial safety net, it primarily discusses issues around resolving DFS providers and briefly touches on deposit insurance as it applies to e-money.

4.8.1 RESOLVING DFS PROVIDERS

In most EMDEs there is no specific resolution regime applicable to DFS providers.³⁵ This guide's discussion of “resolution” refers to the process of dealing with failing DFS providers akin to what is understood as a bank resolution regime.³⁶ Some DFS providers, such as EMIs, take funds from the general public. This raises concerns that the lack of a resolution regime may impose losses on a large number of retail customers. While systemic stability concerns are usually not central to the supervision of most DFS providers, protecting retail customers against loss of funds becomes an important topic. In fact, the customer protection concern is present irrespective of the size of the provider collecting funds from the public. So what happens when a DFS provider fails?

In the case of EMI failure, customers are potentially exposed to loss or inaccessibility of their funds. That is why most countries impose fund safeguarding requirements on EMIs.³⁷ In cases where safeguarding requirements do not exist, customers of a failing EMI could be lined up with other unsecured creditors (Izagirre et al. 2019). In fact, customers could be of lower priority than many other creditors in the distribution of the EMI's assets and there is no guarantee they will

33 For more information on potential corrective measures and enforcement actions (albeit focused on banks), see BCBS (2015).

34 A market conduct regulatory and supervisory framework complements and supports the prudential perspective.

35 The international standards for resolution regimes are set by the Financial Stability Board's Key Attributes of Effective Resolution Regimes for Financial Institutions (FSB 2014). Additional guidance for bank resolution, some of which may apply to nonbanks, is provided by Bolzico, Mascaró, and Granata (2007).

36 This guide uses the term “resolution” in line with the definition provided by FSB (2014), according to which resolution includes liquidation. In many countries and jurisdictions (e.g., the E.U.), resolution is limited to the application of extraordinary tools such as bail-in, bridge bank, sale of assets, and the use of asset management companies. It excludes liquidation procedures.

37 An overview of fund safeguarding requirements can be found in Kerse and Staschen (2018), Dobler et al. (2021), and section 7.6 of Boeddu et al. (2021).

get money back. Strong supervision goes a long way in avoiding such situations, but failure can still occur among DFS providers and trigger a myriad of negative consequences (see [Box 10](#)).³⁸

In the absence of a specific resolution regime, authorities may have no option but to let DFS providers fall under the standard corporate insolvency regime. These regimes do not consider the particulars of FSPs, in particular entities that collect repayable funds from the public. It is important to ensure that failing DFS providers like EMIs can be resolved in an orderly manner and to guarantee prompt reimbursement of customer funds.

BOX 10. **The case of Wirecard**

The now defunct German payment services provider Wirecard became insolvent due to rampant internal fraud (Reuters 2021). In 2019 the company was processing millions in payments through approximately 280,000 partners across many countries, including as a member of the Visa and Mastercard networks. Wirecard was Germany's third largest financial group by stock value. Its collapse impacted a number of bank and nonbank partners offering banking and payment services (e.g., Pockit, Curve, CardOneMoney, Payoneer, Revolut, Soldo, BBVA-owned Holvi). As a result of the suspension of their accounts and bank cards, millions of customers were unable to access their funds, including paid-in salaries. External auditors faced legal suits for failing to flag improperly booked payments. Supervisory authorities were heavily criticized by politicians and society, and the case implicated Germany's top leadership. While Wirecard offered no systemic risk to Germany's financial sector, the undesirable consequences of its failure were far reaching.

Countries should have a resolution regime financial authorities can use to deal with DFS provider failures. The regime would aim to minimize the failure's negative impacts on customers, the real economy, financial stability, and taxpayers. It would include a resolution plan (FSB 2014) that equips a resolution authority³⁹ with unequivocal powers and a range of tools to deal with DFS providers that are no longer viable, or likely to be no longer viable, and whose failure may significantly impact policy goals—including, for instance, power and policies to transfer part or the total of a provider's operations to another provider in order to preserve critical functions and minimize disruptions.

When no specific resolution regime is in place for DFS providers, as is the case in most EMDEs, the legal power and related policies and plans to deal with failing DFS providers also does not exist. A DFS provider may need to go into ordinary liquidation under the country's general legal framework as it applies to nonfinancial companies. The process is usually lengthy and an inadequate way to reimburse customers, as the U.K. case in [Box 11](#) illustrates. While authorities may choose to liquidate smaller failing DFS providers, a specific regime would give them the option to call on other resolution powers when deemed necessary to curtail the broad negative repercussions of failure.

As the Wirecard case in [Box 10](#) illustrates, the failure of a large DFS provider (even one that does not take funds from the public) may not only impact customers but also other DFS providers and the reputation of the supervisor. A specific resolution regime would allow authorities to take the following actions, among others:

- Remove and replace senior management and directors of the DFS provider
- Appoint an administrator to take control of and manage the DFS provider
- Operate and resolve the DFS provider, including powers to terminate contracts, continue or assign

38 Gispert et al. (2022) provides examples of failures of DFS providers that involve fraud and misconduct.

39 In many EMDEs the resolution authority, which has the responsibility of leading the resolution process, is the supervisory authority itself. In others, the resolution authority is a separate body. Such a body may also manage the deposit insurance scheme and related funds. Resolution procedures usually only start when the supervisor or the resolution authority makes the declaration that a DFS provider has reached the "point of no viability" or similar trigger, depending on country context.

BOX 11. The FCA and insolvency in EMIs

Authorized payment institutions and EMIs in the U.K. are required to protect customer money via fund safeguarding (FCA 2022b). They either keep customer money separate from their own or protect it with insurance or a comparable guarantee. On its website, the FCA informs the general public that fund safeguarding may produce worse consumer outcomes than the past performance of the U.K.'s deposit insurance scheme. It may take longer for customers to get their funds back or there may be no funds left after the administrator or liquidator of an insolvent EMI deducts costs from the EMI's assets. Customers may not get their money back at all. The FCA also warns consumers that there is a chance that EMIs or authorized payment institutions may not properly safeguard customer funds. Moreover, in the case of a failure, customers may need to take the initiative to contact the administrator or liquidator to get their money back. These situations are especially inappropriate for EMDEs, where e-money is a major retail product used by a large portion of the population, including vulnerable individuals.

In the U.K., six authorized payment institutions and EMIs have entered insolvency since 2018. Only one has returned customer funds. Supercapital Ltd. was

one of the firms that became insolvent (FCA 2019). In September 2019, administrators were appointed to take control of the firm, including managing customer claims against it. The FCA advised that customers would need to contact the administrators to get their funds back. According to the administrators, Supercapital was short approximately £585,000 owed to customers. By 2020, the prospect of recovering these sums was uncertain (England and Wales High Court 2020). This shortfall would likely have been detected if the firm had in place effective reconciliation procedures as described in Dias and Staschen (2018a).

The Supercapital case demonstrates how crucial it is to ensure that regulations are in place for fund safeguarding, together with proper segregation requirements. Also due to the shortcomings of applying a general insolvency regime to financial institutions, the U.K. recently issued the Payment and Electronic Money Institution Insolvency Regulations, which introduce a special administrative regime for insolvent payment institutions and EMIs. The objective is to ensure that customers are reimbursed without delay and to minimize shortfalls in meeting the amounts they are owed (Lawrence et al. 2021).

contracts, purchase or sell assets, write down debt, and take any other action necessary to restructure or wind down operations

- Transfer or sell assets and liabilities, legal rights, and obligations to a solvent third party
- Transfer certain functions and viable operations of the failing DFS provider to another institution
- Effect the closure and orderly wind down of the whole or part of the DFS provider, with prompt access to customer accounts or funds (FSB 2014)

Effective DFS supervision supports the resolution process by, among other reasons, ensuring the availability of reliable information about the DFS provider. This helps accelerate the process and lower the costs and risks associated with failure. For instance, the supervisor may

have up-to-date and detailed information about the float accounts backing the EMI's operations, which is crucial to making prompt customer reimbursements.

4.8.2 DEPOSIT INSURANCE APPLIED TO E-MONEY

Many EMDEs lack a strong regulatory framework, effective supervision, and a special resolution regime for DFS providers. These weaknesses, compounded by the massive growth of e-money in EMDEs, including its adoption by more vulnerable low-income populations, have triggered the question of whether and how customer money with DFS providers could be insured and DFS providers could participate in a country's deposit insurance system. Izaguirre et al. (2019) discusses this complex topic, highlighting that the prevalent model for applying deposit insurance to e-money (namely the pass-through approach)

has yet to be tested in EMDEs. Where e-money is a major retail product, authorities may consider instituting a type of insurance mechanism akin to deposit insurance schemes that adds an extra layer of consumer protection. However, such mechanisms should not be a substitute for the need to improve the effectiveness of DFS supervision and to create a regime akin to bank resolution regimes for DFS providers.

4.9 Improving coordination and collaboration

Coordination and collaboration among departments within the financial supervisory authority or with domestic and foreign authorities is useful in any type of supervision. This section discusses why it is especially important in DFS supervision.

First, DFS supervision requires expertise in technology. As DFS is technology-driven, its supervision requires sporadic specialized IT inspections. The department in charge of DFS supervision may not have sufficient IT expertise, in which case it may rely on specialists from other supervisory departments. In the absence of specialist supervisors, the supervisors in charge of DFS may coordinate with the IT department for sporadic support. However, this arrangement is not ideal as IT departments often face competing priorities, may lack experience with inspections of regulated entities, and may lack knowledge of applicable regulatory frameworks. IT inspections are not often required and do not cover all DFS providers. Supervisors must plan carefully to optimize scarce IT resources, keeping in mind the risk profile of DFS providers as informed by the risk-based supervision approach.

DFS also blurs the lines of responsibility among financial supervisors. In addition to coordination with IT specialists, DFS supervision likely involves more than one supervisory area due to the various types of DFS providers, business models, and products. For instance, PSP and banking supervisors may coordinate on emerging issues in open finance (see [section 6.3](#)) such as low performance of APIs or lack of transparency in giving client consent for data sharing. Another aspect

finds some DFS products being sold as bundles, or one type of product under one supervisor's remit using a product under another's remit as a channel. In East and West Africa, for instance, mobile savings and insurance are usually distributed through mobile money accounts offered by different DFS providers. Coordination may be needed on an interdepartmental or interagency basis, depending on the country.

The link between prudential and market conduct supervision is another area that needs coordination. DFS brings many opportunities for improving consumer experience, value, and outcomes, especially for financially unserved and underserved individuals, such as more effective disclosure of costs and greater convenience. At the same time, DFS raises consumer protection concerns such as fraud, data misuse, and inadequate redress mechanisms (Chalwe-Mulenga et al. 2022; Boeddu et al. 2021). While a single authority may be responsible for both prudential and market conduct supervision, separate departments may undertake these two tasks. In a few countries (e.g., South Africa, U.K.), different authorities perform prudential and market conduct supervision. Both institutional models require a proper coordination mechanism.⁴⁰ Supervisors can also collaborate on implementing specific supervisory tools, such as market monitoring (Izaguirre et al. 2022), or design and commission research such as demand-side surveys and behavioral research.

AML/CFT concerns require coordination as well. One of the four basic regulatory enablers for DFS is a proportionate framework for DFS providers to implement risk-based customer due diligence (CDD), according to Staschen and Meagher (2018) and Meagher (2019). When disproportional or unclear, AML/CFT rules can become one of the most significant obstacles to a thriving inclusive DFS environment. It is fundamental that the authorities or departments involved in designing and enforcing AML/CFT regulations coordinate, considering the need to balance both AML/CFT and financial inclusion goals. For instance, collaborative CDD mechanisms (Lyman et al. 2019) carry potential benefits for DFS providers, customers, and supervisors

40 For guidance on developing a risk-based approach to market conduct supervision, see Gomes et al. (2022).

but have yet to be developed in most EMDEs, partially because they require interagency coordination.

Coordination may also be needed between financial and nonfinancial authorities such as telecommunications, competition, and data protection—for example, DFS providers owned by MNOs or that are themselves MNOs.⁴¹ Issues in the regulatory domains of telecommunications and competition can impact the financial sector, including fair access to, quality of, and pricing of USSD services by MNOs to different DFS providers (Soursourian and Plaitakis 2019). Data protection and privacy issues may also become prominent due to the extensive use of digital personal data in DFS. New approaches to data protection that are more appropriate for low-income segments may be needed (Medine and Murthy 2020). For better interagency collaboration and coordination, including the clarification of respective responsibilities over DFS providers, authorities could consider signing memoranda of understanding (MoUs) as a first step. Examples include the MoU between the Bank of Ghana and the National Communications Authority (AFI 2017) and the MoU between the Reserve Bank of Malawi (RBM) and the Malawi Communications Regulatory Authority (RBM 2013).

Finally, international cooperation and peer learning can help supervisors improve DFS supervision. Many DFS providers operate on a regional or global level. In such cases, supervisors should have cross-border collaboration agreements with other supervisors to access relevant information from the provider's home country and vice versa. Moreover, peer learning can be extremely valuable for EMDE supervisors in areas such as experimenting with suptech and dealing with open finance and modularization. One opportunity for peer learning is the Global Financial Innovation Network (GFIN), a network of financial authorities supporting innovation. GFIN organizes research and exchange events focused on cutting-edge regulatory and supervisory issues. The Alliance for Financial Inclusion (AFI), a network of financial authorities that supports the financial inclusion agenda, offers another peer learning opportunity.

