INTERNATIONAL MONETARY FUND

MONETARY AND CAPITAL MARKETS DEPARTMENT

Good Practices in Cyber Risk Regulation and Supervision

Prepared by Tamas Gaidosch, Emran Islam,
Tanai Khiaonarong, Rangachary Ravikumar, and
Chris Wilson

2026

DEPARTMENTAL PAPER

INTERNATIONAL MONETARY FUND

MONETARY AND CAPITAL MARKETS DEPARTMENT

DEPARTMENTAL PAPER

Good Practices in Cyber Risk Regulation and Supervision

Prepared by Tamas Gaidosch, Emran Islam,
Tanai Khiaonarong, Rangachary Ravikumar,
and Chris Wilson

Cataloging-in-Publication Data
IMF Library

Names: Gaidosch, Tamas, author. | Islam, Emran, author. | Tanai Khiaonarong, author. | Ravikumar, Rangachary, author. | Wilson, Christopher (Christopher Lindsay) | International Monetary Fund, publisher.
Title: Good practices in cyber risk regulation and supervision / Tamas Gaidosch, Emran Islam, Tanai Khiaonarong, Rangachary Ravikumar, and Chris Wilson
Other titles: International Monetary Fund. Monetary and Capital Markets department.
Description: Washington, DC : International Monetary Fund, 2026. | Includes bibliographical references.
Identifiers: ISBN:

9798229026185	(paper)
9798229029735	(ePub)
9798229029711	(WebPDF)

Subjects: LCSH: Computer security. | Computer security—Law and legislation.
Classification: LCC QA76.9.A25 G3 2026

Acknowledgments

The authors appreciate the valuable inputs from Dirk Jan Grolleman, Jay Surti, and Marina Moretti (all from IMF's Monetary and Capital Markets Department).

The Departmental Paper Series presents research by IMF staff on issues of broad regional or cross-country interest. The views expressed in this paper are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Publication orders may be placed online or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, USA
T. +(1) 202.623.7430
publications@IMF.org
IMFbookstore.org
elibrary.IMF.org

Contents

Executive Summary ... v

Acronyms and Abbreviations ... vii

1. Introduction ... 1
A. Key Concepts ... 1
B. Evolution of the Threat Landscape ... 2
C. Why Is Cyber Risk Important? ... 3

2. IMF Work on Cyber Risk Regulation and Supervision in the Financial Sector ... 5
A. Cyber Risk Assessments in the FSAP ... 7
Where Does the Cyber Risk Workstream Fit in the Overall FSAP? ... 7
B. Cyber Risk Technical Assistance ... 8

3. Good Regulatory Practices ... 11
A. The Regulation Development Process ... 11
Success Factors of Cyber Risk Regulation Development ... 12
Principles-Based versus Prescriptive Regulatory Approaches ... 12
B. Key Expectations that Facilitate Effective Risk Mitigation ... 13
Governance and Internal Controls ... 13
Technology and Cyber Risk Management ... 14
ICT Service Management ... 14
Cybersecurity Operations ... 15
Response and Recovery ... 16
Vulnerability Scanning, Tests, and Exercises ... 16
Independent Assurance ... 16
Outsourcing and Technology Service Provider Management ... 16

4. Good Supervision Practices ... 18
A. Governance and Management of Cyber Risk Supervision ... 19
Staffing, Planning, and Resource Allocation ... 20
Learning and Development ... 21
B. Proportionality ... 23
Examples ... 23
Proportionality and Nonfinancial Risks ... 24
C. Offsite Supervision ... 25
Overview ... 25
Good Practices ... 26
D. Onsite Supervision ... 28
Overview ... 28
Good Practices ... 29
E. Thematic Reviews ... 34
Overview ... 34
Good Practices ... 34

F. Monitoring of Cybersecurity Testing 35
Overview 35
Good Practices 36

5. Cyber Simulation Exercises 39
A. Overview 39
B. Good Practices 40
Stakeholder Engagement 41
Multiyear Preparedness Priorities 41
Improvement Planning 42
Process for Conducting an Individual Exercise 42
Simulation Exercise Design and Development 43
Simulation Exercise Conduct 43
Assessment 43