41 As noted in [section 3.2.1](#), BCBS (2016) recommends that the e-money issuing business be isolated in a separate legal entity rather than performed by a nonfinancial firm like an MNO.

CHAPTER 5

OVERCOMING IMPLEMENTATION CHALLENGES

SUPERVISORS IN VARIOUS EMDES face some common challenges that may be structural or internal in nature. In order to address them, supervisors must actively identify the root of each problem, devise solutions, and push for implementation. While it may not be possible to address all challenges at once or within a short timeframe, supervisors should strive to identify challenges, potential solutions, and the key stakeholders involved. With a better understanding of their relative priority and how challenges could be addressed, supervisors can negotiate gradual, realistic steps to overcome them. This chapter discusses and provides guidance on overcoming several of the challenges EMDE supervisors face (see [Figure 11](#)).

5.1 Structural challenges

Structural challenges relate to the broader environment affecting the supervisory authority, including issues such as:

- Inadequate legal mandate
- Mandate that overlaps with other authorities
- Inadequate enforcement powers or tools
- Inadequate legal protection for supervisors
- Inappropriate regulatory perimeter (e.g., regulation does not cover all relevant types of DFS providers; perimeter is too encompassing and strains supervisory resources)
- Interference or lobby by politicians and industry bodies
- Deficient interagency coordination

FIGURE 11. **Common challenges faced by supervisors in EMDEs**



- Legal limitations on human resources (e.g., hiring process, salary)
- Insufficient budget

Structural challenges are external and need to be addressed by bringing in external stakeholders. They are usually more difficult to resolve than internal challenges, not least because they often involve the legal framework that underpins DFS supervision and thorny budgetary questions. For instance, adequate enforcement powers require clear legal mandates and, within the law, clarity is about the power to use a range of enforcement tools for prudential and market conduct supervision of DFS providers. The same applies to the challenge DFS introduce regarding legal mandates and the regulatory perimeter. Some DFS providers and DFS activities may not clearly fit the existing regulatory and supervisory scope or cut across the remit of different authorities (e.g., payments authorities, banking supervisors). The regulatory perimeter could also be so encompassing that it strains supervisory capacity. These challenges may require both legal reform and interagency coordination (see [section 4.9](#)).

Solving challenges that involve external stakeholders and their own competing priorities requires constant interagency coordination and dialogue. For instance, many rounds of discussion may be required to convince government agencies of the importance of increasing the budget or reforming the funding model of a supervisory authority in charge of DFS supervision to improve data (see [section 4.6](#)) and retain qualified staff. The supervisor may need to prepare well-structured arguments about the importance of DFS supervision and how quality data and qualified staff influence outcomes. Supervisors should also anticipate stakeholder counterarguments, including their competing priorities and resistance to change.

5.2 Internal challenges

Internal challenges to the supervisory authority include:

- Complex or inadequate organizational structure (see [section 3.2.2](#))
- Inadequate supervisory capacity (e.g., expertise, skills, data, technology, internal budget allocation)
- Inadequate organizational culture (e.g., lack of managerial support for a risk-based supervisory approach)
- Ineffective interdepartmental coordination (see [section 4.9](#))
- Inadequately balanced policy goals

To elaborate on the final bullet above, many supervisors in EMDEs are challenged by an expanded mandate that covers multiple policy goals such as financial consumer protection, competition, financial inclusion, safety and soundness of financial institutions, financial stability, and safety of the NPS.⁴² Balancing these policy goals can be challenging. In addition to constant coordination and dialogue with key stakeholders (e.g., other supervisors), supervisors may also implement a structured approach for managing the complex interplay among policy goals such as the I-SIP Approach.⁴³

Internal challenges such as poor quality data may result from external factors (see [section 5.1](#)), including insufficient budget for the supervisory authority. Yet challenges may exist even in the absence of external factors. For instance, in the face of quickly growing and changing DFS markets, the supervisor may fail to recognize the need to provide additional staff training or prioritize improving supervisory data (see [section 4.6](#)). This section provides guidance on one of the major internal challenges supervisors in EMDEs face: supervisory capacity.

⁴² See Kirakul et al. (2021) for a discussion and country examples on a range of financial authority mandates and responsibilities.

⁴³ The main idea of the I-SIP Approach is to identify linkages between four key financial sector policy objectives (i.e., inclusion, stability, integrity, and protection) and manage these linkages to design policies that lead to improved outcomes, where synergies between these objectives are maximized and any trade-offs or negative outcomes are avoided or minimized (Tomilova and Valenzuela 2018).

5.2.1 RAMPING UP SUPERVISORY CAPACITY

Adequate supervisory capacity entails having the necessary resources at appropriate levels to ensure that supervisory responsibilities can be effectively and efficiently carried out. “Resources” includes human resources with the right expertise and skills (see [section 3.2.2.1](#)) but also data and technology—all of which are enabled by sufficient budget (see [Figure 12](#)).

5.2.1.1 Internal budget allocation

In discussions of supervisory capacity in EMDEs, one issue that receives less attention than it deserves is internal allocation of the budget assigned to the financial authority. Without budget it is often impossible to significantly improve capacity in terms of staff numbers, specialized expertise, and supervisory skills. While budget constraints for DFS supervision may be a direct consequence of the overall inadequate budget of the supervisory authority, internal budget allocation between departments can be an issue as well. As with other authority functions, DFS supervision requires adequate financial resources—not only for investments such as improving supervisory data (see [section 4.6](#)) but to effectively discharge core functions such as conducting ongoing offsite monitoring (see [section 4.5](#)).

Budget allocation depends on the internal organization for DFS supervision (see [section 3.2.2](#)). In most authorities, DFS supervision cuts across multiple departments (e.g., market conduct supervision,

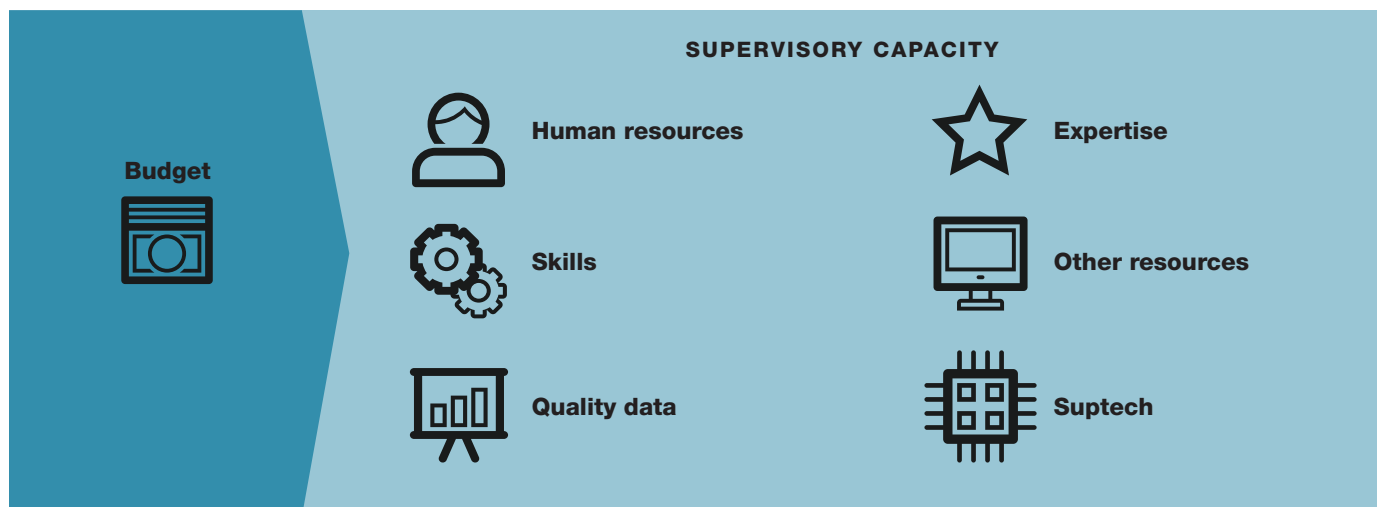
nonbank prudential supervision, payments supervision). Regardless of the chosen internal organization, it is important that all functions involved in DFS supervision receive adequate budget. Bank prudential supervision usually receives more than other supervisory areas. However, budget needs to be effectively reallocated as the importance of nonbank DFS providers increases in terms of number of providers and customers served. Internal negotiations are necessary to achieve a balance in budget allocation. The presence of a central unit for strategic planning can facilitate the process.

5.2.1.2 Improving expertise and skills

A core requirement for effective risk-based DFS supervision is adequate numbers of qualified staff members with an appropriate range of expertise and skills (see [section 3.2.2.1](#))—rarely available in EMDEs from the start. When a new team is formed, new staff members that are externally recruited, in particular, need to go through a period of classroom and on-the-job training to build expertise and, specifically, supervisory skills.

DFS expertise is not the only important qualification. New and even existing staff members often need to learn how to become good supervisors in general. All supervisors need audit, persuasion, interview, and communication skills to effectively undertake supervisory tasks. For example, they need the self-confidence to interact with senior executives of DFS providers, particularly when communicating supervisory judgment

FIGURE 12. **Supervisory capacity depends on adequate budget**



about poor practices. This type of skill is known as a soft skill. Soft skills differ from technical knowledge, which tends to receive much more attention in capacity building efforts by supervisory authorities in EMDEs. Skills development and knowledge development should receive equal attention.⁴⁴

For both knowledge and soft skills, new recruits can benefit from classroom and on-the-job training delivered by more experienced supervisors from their same or other departments and from external resources. Supervisors may also benefit from engagement with peers in other countries to learn how they have developed internal capacity and complemented training and skills development with new approaches to risk-based supervision. Peer engagement (see [section 4.9](#)) can be remote (e.g., email, video conferencing) or via country visits and participation in international events. An additional way to improve DFS expertise is to invest in an innovation facilitator, such as an innovation office, to foster supervisory engagement with and learning from DFS innovators (UNSGSA FinTech Working Group and CCAF 2019).

External resources such as independent auditors and other experts may be engaged to conduct supervisory activities on behalf of the supervisor and to deliver trainings. When an external resource is hired to conduct a specific supervisory task, it is important that the supervisory authority ensure an explicit commitment has been made and a mechanism to transfer knowledge and expertise to supervisory staff has been set up. This could include direct technical assistance such as on-the-job training, guidance development, mock inspections, role playing, case studies, support for supervisory planning, and group discussions of supervisory findings. In all cases, the use of an external party should be seen as a temporary mitigation measure. It should not substitute for the need to build internal expertise and skills.

Finally, to hire and retain good professionals, supervisory authorities need to offer competitive remuneration packages and career development. Data scientists, statisticians and mathematicians, data engineers, cybersecurity experts, financial analysts, fintech business experts, and other professionals may be in high demand in the private sector, which competes with supervisory authorities. Unfortunately, external factors such as the law under which a supervisory authority operates may impose limitations on the hiring process, remuneration, and staff promotion. Supervisors should still identify any challenges in staff hiring and retention that could be internally addressed while external factors remain.

⁴⁴ The adoption of RBS itself requires proper training so staff acquires the right knowledge and skills. Institutions providing risk-based supervision training to financial supervisors in EMDEs include the International Monetary Fund, the World Bank, and the Toronto Centre.

CHAPTER 6

ADDRESSING EMERGING ISSUES IN DFS SUPERVISION

DFS MARKETS ARE CHANGING FAST and disruptive innovations hold implications for supervisors. However, there is still not enough global supervisory experience with some developments nor consensus on which regulatory approach best suits them. CGAP has performed research on how DFS regulators and supervisors have encouraged and monitored disruptive innovation, such as by setting up innovation facilitators (Jenik and Duff 2020) and conducting market monitoring (Izaguirre et al. 2022). CGAP has also begun research on new approaches to regulatory architecture to deal with disruptive innovation.⁴⁵ However, it is generally too early to provide supervisors with guidance on this issue.

This chapter aims to help supervisors in EMDEs understand how certain key types of disruptive innovation could impact their work. The innovations included in this chapter—cloud computing, modularization, open finance, and artificial intelligence and machine learning—have been chosen for their direct relevance to financial inclusion. Rather than providing definitive guidance, the focus is on raising awareness among EMDE supervisors about the potential supervisory implications of these innovations.⁴⁶

6.1 Cloud computing

6.1.1 WHY DOES IT MATTER?

Cloud computing impacts both DFS providers and traditional banks and other institutions. It is at the center of many DFS innovations (Dias and Izaguirre 2019). By pooling resources, cloud computing allows DFS providers to avoid heavy investment in IT resources and expertise, dramatically reducing entry and operating costs. In many markets this has led to greater competition and innovation. Cloud computing also supports inclusive innovation by increasing flexibility and scalability of operations and allowing innovation on product design and delivery. Additionally, cloud services can improve cyber security risk management because large cloud services providers (CSPs) have deep pockets to invest in state-of-the-art cyber defense, plus the ability to spread risk across multiple sectors and even jurisdictions. But what are the risks and trade-offs supervisors need to pay attention to? This section discusses some of the main supervisory implications of cloud computing.

6.1.2 SUPERVISORY IMPLICATIONS

The use of cloud computing in DFS usually involves outsourcing to CSPs. The relevance of outsourcing can vary from minimal to highly significant, depending on services contracted by the DFS provider. Cloud services

⁴⁵ CGAP continues its research into regulatory approaches to disruptive innovations and may issue guidance for DFS regulators and supervisors.

⁴⁶ See World Bank (2021) for country examples of innovation regulation.

can vary from basic infrastructure (e.g., storage) to provision of software and applications that are crucial to the DFS provider's operations. CSP services can also vary in the level of CSP infrastructure sharing among fewer or more CSP clients—from public cloud to hybrid, community, and private cloud. The content and level of infrastructure sharing in outsourcing impacts the DFS provider's level of dependency on the CSP (FSB 2019). Dependency on third parties such as CSPs brings a host of supervisory concerns. DFS providers may have reduced ability to identify, manage, and mitigate the risks of outsourced activities (FSB 2020b). In addition to the benefits and risks CSPs may create for individual DFS providers, large CSPs may impact the whole DFS market and beyond. Hence, CSPs can be a source of systemic risk.

As large-scale use of cloud computing becomes ever more common, it leads to the question of whether general outsourcing regulations remain adequate to address supervisory concerns, particularly for large, internationally active CSPs, most of which are based in the United States and China. Examples of recent reforms to better deal with significant cloud outsourcing include the updated Guidelines on outsourcing arrangements by the European Banking Authority (EBA 2019), the pan-European decision to impose requirements and supervisory arrangements directly on CSPs—now considered “critical third parties” in many economic sectors (European Council 2022), and the U.K.'s move to directly regulate and oversee CSPs in the financial sector as critical third parties (HM Treasury 2022). The next section reviews a few concerns raised by outsourcing to CSPs, some of which are being addressed by the aforementioned regulatory reforms.

6.1.2.1 Management of outsourcing risks by DFS providers

DFS providers are expected to conduct due diligence and monitor CSPs as per general outsourcing guidelines. The DFS provider is usually legally responsible for the regulatory compliance and actions of a CSP contracted within the scope of an agreement between the DFS provider and the CSP. However, the existing regulatory framework in EMDEs may not require a DFS provider to

notify the supervisor or apply for authorization when they engage in significant outsourcing.⁴⁷ Thus, the supervisor may not be able to make an early assessment of a provider's capacity to identify, measure, and manage the risks of cloud outsourcing and their ability to assess the CSP's own risk management practices. Potential supervisory mitigants to the lack of DFS provider capacity to assess CSPs are to:

- Require DFS providers to apply for authorization for material cloud outsourcing, giving the supervisor an opportunity to probe into the application, including questions about related issues such as business continuity (see [section 6.1.2.3](#)) and exit strategies
- Allow pooled audits organized by smaller DFS providers that use the same CSP and third-party certifications of CSPs by experts or supervisor-recognized organizations

6.1.2.2 The supervisor's audit and access rights

As with other types of outsourcing, supervisors usually require the right to access CSP data and facilities to conduct audits remotely and physically, including in the event of CSP or DFS provider failure. Audit and access rights are fundamental (BaFin 2018), thus traditional financial services outsourcing contracts have clauses to that effect. However, large CSPs use standard form contracts that do not always ensure the supervisor's audit and access rights, sometimes due to concerns about the privacy of other clients whose data share the same CSP physical infrastructure. Supervisors may face obstacles such as physically reaching data center locations (potentially in multiple countries), lack of experience in analyzing CSP contracts, or lack of clout to influence contractual changes by large CSPs. Further, distribution and movement of data across jurisdictions may challenge the supervisor's access to the data, creating data sovereignty and legal risks (Dias 2020). Potential supervisory mitigants include:

- Third-party CSP certifications or audits by duly recognized specialists or organizations

⁴⁷ The definition of significant or material outsourcing varies across countries according to local regulations.

- Amending outsourcing regulations to impose minimum contractual clauses to guarantee the supervisor’s audit and access rights, and the power to impose additional requirements to outsourcing arrangements (e.g., characteristics of countries where data can be located, maximum time for CSPs to respond to supervisory requests for data and remote access)
- Direct regulation and supervision of critical CSPs: “criticality” would need to be defined in regulation as per the previously discussed examples of new European and British regulations

6.1.2.3 DFS providers’ business continuity

Many DFS providers outsource critical functions to CSPs. CSP operational disruptions, data breaches, and other problems could have an impact on their business continuity. Financial regulations usually require providers to have business continuity plans that include measures to mitigate the risk of outsourcing. These include contingency plans (e.g., what to do in case of a major event such as a power outage or system hack) and exit strategies that allow the DFS provider to terminate outsourcing arrangements while avoiding operational disruption. However, cloud outsourcing brings challenges. For example, vendor lock-in may occur due to contractual or practical reasons (Dias 2020). A potential lack of alternative CSPs to take over outsourced activities and the technical inability of DFS providers to (re)absorb such activities can hamper business continuity and exit strategies and lead to vendor lock-in. Also, data portability in cloud computing is most often not immediately possible, making it harder to exit a contract to move services to another CSP. Further, cross-country inconsistencies in data protection legislation could make it difficult for globally active DFS providers to use CSPs in different jurisdictions, which could increase operational resilience when data portability becomes possible. Potential mitigants include:

- Prohibit, by regulation, vendor lock-in contractual clauses

- Depending on the situation (e.g., a large, systemic DFS provider outsourcing critical functions), require a multi-CSP or multi-cloud strategy—an arrangement that mixes public, private, and hybrid cloud services but also imposes higher provider costs
- Encourage or impose (if CSPs are directly regulated) data interoperability and portability across CSPs through the use of common data standards or other methods that ensure interoperability of varying standards

It is not recommended to impose strict authorization requirements on all cloud outsourcing due to the potentially adverse effects on innovation and data security. It also drains supervisory capacity. Authorization and reporting requirements should be proportionate to the materiality (significance) of outsourcing. Regulation should require DFS providers to assess the level of materiality of all outsourcing they engage in.

6.1.2.4 Systemic implications

The global cloud computing market is highly concentrated on a handful of CSPs from the United States and China. Many countries replicate this global concentration. For instance, the Bank of England found that “over 65 percent of the U.K. firms used the same four CSPs for cloud infrastructure services” (HM Treasury 2022). On one hand, concentration leads to risks in stability, including through increased interconnectedness among otherwise unrelated financial institutions. A major disruption at a large CSP is a possible source of systemic risk because the CSP becomes a single point of failure. Vendor lock-in and lack of data interoperability/portability exacerbate this risk. On the other hand, large CSPs usually have advanced tools to mitigate cyber security, redundancy, failover,⁴⁸ and other risks, and offer additional services that require deep pockets and processing power such as sophisticated artificial intelligence (AI). Compared to most DFS providers, economies of scale would also allow large CSPs to achieve mitigation less expensively in terms of unit cost. Regulators and supervisors therefore need to clearly understand the services large CSPs offer DFS providers

⁴⁸ Failover is a procedure by which a system automatically transfers control to a duplicate system when it detects a fault or failure.

and other regulated entities in order to understand how such services may change systemic risks.

There is limited experience so far in dealing with the systemic issues raised by CSP concentration, despite new regulatory approach in the E.U. and the U.K.

Nevertheless, supervisors may choose to consider the following steps (Dias 2020):

- Discuss strategies, risk management practices, and business continuity plans related to material cloud outsourcing with senior management at systemic or otherwise relevant DFS providers
- Conduct a survey on cloud outsourcing in relevant markets to map main CSPs, major sub-contractors, and outsourced activities under each type of cloud service model. This could help assess the levels of CSP concentration and interconnection of DFS providers and other financial institutions through CSPs. Mapping could also identify which cloud outsourcing practices and associated risks are most present in DFS providers serving low-income and underserved customers

6.2 Modularization

6.2.1 WHY DOES IT MATTER?

DFS providers increasingly leverage specialized third-party providers that perform specific tasks, activities, or processes, often on a plug-and-play or pay-per-use basis (Zetterli 2021). For example, many DFS providers leverage digital onboarding providers to seamlessly manage remote customer onboarding or use third-party credit scoring models based on AI to target customers with limited or no credit history. Others “borrow” a bank’s license to offer simple banking services.

While outsourcing is not new, modularization is a recent development. It can be defined as the unbundling of value chains in delivering financial services. With modularization, a substantial number of specialized providers are seamlessly involved in meeting customer demand and preferences, operating both on the front and

back end (Zetterli 2021; CPMI 2014). Modularization enables customers to use a greater number of providers for different products, services, and needs. Customers are often unaware of modularization but may experience its positive effects, for example:

- Increased competition from technology-enabled business models that reduces end user prices
- New technological capabilities and intense customer-centricity of DFS providers that leads to better customer experience (e.g., simpler uptake, easier use)
- A growing range of increasingly specialized DFS providers that results in products that are better tailored to different customers’ varying needs
- New products and services—possibly bundled in novel combinations—that create new sources of value

While traditional businesses also use modularization, its greatest inclusion potential is in powering new types of business models by new market entrants. One is the marketplace model, where customers compare and combine services from different DFS providers using a one-stop shop (the “marketplace”) instead of being restricted to the product offerings of a single DFS provider.⁴⁹

Banking-as-a-service (BaaS) models enable any business to offer banking services—without the need for a banking license—by partnering with a licensed bank that operates in the background. This dramatically reduces entry barriers for nonbanks, their time-to-market, and operating costs. Legally, banking operations are conducted by the bank, not the DFS provider. The DFS provider accesses the bank’s BaaS platform via APIs and can select and tailor the banking services it wants to offer its customers. Solarisbank (Europe), Banco Original (Brazil), Vodeno (Poland), and Green Dot (United States) are examples of banks offering BaaS services (Mdluli et al. 2022). Solarisbank has more than 90 clients, including DFS providers (e.g., Coinbase, Kontist, Penta, Tomorrow, Vivid). As one of Solarisbank’s clients, Kontist offers bank accounts to freelancers and the self-employed. Its clients interact exclusively with Kontist, not Solarisbank.

⁴⁹ A notable example is XP Investimentos, a multi-provider investment platform in Brazil that has transformed the country’s investment business. After only a few years in operation, XP has become the largest investment platform in Brazil.

These new models present a range of supervisory implications, some of which may require changes to regulatory and supervisory frameworks. The following section discusses several of them.

6.2.2 SUPERVISORY IMPLICATIONS

6.2.2.1 Larger number and greater depth of third-party relationships

Modularization means a growing web of third-party relationships in the financial sector. This impacts the risk profile of individual DFS providers but it may also change systemic risks. The use of a high number of third parties by DFS providers makes it more difficult for DFS providers to identify, manage, and mitigate the risks of activities outsourced to third parties (see similar concerns with cloud outsourcing in [section 6.1](#)). The potentially limited ability of DFS providers to manage the risks of third-party relationships is particularly important when third parties perform critical functions (e.g., provide the core account system).

In the BaaS model, multiple nonbanks use a licensed bank: the BaaS provider. This raises issues for bank supervisors, such as cyber risks, data leakages, reputational risk, and operational disruption. All parties involved in the BaaS model should have a proper cybersecurity framework along with business continuity, recovery, and disaster response plans. Contractual agreements among parties should allow DFS providers to conduct risk assessments and oversight on the third party and guarantee the supervisor audit and access rights.

In addition to the difficulties involved in managing a larger number of third-party relationships, DFS providers may lack the necessary expertise to assess the risks of outsourcing and other types of partnerships. Supervisors should make a judgment call on the ability of large or otherwise relevant DFS providers to perform such risk assessments. DFS providers should also have in place effective third-party risk management procedures, including appropriate due diligence, as part of the operational risk management framework (BCBS 2021). This potentially includes the use of specialized auditors in cases where the DFS provider lacks expertise. As [section](#)

[6.1](#) on cloud computing highlights, prior authorization for and reporting of material outsourcing may be required.

6.2.2.2 Perimeter questions

One of the questions in modularization is where risk and liability reside. A fragmented value chain creates confusion about who is ultimately accountable to supervisors and customers (Feyen et al. 2022). Who should be regulated and supervised—and how? Specifically in BaaS, who is really the third party: the bank or the DFS provider using BaaS? In BaaS, the customer relationship (legally held by the bank since the DFS provider is not licensed to provide banking services) is completely outsourced—from product design to customer service. Still, the bank would be held liable before the supervisor for the actions and omissions of third parties. However, outsourcing works the other way around from the perspective of the DFS provider using BaaS. Knowing that the bank has strict regulatory compliance obligations, the DFS provider may have limited incentive to effectively manage risks, including consumer risks. Bank supervisors and supervisors of DFS providers should coordinate to devise approaches to supervise BaaS, including knowledge exchange with peers in other countries.