6. Monitoring and Mitigating System-wide Cyber Risk 45
A. Key Pillars for Resilience and Stability 45
B. Financial Market Infrastructures—Systemic Players 46

7. Conclusions 50

References 51

BOXES

Box 1. Australian Prudential Regulation Authority's Supervisory Approach—CPS 234 Independent Assessment 33
Box 2. Supervision versus Oversight: Key Differences 47

FIGURES

Figure 1. Selected Global Cyber Risk Metrics, 2004–25 3
Figure 2. Cybersecurity and Macrofinancial Stability: Channels of Transmission 4
Figure 3. Number of TA Missions on Cyber Risk 6
Figure 4. Example Regulation Development Process Flow 11
Figure 5. Core Supervisory Processes and Interrelationships 18
Figure 6. Continuous Learning and Capacity Development 22
Figure 7. Offsite Supervision Phases 25
Figure 8. Onsite Examination Phases 29
Figure 9. TLPT Phases 36
Figure 10. Cyber Crisis Exercises Step by Step 43

TABLES

Table 1. FSAP Missions with In-Depth Coverage of Cyber Risk 5
Table 2. The Three Pillars of the IMF's Financial Stability Assessment Program 8
Table 3. Key Benefits of Cyber Crisis Exercises 39
Table 4. Recommendations to Strengthen FMI Cyber Resilience 48
Table 5. Recommendations to Strengthen FMI Supervision and Oversight 49

Executive Summary

Cyber risk in the financial sector is a critical concern because of the sensitivity, volume, and value of the data handled by financial institutions (FIs)[1] and financial market infrastructures (FMIs).[2] The importance of this challenge is underscored by the rapid increase in the scope and intensity of cyber threats. The financial sector is a prime target of cybercriminals given the significant growth and still rising prominence of digital financial services and online transactions. Moreover, critical infrastructure, such as payments, clearing, and settlement, can be targeted by adversaries seeking disruption.

FIs and FMIs manage vast amounts of personal and financial data, including bank account details, credit card information, customer identification, transaction histories, and other sensitive information. A security breach can lead to identity theft, financial loss, and reputational damage for both the FI and its customers. A systemic cyber incident—for example, a cyberattack that incapacitates a systemic FMI—may adversely impact financial stability and exert negative spillovers on the macroeconomy. Therefore, it is important that financial regulatory, supervisory, and oversight authorities treat cyber risk as among the top risks the sector faces, develop commensurate cyber-risk-management requirements, and ensure adherence thereto.

Over time, cyberattacks have become stronger, more frequent, and ever more sophisticated. Given the continuous strengthening of cyber threat actors and the ever more critical and complex information and communication technology (ICT) that the financial system depends on, the way forward is toward strengthening cybersecurity expectations and enforcement.

In terms of regulation, this can be accomplished without increasing complexity and proactively addressing emerging priorities by clarifying expectations regarding supervisory tools.

- A key opportunity for improvement is in the way regulators understand and reflect the interrelationship between ICT and cyber risk in their expectations. For example, it makes sense to integrate ICT and cyber-risk-management regulation, separated thus far, into one coherent technology-risk-management regulatory framework. This should be achievable in many jurisdictions, albeit it may pose a greater operational challenge in countries with multiple and partially overlapping existing regulations.

- Specific expectations around cybersecurity testing, crisis exercises, and third-party risk management appear to be the most impactful in recent times. The true value of cybersecurity testing becomes evident only through its practical application, wherein it becomes clear that it is imprudent to consider a system, process, or facility secure unless it has been tested for possible intrusion. Cybersecurity testing has been used by the industry for some time, albeit the absence of baseline regulatory expectations has led to significant variation in approaches and quality, limiting its use for supervisory purposes. With major jurisdictions having taken the lead in formalizing and mandating cybersecurity testing recently, it is now becoming a key tool to strengthen the cyber resilience of national financial systems in many countries. In a similar vein, cyber crisis exercises coordinated and overseen by supervisory authorities are becoming essential to preparing for systemic cyber risk events.