6.2.2.3 Systemic implications

The growing reliance of multiple DFS providers on the same set of third-party providers to perform critical functions can create significantly concentrated risk across the financial sector. The failure of a specific third party could have significant impact on multiple DFS providers, including their failure due to major operational disruptions. The situation may create contagion risk, which may lead to the failure of other DFS providers, including incumbents, or even other types of FSPs. In addition, big techs increasingly collaborate with banks and DFS providers to offer financial services without having to obtain a license. Some big techs use multiple banks and DFS providers that may also use services provided by the big tech (e.g., cloud-computing, data analytics services). Relationships that go in both directions increase interdependencies between parties (Crisanto et al. 2022). The systemic implications of these relationships are similar to issues discussed in the context of cloud outsourcing in [section 6.1](#).

6.3 Open finance

6.3.1 WHY DOES IT MATTER?

CGAP defines open banking regimes as consent-based data-sharing schemes that are mandated or supported by regulators with the goal of creating competition and fostering innovation (Plaitakis and Staschen 2020). While the purpose of open banking is to make consumer data held by banks available to others, the goal of open finance is to reciprocally share consumer data held by a wider set of FSPs, including DFS providers. The institution holding the data is called the data holder; the one requesting and using the data is called the data user. DFS providers can be both data holders and data users. Participants in the open banking/finance scheme are subject to rules such as registration and technical and security standards. In addition to data sharing, open finance may include functionalities such as payment initiation: enabling a data user to offer services that require moving customer funds from accounts held in third-parties, such as banks. However, this is not enabled everywhere.

Designing and implementing open finance regimes is a new area for most countries, including EMDEs. Most regimes in EMDEs are in their first years of implementation (e.g., Brazil, Colombia, Indonesia, Mexico, Nigeria, Philippines, South Africa). After years of experience with open banking, U.K. authorities are designing its expansion to open finance and planning for open data (DBEIS 2021).⁵⁰ Australia is already implementing its ambitious agenda for open data based on an overarching consumer data rights law (ACCC 2022).

Open finance offers the potential for DFS providers to take advantage of the wealth of digital data that customers create across the financial sector. Uses for the data include improving product design, customization (e.g., financial advice), improving risk assessments (e.g., credit, insurance), building price comparison tools, and helping customers switch providers. Open finance can ultimately advance financial inclusion in seven ways:

1. Smoothing volatile incomes
2. Lowering tariffs on household bills

3. Overcoming lack of documentation
4. Encouraging healthy financial behaviors
5. Responsibly expanding access to credit
6. Supporting debt rehabilitation services
7. Reducing reliance on overdrafts and other excessively priced credit products (Staschen and Plaitakis 2020)

6.3.2 SUPERVISORY IMPLICATIONS

Since supervisors may get involved in the implementation of open finance, they need to understand its basic mechanics. There is wide variation in country approaches but the basis of most regimes is the required use of standard APIs to facilitate data sharing and a process to authenticate participants before the data flow from holder to user. Participants that are not regulated by the financial authority need to show they comply with minimum qualification requirements, such as cybersecurity defenses, through an accreditation process. In some cases, like in Brazil, unregulated entities cannot directly participate in the data sharing scheme.

The scheme may be governed by a private body (e.g., U.K.) or a government body (e.g., Australia). The body may be responsible for key functions, including:

- Maintaining a directory of participants (data holders and data users)
- Accrediting new participants (ensuring they comply with minimum requirements)
- Authenticating data users requesting data before the data holder transfers the data
- Setting data privacy, consent, and user experience standards
- Setting and monitoring API performance (e.g., availability of APIs to data users, speed in responding to data requests)
- Setting up a redress mechanism to resolve disputes among scheme participants
- Taking enforcement action against participants that breach scheme rules

⁵⁰ Open data would be the sharing of consumer data held by institutions of a broader range of economic sectors, including financial institutions, utility providers, health service providers, and telecoms.

BOX 12. Performance indicators of open banking in the U.K.

The figures in the charts below are examples from the U.K. of what monitoring API performance could mean for a supervisor eventually charged with this function. Chart 1 shows the average availability of bank APIs and Chart 2 shows the number of successful API calls made by data users. Successful API calls are defined as those where a bank fulfills a data user’s request for data sharing.

These and other indicators disaggregated by data holder are published online by the Open Banking Implementation Entity (OBIE). Dissemination can help promote market transparency and empower consumers with information about service quality.

FIGURE 13. Unweighted average API availability of account providers’ open banking APIs (September 2020–September 2022)

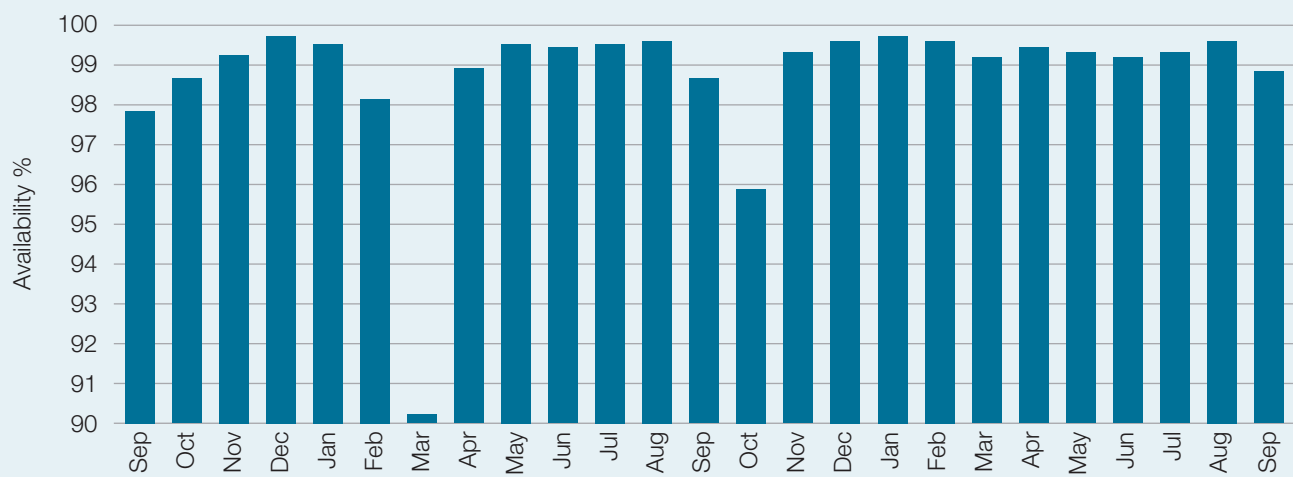
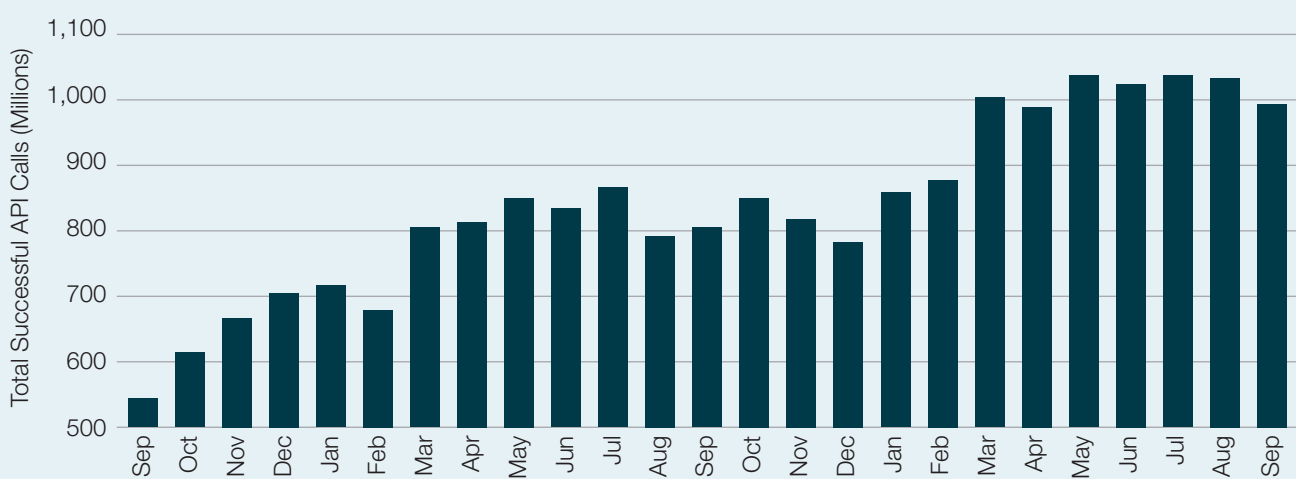


FIGURE 14. Successful API calls made by third parties using account providers’ open banking APIs (September 2020–September 2022)



Source: OBIE 2022.

It is unclear to which extent supervisors may get involved in the implementation of open finance regimes, particularly the functions listed above. Their role depends on regulatory design: the more that is set by regulation (e.g., accreditation requirements for participants, minimum API performance standards), the greater the chance they may need to be involved. For instance, the supervisor may be responsible for accrediting participants and monitoring API performance of DFS providers (see an example of performance indicators in [Box 12](#)). In Brazil, the central bank's regulatory and supervisory departments are both currently monitoring API performance via a dashboard made available by the governing body. The supervisor may also become involved in consumer issues, such as financial losses derived from open finance products involving payment initiation services.

It is important that regulators designing open finance regimes closely coordinate with supervisors before deciding upon charging the supervisor with implementation functions. They should also discuss potential impacts on supervision, licensing, and accreditation, particularly if new types of entities are added to the supervisory scope (e.g., payment initiation service providers, account service providers). New responsibilities and an expanded perimeter may require skills, knowledge, and resources that supervisors currently lack.⁵¹

6.4 The use of artificial intelligence and machine learning

6.4.1 WHY DOES IT MATTER?

Artificial intelligence can be described as a system that displays intelligent behavior by analyzing its environment and taking actions—with some degree of autonomy—to accomplish predetermined goals (EC 2018). Machine learning (ML) is a field within AI where algorithms leverage data to build and modify models to perform a

set of tasks. DFS providers increasingly leverage ML to automate customer service processes, customize product offerings to different segments, assess borrower credit risk, and perform other tasks. ML enables DFS providers to analyze and harness a wide range of sources and types of alternative data that go beyond traditional financial sector data to monitor customer behavior in real time, among other tasks. Service differentiation can also help DFS providers become more competitive and increase their market share.

One common use of ML is in credit scoring models. It can be challenging to use structured, historical credit data on customer loans, payments, and financial transactions to estimate creditworthiness of low-income customers who possess little or no financial sector history. DFS providers use new credit scoring models that employ ML to process alternative data from different sources and in different formats. Examples include data from utility bills, mobile phones, and satellite information which, in conjunction (or not) with traditional credit history data, can estimate creditworthiness.⁵² DFS providers use these models to make automated credit decisions in seconds. This development is highly relevant to financial inclusion as it enables individuals with little or no credit history to access credit. It helps DFS providers compete in credit markets and reduces the costs of assessing credit risks for low-value loans, which could be prohibitive when using traditional risk assessment methods. DFS providers in Brazil, for instance, use these types of scoring models to lend to consumers rejected by banks. (Practitioners estimate that banks reject over 70 percent of all retail loan applications.)⁵³

6.4.2 SUPERVISORY IMPLICATIONS

6.4.2.1 Unfair discrimination

An increasing concern around the use of AI and ML in financial services is whether algorithms can lead to or exacerbate unfair discrimination against specific customer groups based on gender, ethnicity, place of residence, age, race, or sexual orientation. While algorithms are useful in

51 In this context it is worth mentioning the case of India. In 2018, the Reserve Bank of India created the account aggregator (AA) system to simplify consent-based data exchange. AAs are regulated as nonbank financial companies licensed exclusively to act as data intermediaries. They sit between data holders and data users to facilitate data exchange (Datwani and Raman 2020).

52 For examples of these data types, see Kelly and Mirpourian (2021).

53 According to CGAP interviews with fintech firms in Brazil.

customizing the offering of tailored products or services to different customer segments, of key concern is whether such decisions unfairly disadvantage certain customers (IIF 2021a). Credit decision-making is one area of special concern. Well-designed and managed algorithms can more effectively and efficiently make accurate and fair predictions than more manual methods (IIF 2021b). “Well-designed and managed” includes human intervention to reduce the risk of unfair discrimination, including gender-based discrimination, and algorithm errors that could increase consumer and prudential risks (Prenio and Yong 2021).

The use of complex algorithms based on AI and ML could introduce or exacerbate unfair biases in credit decisions due to historical biases reflected in the data the algorithm uses (input data), biases created by the algorithm itself, or biases introduced via human intervention. For instance, an algorithm may rate a customer from an ethnic group as at higher risk of default because historically customers

from that group have thinner credit histories due to lower levels of bank access. Some scoring models mitigate the risk of unfair discrimination by excluding data on sensitive attributes like race, ethnicity, religion, sexual orientation, and gender. The lender may also correct for biases in algorithm outputs via human intervention based on a clear policy and predetermined procedures to avoid unfair discrimination. This can be useful even in an ex ante effort to correct input data because AI models may use proxies for certain attributes. Proxies for gender, sexual orientation, and other attributes include mobile phone models, mobile phone apps installed, zip codes, and social media contacts. It becomes clear that providers need robust AI model risk management. There is an emerging body of principles, guidance, and, less often, regulations addressing AI model governance in the financial sector (see [Box 13](#)). However, supervisory practice is still limited (Prenio and Yong 2021).

BOX 13. **Examples of rules and principles for the responsible use of AI**

The **European Commission** has proposed rules and actions to guarantee the safety and fundamental rights of people and businesses while strengthening AI uptake, investment, and innovation across the E.U. The proposed framework follows a risk-based approach and differentiates AI use according to whether it creates unacceptable, high, or low risk. As per the proposed rules, prior to taking a model to market, businesses or public authorities that develop or use AI applications that constitute a high risk for the safety or fundamental rights of citizens would have to comply with specific requirements and obligations, including an adequate risk management system, appropriate data governance and management practice, traceability of results, provision of adequate information about the AI system to end users, guarantee of a high level of security, and adequate human oversight. AI systems used to produce credit scores or evaluate creditworthiness of natural persons should be classified as high risk since they may lead to discrimination of people or groups, perpetuate historical patterns of discrimination, or create new forms of discriminatory impacts (EC 2021).

The **Hong Kong Monetary Authority** recently published guiding principles on consumer protection with respect to the use of big data, analytics, and AI that aim to support their healthy development in the banking industry and enhance customer confidence in using services that adopt these technologies. The guiding principles focus on governance and accountability, fairness, transparency, disclosure, and data privacy and protection (HKMA 2019).

The **Monetary Authority of Singapore** issued the Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector. The principles were developed in consultation with the industry and close coordination between MAS and the authorities responsible for data protection and communications. They complement previously existing principles and regulations for internal governance frameworks and must be applied and calibrated according to the materiality of the different AI models used by financial institutions (MAS 2018).

6.4.2.2 Potential lack of transparency in ML models

Some ML models lack transparency and “explainability,” which refers to the ability of a provider to explain the outputs of an ML model. However, EMDEs often experience less developed regulation and oversight of this issue and other issues involving ML. For instance, providers may not be required to disclose which types of data they use in credit scoring. Credit scoring and other models may also be developed and maintained by a third party that treats a model and the data it uses as its intellectual property, potentially imposing obstacles for transparency, accountability, risk management, and supervision. Black box ML models are another issue (i.e., the provider is unable to explain how the algorithm works). The World Bank and the International Committee on Credit Reporting (ICCR) highlight the risk of model opaqueness in credit scoring (World Bank and ICCR 2019). However, not all ML models fall into the black box category, and explainability is a matter of model design. It could therefore be argued that ML

BOX 14. ECB oversight of the use of third-party AI providers

The **European Central Bank’s** guide to assessments of fintech credit institution license applications highlights the following: if a fintech credit institution uses credit scores provided by a third-party vendor (outsourced credit scoring) and the vendor uses alternative data sources to build scorecards, the ECB and competent national authorities would assess the adequacy of the institution’s risk controls. Aspects they would consider include whether outsourcing risks are adequately managed and whether the credit-scoring process and data sources are properly documented and understood throughout the institution. The assessment would also consider the applicant’s capacity to exercise contractual rights to permit both the institution and supervisors to audit outsourced credit scoring activities (ECB 2018).

should be explainable when used in financial services for tasks such as credit scoring.

6.4.2.3 Outsourcing risks and concentration risks

The use of AI and ML systems requires proper consideration of outsourcing risks and concentration risks. As discussed earlier in this chapter, DFS providers are usually required to assess the risk stemming from outsourced parties and are fully responsible for their compliance with relevant laws and regulations. DFS providers that use AI and ML systems developed by third parties may lack the capacity or expertise to assess such risks.⁵⁴ The European Central Bank has adopted a specific framework to deal with the use of credit scoring models developed by third parties (see [Box 14](#)).

The United States is also starting to regulate the use of AI and ML models by credit providers (see [Box 15](#)).

BOX 15. Requirements for the algorithmic decision-making process in the United States

The draft bill of the U.S. Consumer Online Privacy Rights Act requires that entities engaging in algorithmic decision-making to facilitate credit opportunities must annually conduct an impact assessment that:

- Describes and evaluates the development of the entity’s algorithmic decision-making process, including the design and training data used to develop the process and how it was tested for accuracy, fairness, bias, and discrimination
- Assesses whether the algorithmic decision-making system produces discriminatory results based on an individual’s or class of individuals’ actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability

The entity may use an external independent auditor or researcher to conduct assessments.

54 Outsourcing risks and concentration risks in outsourcing are also discussed in sections [6.1](#) and [6.2](#).

Moreover, concentration risk could exist. In some markets, DFS providers rely on a relatively small number of AI and ML providers. The supervisor needs to monitor concentration risk at the market level since DFS providers could be impacted if one or more dominant AI/ML providers experience significant disruptions or cease operations. The risk would vary depending on the functions of the DFS provider supported by AI and ML applications. The increasing use of AI and ML by DFS providers requires that supervisors have some level of technical expertise to understand the different models, AI/ML providers and their relationship with DFS providers, and the risks arising from such relationships. This is a developing area of supervision and approaches are still emerging. However, there is a growing sense among supervisors in EMDEs that they will need the ability to effectively oversee the use of AI and ML, including by assessing models used at significant scale, to make judgment calls about whether models produce unfairly discriminatory results based on gender, race, ethnicity, and sexual orientation—and how they affect credit risk at DFS providers.

GLOSSARY

Application programming interface (API) is a set of routines, protocols, and tools for building software applications. APIs are the conduit for data transmission between two parties.

Artificial intelligence (AI) is defined as IT systems that perform functions requiring human capabilities. AI can ask questions, discover and test hypotheses, and automatically make decisions based on advanced analytics operating on extensive data sets. Machine learning (see below) is one subcategory of AI (BCBS 2018).

Banking-as-a-service (BaaS) provider is a tech company with a banking license that represents the vision of banks as market utilities. BaaS improves access to cutting-edge technology and brings economies of scope and scale. BaaS is a combination of banking tech stack and banking license, which necessitates compliance with banking regulation and allows the BaaS provider to build a banking balance sheet (Jenik and Zetterli 2020).

Big data refers to the large volume of data that can be generated, analyzed, and increasingly used by digital tools and information systems. This capability is driven by the increased availability of structured data and the ability to process unstructured data, increased data storage capabilities, and advances in computing power (BCBS 2018).

Big tech refers to large global companies whose primary role is to provide digital services rather than financial services. Examples include Amazon, Facebook, and Google.

Cloud computing refers to the use of an online network (cloud) of hosting processors to increase the scale and flexibility of computing capacity. This model enables convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers,

storage facilities, applications, services) that can be rapidly released with minimal management effort or service provider interaction (BCBS 2018).

Consent-based customer data refers to retail customer data held by banks (e.g., customer transactions, personal identification data, customer financial history) that is permissioned by the bank's customer to be accessed by a third party (BCBS 2019b).

Deposit insurance is the protection a deposit insurer provides to ensure that deposits up to a certain amount are reimbursed to depositors in the event a deposit-taking institution fails and is thus unable to meet its obligations to depositors (Izaguirre et al. 2019).

Deposit-taking institutions (DTIs) include conventional banks and nonbank institutions authorized to receive deposits from the public, such as deposit-taking microfinance institutions and financial cooperatives.

Digital financial services (DFS) are the range of financial services accessed through digital devices and delivered through digital channels, including payments, credit, savings, and remittances (AFI 2016). Digital channels may include mobile phones, cards combined with card readers, computers connected to the internet, and automated teller machines (ATMs), among others.

Digital financial services provider (DFS provider) refers to a provider that delivers digital financial services to its customers. A DFS provider could be a nonbank e-money issuer or any other regulated entity. In this guide, the focus is on entities that are not regulated and supervised as a bank.

Direction of risk refers to the potential change in the risk of a particular significant activity. It could be increasing, decreasing, or constant—based on the supervisor's

assessment of current and potential changes and trends within the DFS provider, among other factors.

Electronic money (e-money) refers to a monetary value electronically stored on a system or device that can be used for making payments and transfers to entities and people other than the e-money issuer. E-money may be referred to by other names such as stored value facility or mobile money.

Financial safety net is a broad framework that aims to reduce the probability of DTI failures and their impact on individual depositors, other DTIs, and the entire financial system. It includes prudential regulation and supervision and the functions of resolution, lender of last resort, and deposit insurance (IADI 2014).

Financial services provider (FSP) is a type of entity that provides financial services to consumers and other businesses. FSPs include conventional banks and DFS providers, among others.

Financial supervision (supervision) refers to the assessment and enforcement of FSP compliance with laws, regulations, or other rules intended to ensure FSPs operate in a safe and sound manner and hold capital and reserves sufficient to support the risks that arise in their business (CPMI 2003).

Financial technology (fintech) is a technologically enabled innovation in financial services that could result in new business models, applications, processes, or products, with an associated material effect on financial markets and institutions and the provision of financial services (Plaitakis and Staschen 2020).

Float (electronic float, e-float) refers to the total outstanding value of e-money liabilities of the e-money issuer to its customers at any point in time.

Float account (electronic float account, e-float account) is an account opened in a bank or other deposit-taking institution where the e-money issuer is required to deposit all funds collected from customers in exchange for e-money issued at par value.

Fund safeguarding regulatory requirements aim to protect e-money customers against risk of loss and unavailability of funds. These requirements aim to

ensure that float is sufficient, safe, and liquid to meet customer demand for converting e-money into cash. Measures generally include the following: (i) Regulations require that float only be invested (if any investment is permitted) in liquid and low-risk assets such as government bonds, or simply in an account with a commercial bank; (ii) Some regulations require EMIs to spread float among different DTIs to protect against the risk of the failure of the DTI holding the float; and (iii) Ring-fencing arrangements protect 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 (Dias and Staschen 2018a).

Innovation facilitator is a public sector initiative to engage with the fintech sector, for example, a regulatory sandbox, innovation hub, or innovation accelerator (FSB 2017).

Innovation hub/office refers to an innovation facilitator set up by a regulator. It provides support, advice, or guidance to regulated or unregulated firms in navigating the regulatory framework or identifying supervisory policy or legal issues and concerns. An innovation hub can take various forms, depending on the regulator's appetite and mandate. It is most often a central contact point to streamline queries and provide support, advice, and guidance. Support can be direct or indirect via guidance to the market and generally does not include testing products or services (Appaya and Gradstein 2020).

Legacy systems refers to potentially outdated computer systems, programming languages, or software. For traditional banks, it often means a system that cannot be taken out of service and the cost of designing a new system with a similar level of availability would be high. For example, systems to handle customer accounts (Dias and Staschen 2017).

Machine learning (ML) is a method of designing problem-solving rules that automatically improve through experience. Machine learning algorithms give computers the ability to learn without specifying all the knowledge the computer would need to perform the desired task, as well as to study and build algorithms that can learn from and make predictions based on data and experience (BCBS 2018).

Mobile financial services refers to a type of DFS primarily delivered through mobile phones. It may include mobile money, mobile insurance, mobile savings, and other services.

Mobile money is a type of digital financial service, more specifically a type of e-money delivered primarily through mobile phones and mobile money agents.

Nonbank is an institution that is not regulated and supervised as a bank or other DTI.

Nonbank electronic money issuer (EMI) is a nonbank institution authorized and dedicated to issuing e-money against the collection of customer funds, offering e-money accounts and related payment and storage services. EMIs are often prohibited from engaging in credit operations, that is, they cannot intermediate funds collected from e-money customers (Izaguirre et al. 2019).

Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, including, for example, those that provide real-time payments, greater financial transparency options for account holders, marketing, and cross-selling opportunities. Individual jurisdictions may define open banking differently (BCBS 2019b).

Open data is defined as the exchange of consumer data between private sector institutions, including FSPs and nonbank FSPs such as electronic money issuers, utility providers, and telecoms, with other such institutions on the basis of customer consent (Plaitakis and Staschen 2020).

Open finance is the exchange of customer data held by a wider set of FSPs including banks, insurance providers, mortgage providers, or investment advisors with each other on the basis of customer consent. FSPs can either be data holders or data users. Uses for such data include improving product design, customization (e.g., financial advice), improving risk assessments (e.g., credit, insurance), building price comparison tools, and helping customers to switch providers.

Payment initiation is a third-party service that facilitates the initiation of customer payments.

Payment initiation service provider refers to a third-party service provider that allows a consumer to make a payment from their bank account directly to the merchant, typically by establishing an electronic payment link between payer and online merchant via the payer's online banking module.

Payment services provider (PSP) is a legal entity that provides services enabling funds to be deposited and withdrawn from an account; payment transactions involving transfers of funds; the issuance and/or acquisition of payment instruments such as checks, e-money, credit cards, debit cards, and remittances; and other services central to the transfer of funds. PSPs include banks and other deposit-taking institutions, money transfer operators, and nonbank e-money issuers, among others (AFI 2016).

Regtech (regulatory technology) refers to technology solutions to improve compliance at potentially lower costs by regulated institutions, including solutions for regulatory reporting.

Regulatory sandbox is a framework set up by a financial sector regulator to allow private firms to live test small-scale innovations in a controlled environment—operating under a special exemption, allowance, or other limited time-bound exception—under the regulator's supervision (Jenik and Lauer 2017).

Remote inspection refers to a supervisory tool that can be implemented through techniques such as video conferencing, electronic document and file reviews, and other technological tools. The use of APIs to access the DFS provider's system helps supervisors remotely conduct audits and tests.