[1] Includes banks, insurance companies, nonbank financial institutions, and securities companies, among others.

[2] The CPMI-IOSCO definition of a financial market infrastructure (FMI) includes payment systems, central counterparties, securities settlement systems, central securities depositories, https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bis.org%2Fcpmi%2Fpubl%2Fd101a.pdf&data=05%7C02%7CNAminiAbbas%40imf.org%7Ca892dc928a924252960c08de292c9964%7C8085fa43302e45bdb171a6648c3b6be7%7C0%7C0%7C638993469219110265%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=mZfk4bjoq6iPDRiBrhs9D1rdhV5z5JruDxzluOJihsg%3D&reserved=0.

- The next major challenge is to respond to risks posed by the extraordinary growth and reliance on third-party technology services by bringing critical providers under a cyber risk oversight framework.

In terms of prudential supervision and central bank oversight of cyber risk, the approach that is probably the most consequential in improving the cybersecurity stance of the financial sector is the presence and thoroughness of the supervisor. Whether it is offsite or onsite supervision, industry outreach, or consultations, supervisors should make their presence felt by frequent and inquisitive contact with FIs and FMIs, thorough analyses, strong feedback, and diligent follow-up on identified issues.

Two overarching attributes underpin effective cyber risk regulation and supervision. First, a balanced approach that blends principles-based and prescriptive elements, matching the maturity of cyber-risk-management practices within the financial system. In regulation, this manifests itself in a focus on desired outcomes, while being technology agnostic, which provides flexibility in how FIs and FMIs meet expectations. In supervision, this results in greater reliance on professional judgment, which is more important in ICT and cyber risk than in other risk disciplines, where there is often a prevalence of quantitative methods because of the easier access to more data. Second, applying proportionality. One size does not fit all, with neither regulation nor supervision. For systemically important and complex FIs and FMIs, the highest standards need to be applied across all dimensions, whereas for smaller, less sophisticated, non-systemic FIs, supervisory expectations can be adapted to fit their risk profiles. However, it is to be noted that in an interconnected chain, security is as strong as its weakest link.

Acronyms and Abbreviations

AI	Artificial Intelligence
BCBS	Basel Committee on Banking Supervision
BCP	Basel Core Principles for Effective Banking Supervision
CISO	Chief Information Security Officer
CPMI	Committee on Payments and Market Infrastructures
DC	Data Center
FI	Financial Institution (banks, insurance companies, and other nonbank financial institutions)
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
IAM	Identity and Access Management
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
TA	Technical Assistance
TLPT	Threat-Led Penetration Testing
TSP	Technology Service Provider

1. Introduction

This paper consolidates the practical experience and lessons learned from the IMF's cyber risk regulation and supervision work program since its inception in 2017 across several advanced, emerging, and developing economies. Based on empirical evidence and country work, we share regulatory expectations and practices that contribute significantly to improving the cybersecurity posture of the financial system ("good practices"). These are neither exhaustive nor universally applicable and are not intended to establish principles or standards. The global scope and maturity of the IMF's work program make it possible to draw conclusions regarding practices that can strengthen the financial system's cyber resilience when developing or improving cyber risk regulatory and supervisory approaches.

The cyber risk regulation and supervision work program is demand driven, with most in-field work being conducted for the benefit of central banks and banking supervisors. Good practice recommendations arising from this work remain valid for other segments of the financial system also once their distinct business risk profiles are accounted for, because cyber-risk-management principles are consistent across industries.

The paper is targeted at subject matter experts, managers, and senior leadership of financial sector regulation, supervision, and oversight authorities. It is organized as follows. The remainder of this section sets out brief definitions of key terms and concepts in the area of cyber risk and presents important trends in the evolution of the cyber threat landscape. The next chapter provides an overview of the IMF's cyber risk work program and discusses how cyber risk is addressed in the IMF's Financial Sector Assessment Program (FSAP) and Capacity Development Technical Assistance (TA) work. Chapter 3 discusses good practices observed in the creation of relevant regulations and the requirements that make them effective in managing cyber risk. Chapter 4 offers insights on good practices in enforcing cyber risk regulations through prudential supervision and central bank oversight ("supervision and oversight"). Chapter 5 discusses cyber simulation exercises. Chapter 6 provides insights on system-wide cyber risk oversight, including FMIs. Chapter 7 concludes.