Resolution is a disposition plan and process for a nonviable deposit-taking institution. Resolution may include liquidation and depositor reimbursement; transfer and/or sale of assets and liabilities; establishment of a temporary bridge institution; and write-down or conversion of debt to equity. Resolution may also include the application of procedures under insolvency law to parts of an entity in resolution, in conjunction with the exercise of resolution powers (IADI Glossary).

Resolution authority is a public authority that is responsible, either alone or together with other authorities, for the resolution of FSPs established in its jurisdiction, including resolution planning functions (IADI Glossary).

Structured data is data that have been organized into a formatted repository, typically a database, so their elements can be made addressable for more effective processing and analysis. A data structure is a kind of repository that organizes information for that purpose. In a database, for example, each field is discrete and its information can be retrieved either separately or along with data from other fields in a variety of combinations (TechTarget 2015).

Supervisory authority refers to a financial authority in charge of financial supervision, for example, central banks, financial market authorities, and financial conduct authorities. It does not include regulators of other sectors (e.g., telecom regulators).

Suptech (supervisory technology) refers to technological solutions focused on improving the processes and effectiveness of financial supervision and regulation.

Third-party provider is a type of legal entity that is not a part of the DFS provider. It can be a supervised FSP (e.g., bank, other DTI) or a non-supervised entity (e.g., fintech, cloud services provider).

Transaction accounts are accounts held with banks or other authorized and/or regulated service providers (including nonbanks) that can be used to make and receive payments and to store value. Transaction accounts can be further differentiated into deposit transaction accounts and e-money accounts (CPMI and World Bank 2020).

Unstructured data are data in nonstandardized formats that cannot be organized in traditional databases with searchable fields for sorting, extraction, and analysis.

REFERENCES

- Alliance for Financial Inclusion (AFI). 2016. “Digital Financial Services—Basic Terminology.” Guideline Note No. 19. Kuala Lumpur, Malaysia: AFI, August. <https://www.afi-global.org/sites/default/files/publications/2016-08/Guideline%20Note-19%20DFS-Terminology.pdf>
- Alliance for Financial Inclusion (AFI). 2017. “Strengthening Cooperation between Financial and Telecom Regulators on DFS Issues: A Case Study of Ghana.” Case Study No. 1. Kuala Lumpur, Malaysia: AFI, October. https://www.afi-global.org/sites/default/files/publications/2017-10/AFI_AFPI_case%20study_AW_digital.pdf
- Alliance for Financial Inclusion (AFI). 2020. “Digital Financial Services Supervision in Bangladesh.” Case Study. Kuala Lumpur, Malaysia: AFI, December. https://www.afi-global.org/wp-content/uploads/2020/12/AFI_DFS_Bangladesh_AW3_digital.pdf
- Appaya, Sharmista, and Helen Luskien Gradstein. 2020. “How Regulators Respond to Fintech: Evaluating the Different Approaches—Sandboxes and Beyond.” Working Paper. Washington, D.C.: World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/579101587660589857/how-regulators-respond-to-fintech-evaluating-the-different-approaches-sandboxes-and-beyond>
- Appaya, Sharmista, Matei Dohotaru, Byungnam Ahn, Tatsiana Kliatskova, Prasanna Seshan, and Ion Pascaru. 2020. “A Roadmap to SupTech Solutions for Low-income (IDA) Countries.” Fintech Note No. 7. Washington, D.C.: World Bank. <https://openknowledge.worldbank.org/handle/10986/34662>
- Asana. 2021. “What Is a Matrix Organization and How Does It Work?” Asana Resources. Business Strategy. 26 August. <https://asana.com/resources/matrix-organization>
- Australian Competition and Consumer Commission (ACCC). “The Consumer Data Right (CDR).” Project overview. Accessed on September 14, 2022. <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>
- BaFin. 2018. “Cloud Computing: Compliance with the Supervisory Requirements Regarding Rights of Information and Monitoring and the Ability to Monitor.” Federal Financial Supervisory Authority. Expert Articles. 7 May. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1804_Cloud_Computing_en.html
- Bank of England. 2020. “Transforming Data Collection from the U.K. Financial Sector.” Discussion Paper. January. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/transforming-data-collection-from-the-uk-financial-sector.pdf?la=en&hash=6E6132B4F7AF681CCB425B0171B-4CF43D82E7779>
- Bank of England. 2021. “Transforming Data Collection from the U.K. Financial Sector: A Plan for 2021 and Beyond.” 23 February. <https://www.bankofengland.co.uk/paper/2021/transforming-data-collection-from-the-uk-financial-sector-a-plan-for-2021-and-beyond>
- Basel Committee on Banking Supervision (BCBS). 2015. “Guidelines for Identifying and Dealing with Weak Banks.” Basel, Switzerland: BIS, July. <https://www.bis.org/bcbs/publ/d330.htm>
- Basel Committee on Banking Supervision (BCBS). 2016. “Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision Institutions Relevant to Financial Inclusion.” Basel, Switzerland: BIS, 27 September. <https://www.bis.org/bcbs/publ/d383.htm>
- Basel Committee on Banking Supervision (BCBS). 2018. “Implications of Fintech Developments for Banks and Bank Supervisors.” Basel, Switzerland: BIS, February. <https://www.bis.org/bcbs/publ/d431.pdf>
- Basel Committee on Banking Supervision (BCBS). 2019a. “Core Principles for Effective Banking Supervision.” Basel, Switzerland: BIS, December. https://www.bis.org/basel_framework/standard/BCP.htm
- Basel Committee on Banking Supervision (BCBS). 2019b. “Report on Open Banking and Application Programming Interfaces.” Basel, Switzerland: BIS, November. <https://www.bis.org/bcbs/publ/d486.pdf>
- Basel Committee on Banking Supervision (BCBS). 2021. “Revisions to the Principles for the Sound Management of Operational Risk.” Basel, Switzerland: BIS, March. <https://www.bis.org/bcbs/publ/d515.pdf>
- Biallas, Margarete, and Felicity O’Neill. 2020. “Artificial Intelligence Innovation in Financial Services.” Note 85. International Finance Corporation (IFC), June. <https://www.ifc.org/content/dam/ifc/doc/mgrt/emcom-pass-note-85-ai-innovation-in-financial-services.pdf>
- Bolzico, Javier, Yira Mascaró, and Paola Granata. 2007. “Practical Guidelines for Effective Bank Resolution.” Policy Research Working Paper No. 4389. Washington, D.C.: World Bank. <https://openknowledge.worldbank.org/handle/10986/7548>

- Borio, Claudio, Stijn Claessens, and Nikola Tarashev. 2022. "Entity-based vs Activity-based Regulation: A Framework and Applications to Traditional Financial Firms and Big Techs." FSI Occasional Paper No. 19. Basel, Switzerland: BIS. <https://www.bis.org/fsi/fsipapers19.htm>
- Central Bank of Brazil. 2022. Organizational chart. Accessed on September 15, 2022. <https://www.bcb.gov.br/acessoinformacao/organograma/>
- CGAP Background Documents. 2017. "Data Collection by Supervisors of DFS: Examples, Cases, and Templates." Washington, D.C.: CGAP, December. <https://www.findevgateway.org/guide-toolkit/2017/12/data-collection-supervisors-dfs-examples-cases-and-templates>
- Chalwe-Mulenga, Majorie, Eric Duflos, and Gerhard Coetzee. 2022. "The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence." Slide Deck. Washington, D.C.: CGAP, February. <https://www.cgap.org/research/reading-deck/evolution-nature-and-scale-dfs-consumer-risks-review-evidence>
- Committee on Payments and Market Infrastructures (CPMI). 2014. "Nonbanks in Retail Payments." Basel, Switzerland: BIS, September. <https://www.bis.org/cpmi/publ/d118.pdf>
- Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). 2012. "Principles for Financial Market Infrastructures." Basel, Switzerland: BIS, April. <https://www.bis.org/cpmi/publ/d101.htm>
- Committee on Payments and Market Infrastructures (CPMI) and World Bank. 2020. "Payment Aspects of Financial Inclusion in the Fintech Era." Basel, Switzerland: BIS, April. <https://www.bis.org/cpmi/publ/d191.pdf>
- Committee on Payment and Settlement Systems. 2003. "A Glossary of Terms Used in Payments and Settlement Systems." Basel, Switzerland: BIS, March. https://www.bis.org/cpmi/glossary_030301.pdf
- Committee on Payment and Settlement Systems. 2005. "Central Bank Oversight of Payment and Settlement Systems." Basel, Switzerland: BIS, May. <https://www.bis.org/cpmi/publ/d68.pdf>
- Crisanto, Juan Carlos, Johannes Ehrentraud, Marcos Fabian, and Amelie Monteil. 2022. "Big Tech Interdependencies—A Key Policy Blind Spot." FSI Insights on Policy Implementation No. 44. Financial Stability Institute, Basel, Switzerland: BIS, July. <https://www.bis.org/fsi/publ/insights44.htm>
- Datwani, Leena, and Anand Raman. 2020. "India's New Approach to Personal Data-sharing." Working Paper. Washington, D.C.: CGAP, July. <https://www.cgap.org/research/publication/indias-new-approach-personal-data-sharing>
- Delort, Dorothee, and Jose Antonio Garcia Luna. 2022. "Innovation in Payments: Opportunities and Challenges for EMDEs." Fintech and the Future of Finance Flagship Technical Note. Washington, D.C.: World Bank, 18 May. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099735104212220539/p1730060f0f36d0ef09ecb0c5e283741c3a>
- Department for Business, Energy, and Industrial Strategy (DBEIS). 2021. "Smart Data Working Group: Spring 2021 Report." June. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993365/smart-data-working-group-report-2021.pdf
- di Castri, Simone, Matt Grasser, and Arend Kulenkampff. 2018. "An API-based Prudential Reporting System for the Bangko Sentral ng Pilipinas (BSP): R2A Project Retrospective and Lessons Learned." August. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3596276
- di Castri, Simone, Stefan Hohl, Arend Kulenkampff, and Jermy Prenio. 2019. "The SupTech Generations." FSI Insights on Policy Implementation No. 19. Financial Stability Institute, October. <https://www.bis.org/fsi/publ/insights19.pdf>
- Dias, Denise. 2018. "SupTech: Leveraging Technology for Better Supervision." TC Notes. Toronto Centre, July. https://www.torontocentre.org/index.php?option=com_content&view=article&id=83&Itemid=99#:~:text=Based%20on%20multiple%20data%20streams,for%20example%20for%20misconduct%20risk
- Dias, Denise. 2020a. "Cloud Computing: Issues for Supervisors." TC Notes. Toronto Centre, November. https://www.torontocentre.org/index.php?option=com_content&view=article&id=226&Itemid=99
- Dias, Denise. 2020b. "How Can Licensing Regimes Keep Up with Financial Innovation in 2020?" Blog. Washington D.C.: CGAP, 26 February. <https://www.cgap.org/blog/how-can-licensing-regimes-keep-financial-innovation-2020>
- Dias, Denise, and Juan Carlos Izaguirre. 2019. "Regulator's Friend or Foe? Cloud Computing in Financial Inclusion." Blog. Washington, D.C.: CGAP, 16 September. <https://www.cgap.org/blog/regulators-friend-or-foe-cloud-computing-financial-inclusion>
- Dias, Denise, and Mehmet Kerse. 2021. "Regulatory Approaches to the Interest Earned on E-money Float Accounts." Technical Note. Washington, D.C.: CGAP, May. https://www.cgap.org/sites/default/files/publications/2021_05_Technical_Note_Interest_Float_Accounts_updated.pdf
- Dias, Denise, and Stefan Staschen. 2017. "Data Collection by Supervisors of Digital Financial Services." Working Paper. Washington, D.C.: CGAP, December. <https://www.cgap.org/research/publication/data-collection-supervisors-digital-financial-services>
- Dias, Denise, and Stefan Staschen. 2018a. "A Guide to Supervising E-money Issuers." Technical Guide. Washington, D.C.: CGAP, December. https://www.cgap.org/sites/default/files/publications/Technical-Guide-EMI-Supervision-Dec-2018_1.pdf
- Dias, Denise, and Stefan Staschen. 2018b. "Data Collection by Supervisors of Digital Financial Services." Slide Deck. Washington, D.C.: CGAP, January. <https://www.findevgateway.org/slide-deck/2018/01/data-collection-supervisors-digital-financial-services-slide-deck>