A. Key Concepts

The key concepts and terms used in this paper are as defined in the Financial Stability Board's (FSB) Cyber Lexicon (FSB 2023). Essential definitions are explained in the following section; for the rest, readers are referred to this source.

The definition of cyber risk relies on the concepts of "cyber," "cybersecurity," and "cyber incident," among others.

Cyber is defined as relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Therefore, cyber is not just about ICT, such as computers and networks, but equally encompasses people and processes that work with, or are supported by, ICT (which in turn store and process data). This also means that cyber risks stem from people and processes to the extent and in the context of their interaction with ICT.

Cybersecurity is the preservation of confidentiality, integrity, and availability of information or of information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability, can also be involved. Because cyber involves people and processes as well, cybersecurity deals with their security properties, issues, and solutions too. This is why, for example, employee background checks are part of cybersecurity measures.

Different information and information systems have different confidentiality, integrity, and availability requirements because they face different risks. Cybersecurity is achieved when those requirements are met. The strength of cybersecurity measures should be proportional to the requirements, and thus to the risks involved—not only from the perspective of an individual FI or FMI but from that of the system—that is, taking externalities appropriately into account. In other words, making the security posture and expenditure reasonable from an economic perspective. Underspending results in too much risk, and overspending leads to the inefficient use of funds. Given the presence of externalities, which are clear when cyber risk of systemically important FIs and FMIs is being considered, adequacy of risk mitigation and, correspondingly, reasonable cost will be seen differently by regulators and industry. This is at the foundation of cyber risk regulation and supervision.

A **cyber incident** is an event in the cyber domain (a cyber event) that either (1) jeopardizes the cybersecurity of an information system or the information the system processes, stores, or transmits; (2) violates the security policies, security procedures, or acceptable use policies, whether resulting from malicious activity or not; or (3) impacts any daily or normal operations of an organization's IT infrastructure.

An important characteristic of cyber incidents in this definition is that they do not necessarily breach cybersecurity; jeopardizing is sufficient. For example, a malicious actor unsuccessfully trying to exploit a vulnerability is a cyber incident, even though the system withstood the attack. Similarly, trying to read a file without appropriate access rights is a cyber incident, even if the attempt is blocked by the operating system. For obvious reasons, incidents that breach cybersecurity are dealt with much more emphasis in practical cyber-risk management.

Another key aspect of cyber incidents in this definition is that they may occur irrespective of intent. For example, events that occur because of user error or technology failure and can cause harm to information systems are also considered cyber incidents.

Cyber risk is the combination of the probability of cyber incidents occurring and their impact. This is the classic definition of risk applied to the cyber domain.[3]

The definition is broad because it is based on the similarly broad definition of cyber incidents. There is no universally held consensus in industry or among regulators whether cyber risk should include risk stemming from nonmalicious actions or technology failures. Sometimes the risk is split into ICT risk (stemming from nonmalicious actions such as errors or technology failures) and narrowly defined cyber risk (stemming from malicious activity). This is a valid approach; for example, it is useful to differentiate incident response based on the cause, whether it is a hacker attack or something else.[4] However, if it is extended to regulation, then it becomes difficult to neatly delineate ICT-risk-management and cyber-risk-management requirements in a way that avoids overlaps or inconsistencies. This is because many risk mitigation measures (also referred to as controls) are shared and effective on both fronts.