- Dias, Denise, and Stefan Staschen. 2019. "Nonbank E-money Issuers vs. Payments Banks: How Do They Compare?" Technical Note. Washington, D.C.: CGAP, December. https://www.cgap.org/sites/default/files/publications/2019_12_Technical_Note_Nonbank_EMoney_Issuers_vs_Payment_Banks_0.pdf
- Elderson, Frank. 2020. "COVID-19—A Digitalisation Boost and the Supervisory Response." Speech by Mr. Frank Elderson, Executive Director of Supervision of the Netherlands Bank at the SSM Roundtable, Berlin. Bank of International Settlements (BIS) Central Bank Speech. 1 October. <https://www.bis.org/review/r201001d.htm>
- England and Wales High Court. 2020. "In the Matter of Supercapital Ltd. and in the Matter of Insolvency Act 1986." 18 April. <https://www.bailii.org/ew/cases/EWHC/Ch/2020/1685.html>
- European Banking Authority (EBA). 2017. "Peer Review of the ITS on Supervisory Reporting Requirements." Final Peer Review Report. February. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1720738/01eb7247-7566-470c-a3de-5842108e4464/Final%20report%20on%20peer%20review%20on%20ITS%20on%20supervisory%20reporting.pdf?retry=1>
- European Banking Authority (EBA). 2019. "Final Report on EBA Guidelines on Outsourcing Arrangements." EBA/GL/2019/02. 25 February. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1>
- European Banking Authority (EBA). 2021a. "Study of the Cost of Compliance with Supervisory Reporting Requirements." EBA/Rep/2021/15. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1013948/Study%20of%20the%20cost%20of%20compliance%20with%20supervisory%20reporting%20requirement.pdf
- European Banking Authority (EBA). 2021b. "EBA Report on a Feasibility Study of an Integrated Reporting System under Article 430C CRR." EBA/REP/2021/38. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/Integrated%20reporting/1025496/EBA%20Final%20report%20on%20Feasibility%20study%20of%20the%20integrated%20reporting%20system.pdf
- European Central Bank (ECB). "Bringing Artificial Intelligence to Banking Supervision." Accessed on September 14, 2022. https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl191113_4.en.html
- European Central Bank (ECB). 2018. "Guide to Assessments of Fintech Credit Institution Licence Applications." Banking Supervision. March. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing_en.pdf
- European Commission (EC). 2018. "Artificial Intelligence for Europe." Brussels, April. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>
- European Commission (EC). 2021. "Proposal for a Regulation on Artificial Intelligence." Brussels, April. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>
- European Council. 2022. "Digital Finance: Provisional Agreement Reached on DORA." Press Release. Council of the European Union, 11 May. <https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/>
- Feyen, Erik, Jon Frost, Leonardo Gambacorta, Harish Natarajan, and Matthew Saal. 2022. "Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy." Report. Washington, D.C.: World Bank, 18 May. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099735304212236910/p17300608cded602c0a6190f4b8caaa97a1>
- Financial Conduct Authority (FCA). 2019. "Supercapital Ltd. Has Entered Administration." 1 October. <https://www.fca.org.uk/news/news-stories/supercapital-ltd-has-entered-administration>
- Financial Conduct Authority (FCA). 2020. "Digital Regulatory Reporting." 14 October. <https://www.fca.org.uk/innovation/regtech/digital-regulatory-reporting>
- Financial Conduct Authority (FCA). 2022a. "Data Strategy 2022." 24 June. <https://www.fca.org.uk/publications/corporate-documents/data-strategy-update-2022>
- Financial Conduct Authority (FCA). 2022b. "Using Payment Service Providers." 3 August. <https://www.fca.org.uk/consumers/using-payment-service-providers>
- Financial Stability Board (FSB). 2014. "Key Attributes of Effective Resolution Regimes for Financial Institutions." 15 October. https://www.fsb.org/wp-content/uploads/r_141015.pdf
- Financial Stability Board (FSB). 2017. "Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention." 27 June. <https://www.fsb.org/wp-content/uploads/R270617.pdf>
- Financial Stability Board (FSB). 2019. "Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications." 9 December. <https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/>
- Financial Stability Board (FSB). 2020a. "The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. Market Developments and Financial Stability Implications." 9 October. <https://www.fsb.org/wp-content/uploads/P091020.pdf>
- Financial Stability Board (FSB). 2020b. "Regulatory and Supervisory Issues Relating to Outsourcing and Third-party Relationships." Discussion Paper. 9 November. <https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/>

- Gispert, Tatiana Alonso, Pierre-Laurent Chatain, Karl Driessen, Danilo Palermo, and Ariadne Plaitakis. 2022. “Regulation and Supervision of Fintech: Considerations for EMDE Policymakers.” Fintech and the Future of Finance Flagship Technical Note. Washington, D.C.: World Bank, 18 May. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099735204212215248/p173006033b45702d09522066cbc8338dcb>
- Gomes, Sergio Jose de Mesquita, Aute Kasdorp, Gian Boeddu, and Jennifer Chien. 2022. “An Introduction to Developing a Risk-based Approach to Financial Consumer Protection Supervision.” Guidance Note. Washington, D.C.: World Bank, December. <https://openknowledge.worldbank.org/handle/10986/38419>
- Government of Ghana. 2020. “Digital Financial Services Policy.” Ministry of Finance. https://www.mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf
- HM Treasury. 2022. “Critical Third Parties to the Finance Sector: Policy Statement.” Policy Paper. 8 June. <https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement#fn:3>
- Hong Kong Monetary Authority (HKMA). 2019. “Guiding Principles on Consumer Protection with Respect to the Use of Big Data Analytics and Artificial Intelligence.” <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf>
- Institute of International Finance (IIF) Finance Regulation Technology (FRT). 2021a. “Explainable AI and the U.S. Request for Information.” Podcast Episode 103. 22 July. <https://www.iif.com/Publications/ID/4522/FRT-Episode-103-Explainable-AI-and-the-US-Request-for-Information-with-Wells-Fargos-Agus-Sudjianto>
- Institute of International Finance (IIF) Finance Regulation Technology (FRT). 2021b. “Ethical Handling of Customer Data and the IIF Data Ethics Charter.” Podcast Episode 104. 5 August. <https://www.iif.com/Publications/ID/4533/FRT-Episode-104-Ethical-Handling-of-Customer-Data-and-the-IIF-Data-Ethics-Charter-with-Jade-Haar-from-NAB-and-David-Hardoon-from-UnionBank-of-the-Philippines>
- International Association of Deposit Insurers (IADI). Glossary. <https://www.iadi.org/en/core-principles-and-guidance/glossary/>
- International Association of Deposit Insurers (IADI). 2014. “Core Principles for Effective Deposit Insurance Systems.” November. <https://www.iadi.org/en/assets/File/Core%20Principles/cprevised2014nov.pdf>
- International Finance Corporation (IFC) and the MasterCard Foundation. 2016. “Digital Financial Services and Risk Management Handbook.” <https://documents1.worldbank.org/curated/en/226461531293264583/pdf/Digital-financial-services-and-risk-management-handbook.pdf>
- Izaguirre, Juan Carlos, Denise Dias, Eric Duflos, Laura Brix Newbury, Olga Tomilova, and Myra Valenzuela. 2022. “Market Monitoring for Financial Consumer Protection.” Toolkit. Washington, D.C.: CGAP. <https://www.cgap.org/topics/collections/market-monitoring>
- Izaguirre, Juan Carlos, Denise Dias, and Mehmet Kerse. 2019. “Deposit Insurance Treatment of E-money: An Analysis of Policy Choices.” Technical Note. Washington DC.: CGAP, October. <https://www.cgap.org/research/publication/deposit-insurance-treatment-e-money-analysis-policy-choices>
- Jenik, Ivo. 2022. “TymeBank Case Study: The Customer Impact of Inclusive Digital Banking.” Washington D.C.: CGAP, January. <https://www.cgap.org/research/publication/tymbank-case-study-customer-impact-inclusive-digital-banking>
- Jenik, Ivo, and Kate Lauer. 2017. “Regulatory Sandboxes and Financial Inclusion.” Working Paper. Washington D.C.: CGAP, October. <https://www.cgap.org/research/publication/regulatory-sandboxes-and-financial-inclusion>
- Jenik, Ivo, and Peter Zetterli. 2020. “Digital Banks: How Can They Deepen Financial Inclusion?” Slide Deck. Washington D.C.: CGAP, February. https://www.cgap.org/sites/default/files/publications/slide-deck/2020_02_Slidedeck_Digital_Banking_and_FI_updated.pdf
- Jenik, Ivo, and Schan Duff. 2020. “How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers.” Technical Guide. Washington, D.C.: CGAP, September. <https://www.cgap.org/research/publication/how-build-regulatory-sandbox-practical-guide-policy-makers>
- Kaffenberger, Michelle, Edoardo Totolo, and Matthew Soursourian. 2018. “A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania.” Working Paper. Washington D.C.: CGAP, October. <https://www.cgap.org/research/publication/digital-credit-revolution-insights-borrowers-kenya-and-tanzania>
- Kelly, Sonja, and Mehrdad Mirpourian. 2021. “Algorithmic Bias, Financial Inclusion, and Gender.” Women’s World Banking, February. https://www.womensworldbanking.org/wp-content/uploads/2021/02/2021_Algorithmic_Bias_Report.pdf
- Kerse, Mehmet, and Stefan Staschen. 2018. “Safeguarding Rules for Customer Funds Held by EMIs.” Technical Note. Washington, D.C.: CGAP, December. <https://www.cgap.org/research/publication/safeguarding-rules-customer-funds-held-emis>
- Kerse, Mehmet, Patrick Meagher, and Stefan Staschen. 2020. “The Use of Agents by Digital Financial Services Providers.” Technical Note. Washington, D.C.: CGAP, February. <https://www.cgap.org/research/publication/use-agents-digital-financial-services-providers>
- Kirakul, Sasin, Jeffrey Yong, and Raihan Zamil. 2021. “The Universe of Supervisory Mandates—Total Eclipse of the Core?” FSI Insights on Policy Implementation No. 30. Financial Stability Institute, Bank for International Settlements (BIS), March. <https://www.bis.org/fsi/publ/insights30.pdf>

- Lastra, Rosa M., Rodrigo Olivares-Caminal, and Constanza A. Russo. 2017. “The Provision of Critical Functions at Global, National and Regional Level—Is There a Need for Further Legal/Regulatory Clarification if Liquidation Is the Default Option for Failing Banks?” Banking Union Scrutiny. In-depth analysis requested by the ECON Committee. Economic Governance Support Unit. Directorate-General for Internal Policies of the Union. European Parliament, November. http://publications.europa.eu/resource/cellar/291500a4-f4f0-11e7-be11-01aa75ed71a1.0001.01/DOC_1
- Lawrence, Jonathan, Kai Zhang, and Max Griffin. 2021. “New U.K. Insolvency Regime for Payment Institutions and Electronic Money Institutions.” K&L Gates, 11 May. <https://www.klgates.com/New-UK-Insolvency-Regime-For-Payment-Institutions-and-Electronic-Money-Institutions-5-11-2021>
- Lyman, Timothy, Louis de Koker, Chrissy Martin Meier, and Mehmet Kerse. 2019. “Beyond KYC Utilities: Collaborative Customer Due Diligence.” Working Paper. Washington, D.C.: CGAP, August. <https://www.cgap.org/research/publication/beyond-kyc-utilities-collaborative-customer-due-diligence>
- Mdluli, Gcinisizwe, Ivo Jenik, and Peter Zetterli. 2022. “Banking-as-a-Service: How It Can Catalyze Financial Inclusion.” Slide Deck. Washington, D.C.: CGAP, August. <https://www.cgap.org/research/reading-deck/banking-service-how-it-can-catalyze-financial-inclusion>
- Meagher, Patrick. 2019. “Risk-Based Customer Due Diligence: Regulatory Approaches.” Technical Note. Washington, D.C.: CGAP, October. <https://www.cgap.org/research/publication/risk-based-customer-due-diligence-regulatory-approaches>
- Medine, David, and Gayatri Murthy. 2020. “Making Data Work for the Poor: New Approaches to Data Protection and Privacy.” Focus Note. Washington, D.C.: CGAP, January. https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor.pdf
- Mitha, Aiize, Faith Chepng’etich Biegon, and Peter Zetterli. 2022. “Banking in Layers: Five Cases to Illustrate How the Market Structure for Financial Services Is Evolving.” Working Paper. Washington, D.C.: CGAP, July. <https://www.cgap.org/research/publication/banking-in-layers-five-cases-to-illustrate-how-market-structure-for-financial>
- Monetary Authority of Singapore (MAS). 2017. “MAS Sets Up Data Analytics Group.” Media Release. 14 February. <https://www.mas.gov.sg/news/media-releases/2017/mas-sets-up-data-analytics-group>
- Monetary Authority of Singapore (MAS). 2018. “Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector.” <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>
- Newbury, Laura Brix, and Juan Carlos Izaguirre. 2019. “Risk-based Supervision in Low-capacity Environments: Considerations for Enabling Financial Inclusion.” Washington D.C.: CGAP, June. <https://www.findevgateway.org/paper/2019/06/risk-based-supervision-low-capacity-environments>
- Open Banking Implementation Entity (OBIE). “API Performance Stats.” Accessed on September 15, 2022. <https://www.openbanking.org.uk/api-performance/>
- Plaitakis, Ariadne, and Stefan Staschen. 2020. “Open Banking: How to Design for Financial Inclusion.” Working Paper. Washington, D.C.: CGAP, October. <https://www.cgap.org/research/publication/open-banking-how-design-financial-inclusion>
- Prenio, Jermy, and Jeffrey Yong. 2021. “Humans Keeping AI in Check—Emerging Regulatory Expectations in the Financial Sector.” FSI Insights on Policy Implementation No. 35. Financial Stability Institute, Basel, Switzerland: BIS, August. <https://www.bis.org/fsi/publ/insights35.pdf>
- Reserve Bank of Malawi (RBM). 2013. “Memorandum of Understanding between the Reserve Bank of Malawi and the Malawi Communications Regulatory Authority.” December. <https://www.rbm.mw/PaymentSystems/GetContentFile?ContentID=4890>
- Restoy, Fernando. 2021. “Fintech Regulation: How to Achieve a Level Playing Field.” Occasional Paper No. 17. Financial Stability Institute, Basel, Switzerland: BIS, February. <https://www.bis.org/fsi/fsipapers17.pdf>
- Reuters. 2021. “Timeline: The Rise and Fall of Wirecard, a German Tech Champion.” Frankfurt. 16 March. <https://www.reuters.com/article/us-germany-wirecard-inquiry-timeline-idUSKBN2B81J>
- Soursourian, Matthew, and Ariadne Plaitakis. 2019. “Fair Play: Ensuring Competition in Digital Financial Services.” Working Paper. Washington, D.C.: CGAP, November. <https://www.cgap.org/research/publication/fair-play-ensuring-competition-digital-financial-services>
- Staschen, Stefan, and Ariadne Plaitakis. 2020. “Open Banking: 7 Ways Data-sharing Can Advance Financial Inclusion.” Blog. Washington, D.C.: CGAP, 7 May. <https://www.cgap.org/blog/open-banking-7-ways-data-sharing-can-advance-financial-inclusion>
- Staschen, Stefan, and Patrick Meagher. 2018. “Basic Regulatory Enablers for Digital Financial Services.” Focus Note No. 109. Washington, D.C.: CGAP, May. <https://www.cgap.org/research/publication/basic-regulatory-enablers-digital-financial-services>
- Staschen, Stefan, and Patrick Meagher. 2022. “Regulating Platform-based Finance: Seeing the Big Picture.” Blog. Washington, D.C.: CGAP, 13 April. <https://www.cgap.org/blog/regulating-platform-based-finance-seeing-big-picture>
- Taylor, Charles, Christopher Wilson, Eija Holtinen, and Anastasiia Morozova. 2020. “Institutional Arrangements for Fintech Regulation and Supervision.” IMF Fintech Note 19/02. 10 January. <https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Institutional-Arrangements-for-Fintech-Regulation-and-Supervision-48809>
- Tomilova, Olga, and Myra Valenzuela. 2018. “Financial Inclusion + Stability, Integrity, and Protection (I-SIP) Toolkit: Policy Making for an Inclusive Financial System.” Technical Guide. Washington, D.C.: CGAP, November. <https://www.cgap.org/research/publication/i-sip-toolkit-policy-making-inclusive-financial-system>