B. Evolution of the Threat Landscape

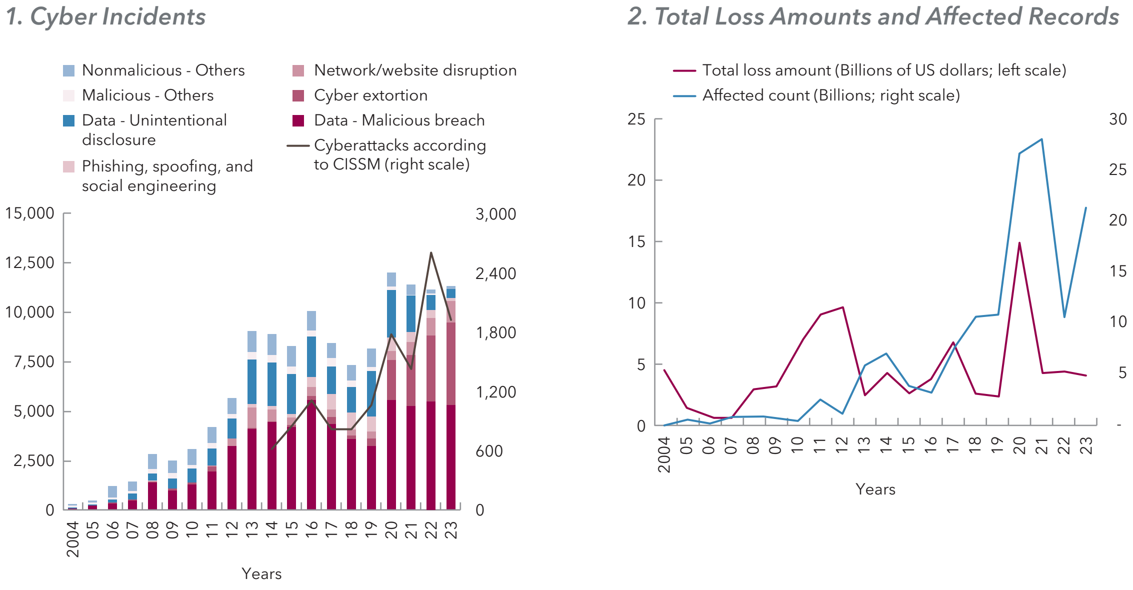
Cyber incidents have become much more frequent and more costly in recent times, especially since 2020. This is true for all incidents, whether with or without malicious intent. For example, the number of cyberattacks during a single year has almost doubled compared with 2019, with losses increasing by more than 25 percent, with an extraordinary spike of approximately 500 percent more in 2020 compared with 2019 (Figure 1).[5]

[3] In economics and finance, the notion of "risk" covers relevant risk factors to which a financial institution (FI) is exposed and, potentially, the likelihood of the realization or activation of these risk factors. The impact of the realization of risk is a function of the exposure to the activated risk factor(s) and the risk elasticity of the impact (that is, the sensitivity of the impact to the size of the risk-factor shock). The exposure and risk elasticity are commonly referred to as the vulnerability relative to the risk factor, and the impact is a combination of risk and vulnerability.

[4] The real cause may be unclear for some time—for example, whether an application stopped functioning because of a hardware failure or because an attacker crashed it.

[5] Partly because of COVID-19 pandemic-induced constraints and digitalization.

Figure 1. Selected Global Cyber Risk Metrics, 2004–25



1. Cyber Incidents

2. Total Loss Amounts and Affected Records

Source: IMF 2024c.

Cyber risk is especially prominent in the financial sector. Approximately 20 percent of all reported cyber incidents during the past two decades have affected the financial sector. Banks have been the most frequent targets, followed by insurers and asset managers. Total direct losses from reported cyber incidents impacting the financial sector from 2020 to 2023 stood at $2.5 billion (IMF 2024c). Cyber incidents are generally underreported, and indirect losses exceed direct losses by several multiples. Hence, total losses in the sector are very likely to be much higher than the reported amount.

Several factors contribute to this increase in cyber risk. From the technical perspective, there is increasing dependency on ICT, with faster financial innovation resulting in faster system development cycles and less time spent on testing and fixing software bugs—a major source of security vulnerabilities.