- Turner, Johannes. 2015. “European Reporting Framework—A Possible Solution to Reporting Challenges for Banks.” Presentation by Johannes Turner, Director Statistics Department of the Oesterreichische Nationalbank, at the 60th World Statistics Congress, ISI2015. STS 010 “Micro Data for Multipurpose Data Provision.” Rio de Janeiro. https://www.bis.org/ifc/events/ifc_isi_2015/010_turner_presentation.pdf
- UNSGSA FinTech Working Group and CCAF. 2019. “Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech.” Office of the UNSGSA and CCAF. https://www.unsgsa.org/sites/default/files/resources-files/2020-09/UNSGSA_Report_2019_Final-compressed.pdf
- USAID. 2010. “Mobile Financial Services Risk Matrix.” 23 July. <https://www.gsmamobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf>
- World Bank. 2017. “Good Practices for Financial Consumer Protection.” Brief. Washington, D.C.: World Bank, 14 December. <https://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection>
- World Bank. 2021. “Global Fintech-enabling Regulations Database.” Brief. Washington, D.C.: World Bank, 16 November. <https://www.worldbank.org/en/topic/fintech/brief/global-fintech-enabling-regulations-database>
- World Bank and International Committee on Credit Reporting (ICCR). 2019. “Credit Scoring Approaches Guidelines.” Washington, D.C.: World Bank. <https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf>
- Wright, Paul. 2018a. “Risk-based Supervision.” TC Notes. Toronto Centre, March. https://www.torontocentre.org//videos/Risk-Based_Supervision.pdf
- Wright, Paul. 2018b. “Implementing Risk-based Supervision: A Guide for Senior Managers.” TC Notes. Toronto Centre, July. https://www.torontocentre.org//videos/Implementing_Risk_Based_Supervision_A_Guide_for_Senior_Managers_Updated_Links.pdf
- Zetterli, Peter. 2021. “The Great Unbundling: How Technology Is Making Financial Services Modular and What It Means for Inclusion.” Reading Deck. Washington, D.C.: CGAP, November. <https://www.cgap.org/research/slide-deck/great-unbundling-how-technology-making-financial-services-modular>

ADDITIONAL READING

- Alliance for Financial Inclusion. 2022. “Regulatory and Supervisory Technologies for Financial Inclusion.” <https://www.afi-global.org/publications/regulatory-and-supervisory-technologies-for-financial-inclusion/>
- Appaya, Sharmista, Helen Luskin Gradstein, and Mahjabeen N. Haji. 2020. “Global Experiences from Regulatory Sandboxes.” Fintech Note No. 8. Washington, D.C.: World Bank. <https://openknowledge.worldbank.org/bitstream/handle/10986/34789/Global-Experiences-from-Regulatory-Sandboxes.pdf?sequence=5&isAllowed=y>
- Asian Development Bank. 2021. “Cloud-based Core Banking in the Philippines: A Rural Bank Pilot Project.” <https://www.adb.org/sites/default/files/publication/736741/cloud-based-core-banking-philippines.pdf>
- Bank for International Settlements (BIS), Basel Committee on Banking Supervision (BCBS). 2019. “Report on Open Banking and Application Programming Interfaces.” <https://www.bis.org/bcbs/publ/d486.pdf>
- Bank for International Settlements, Consultative Group on Innovation and the Digital Economy. 2020. “Enabling Open Finance through APIs.” December. <https://www.bis.org/publ/othp36.pdf>
- Boeddu, Gian, Jennifer Chien, Ivor Istuk, Ros Grady, and Arpita Sarkar. 2021. “Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches.” Policy Research Paper. Washington, D.C.: World Bank, 1 April. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/515771621921739154/consumer-risks-in-fintech-new-manifestations-of-consumer-risks-and-emerging-regulatory-approaches-policy-research-paper>
- Cambridge Centre for Alternative Finance (CCAF) and World Economic Forum. 2020. “Transforming Paradigms: A Global AI in Financial Services Survey.” January. https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf
- CGAP Collection Webpage. “Fintech and the Future of Banking” <https://www.cgap.org/topics/collections/fintech-future-of-banking>
- Crisanto, Juan Carlos, Conor Donaldson, Denise Garcia Ocampo, and Jermy Prenio. 2018. “Regulating and Supervising the Clouds: Emerging Prudential Approaches for Insurance Companies.” FSI Insights No. 13. Financial Stability Institute, 5 December. <https://www.bis.org/fsi/publ/insights13.htm>
- Crisanto, Juan Carlos, Katharina Kienecker, Jermy Prenio, and Eileen Tan. 2020. “From Data Reporting to Data-sharing: How Far Can Suptech and Other Innovations Challenge the Status Quo of Regulatory Reporting?” FSI Insights No. 29. Financial Stability Institute, 16 December. <https://www.bis.org/fsi/publ/insights29.htm>
- di Castri, Simone, Matt Grasser, and Arend Kulenkampff. 2018. “Financial Authorities in the Era of Data Abundance: Regtech for Regulators and Suptech Solutions.” White Paper. BFA Global, August. <https://bfaglobal.com/wp-content/uploads/2020/01/R2AWhitePaper-1.pdf>
- Dias, Denise, and Juan Carlos Izaguirre. 2020. “Risk-based Supervision Is Key to Financial Inclusion in 2020 and Beyond.” Blog Post. Washington, D.C.: CGAP, February. <https://www.cgap.org/blog/risk-based-supervision-key-financial-inclusion-2020-beyond>
- Dias, Denise, and Stefan Staschen. 2018. “RegTech and Digital Finance Supervision: A Leap into the Future.” Blog Post. Washington, D.C.: CGAP, January. <https://www.cgap.org/blog/regtech-and-digital-finance-supervision-leap-future>
- Dias, Denise, and Stefan Staschen. 2018. “Why Digital Finance Supervisors Should Automate Data Collection.” Blog Post. Washington, D.C.: CGAP, January. <https://www.cgap.org/blog/why-digital-finance-supervisors-should-automate-data-collection>
- Dobler, Marc C., Jose M. Garrido, Dirk Jan Grolleman, Tanai Khiaonarong, and Jan Nolte. 2021. “E-money: Prudential Supervision, Oversight, and User Protection.” Departmental Paper. IMF, 14 December. <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/12/13/E-Money-Prudential-Supervision-Oversight-and-User-Protection-464868>
- Durkee, Mark. 2021. “Ensuring Trustworthy Algorithmic Decision-making.” OECD. AI Policy Observatory. OECE, 8 April. <https://oecd.ai/en/wonk/how-to-achieve-trustworthy-algorithmic-decision-making>
- Ehrentraud, Johannes, Denise Garcia Ocampo, and Camila Quevedo Vega. 2020. “Regulating Fintech Financing: Digital Banks and Fintech Platforms.” FSI Insights No. 27. Financial Stability Institute, 27 August. <https://www.bis.org/fsi/publ/insights27.htm>
- Financial Conduct Authority of the United Kingdom. Thematic Reviews Webpage. https://www.fca.org.uk/publications/search-results?p_search_term=&category=research-thematic%20reviews&sort_by=dmetaZ

- Financial Stability Board. 2017. “Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications.” 1 November. <https://www.fsb.org/wp-content/uploads/P011117.pdf>
- Financial Stability Board. 2019. “Bigtech in Finance: Market Developments and Potential Financial Stability Implications.” 9 December. <https://www.fsb.org/2019/12/bigtech-in-finance-market-developments-and-potential-financial-stability-implications/>
- Global Financial Innovation Network (GFIN). RegTech and SupTech Webpage. <https://www.thegfin.com/regtech-suptech>
- Izaguirre, Juan Carlos, and Ivo Jenik. 2016. “Risk-based Supervision in the Digital Financial Inclusion Era.” Blog Post. Washington, D.C.: CGAP, 26 April. <https://www.cgap.org/blog/risk-based-supervision-digital-financial-inclusion-era>
- Kerse, Mehmet, and Stefan Staschen. 2021. “Digital Banks: How Can They Be Regulated to Deepen Financial Inclusion?” Slide Deck. Washington, D.C.: CGAP, December. <https://www.cgap.org/research/reading-deck/digital-banks-how-can-they-be-regulated-deepen-financial-inclusion>
- Kessler, Alex, and Jacobo Menajovsky. 2021. “Reducing Bias in Algorithmic Decisions Cannot Rely on ‘Blind’ Approaches.” Blog Post. Center for Financial Inclusion, 25 May. <https://www.centerforfinancialinclusion.org/reducing-bias-in-algorithmic-decisions-cannot-rely-on-blind-approaches>
- Smith, Genevieve, and Ishita Rustagi. 2021. “When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity.” Blog Post. Stanford Social Innovation Review, 31 March. https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity
- Taylor, Charles, Aquiles Almansi, and Aurora Ferrari. 2019. “Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits.” Washington, D.C.: World Bank. <https://openknowledge.worldbank.org/bitstream/handle/10986/33221/Prudential-Regulatory-and-Supervisory-Practices-for-Fintech-Payments-Credit-and-Deposits.pdf?sequence=1&isAllowed=y>
- Valenzuela, Myra, and Juan Carlos Izaguirre. 2019. “Cloud Computing for Financial Inclusion: Lessons from the Philippines.” Blog Post. Washington, D.C.: CGAP, 24 September. <https://www.cgap.org/blog/cloud-computing-financial-inclusion-lessons-philippines>
- Vidal, Maria Fernandez, and Jacobo Menajovsky. 2019. “Algorithm Bias in Credit Scoring: What’s Inside the Black Box?” Blog Post. Washington, D.C.: CGAP, 5 September. <https://www.cgap.org/blog/algorithm-bias-credit-scoring-whats-inside-black-box>
- Wibisono, Okiriza, Hidayah Dhini Ari, Anggraini Widjanarti, Alvin Andhika Zulen, and Bruno Tissot. 2019. “The Use of Big Data Analytics and Artificial Intelligence in Central Banking.” IFC Bulletin. No. 50. 28 May. <https://www.bis.org/ifc/publ/ifcb50.htm>
- World Bank and Accenture. 2016. “Cloud Computing Overview.” Paper. June. <https://documents1.worldbank.org/curated/en/837891494407497011/pdf/114837-WP-CloudOverview-PUBLIC.pdf>
- Wright, Paul. 2019a. “The Development and Use of Risk-based and Assessment Frameworks.” TC Notes. Toronto Centre, 30 January. https://www.torontocentre.org/index.php?option=com_content&view=article&id=86:the-development-and-use-of-risk-based-assessment-frameworks&catid=10&Itemid=101
- Wright, Paul. 2019b. “Turning Risk Assessments into Supervisory Actions.” TC Notes. Toronto Centre, August. https://www.torontocentre.org/videos/Turning_Risk_Assessments_Into_Supervisory_Actions_251885006.pdf



BILL & MELINDA GATES foundation