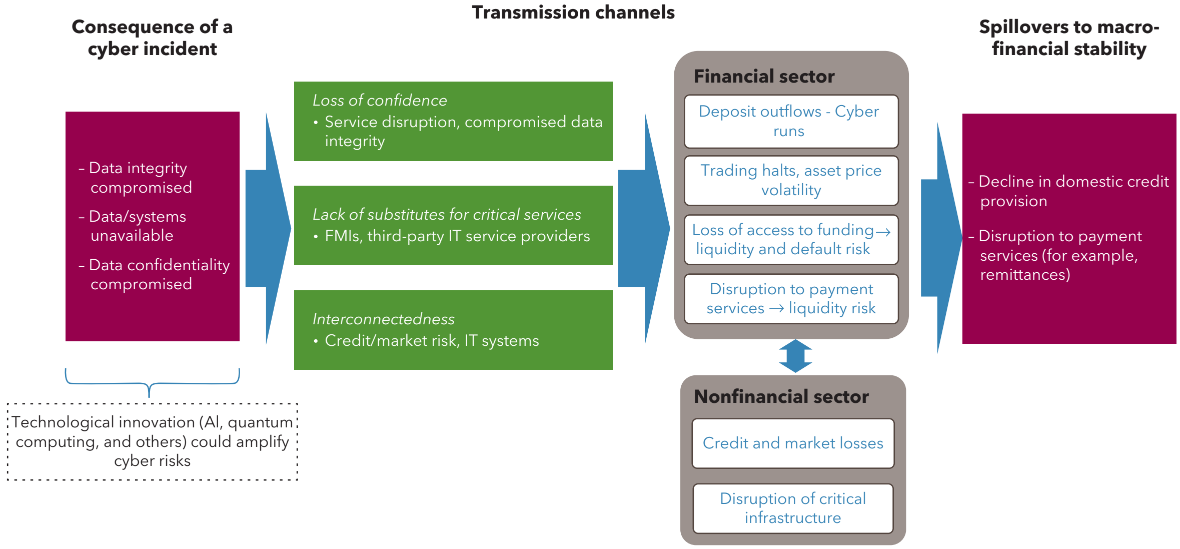
In addition, key trends in cyberattacks are driven not only by technological changes but also by geopolitics and economics. For example, the increase in next-generation phishing using deepfakes and advanced attack automation can be attributed to the widespread adoption of artificial intelligence (AI)-augmented capabilities (IMF 2024a). On the other hand, attacks on critical infrastructure are mostly attributable to rising geopolitical tensions and the increase in insider threats because of economic uncertainty.

C. Why Is Cyber Risk Important?

Cyber risk has emerged as a key material risk for the financial services sector in recent years. The reliance of financial services on ICT and the interconnectedness of the financial system mean that, besides causing significant losses and disruptions at individual institutions, large-scale cyber incidents at key FIs and FMIs can have systemic implications that may affect the continuity of financial services and trust in the financial sector, thereby compromising financial stability.

Cyber incidents can impact the financial system through three channels: loss of confidence, lack of substitutes for critical services, and interconnectedness (Figure 2).

Figure 2. Cybersecurity and Macrofinancial Stability: Channels of Transmission


Consequence of a cyber incident
Transmission channels
Spillovers to macro-financial stability
– Data integrity compromised
– Data/systems unavailable
– Data confidentiality compromised
Technological innovation (AI, quantum computing, and others) could amplify cyber risks
Loss of confidence
• Service disruption, compromised data integrity
Lack of substitutes for critical services
• FMIs, third-party IT service providers
Interconnectedness
• Credit/market risk, IT systems
Financial sector
Deposit outflows - Cyber runs
Trading halts, asset price volatility
Loss of access to funding→ liquidity and default risk
Disruption to payment services → liquidity risk
Nonfinancial sector
Credit and market losses
Disruption of critical infrastructure
– Decline in domestic credit provision
– Disruption to payment services (for example, remittances)

Source: IMF 2024c.

Note: AI = artificial intelligence; FMIs = financial market infrastructures; IT = information technology.

A cyber incident, such as a data breach or a prolonged disruption, may lead to a loss of confidence in the targeted FI, raising liquidity risks that may result in solvency issues and spill over to related parties. If a cyber incident halted an FMI that is not easily substitutable—for example, a real-time gross settlement system, a clearinghouse, or a trading system—then the functioning of the financial system itself could take a severe hit, likely affecting financial stability. Finally, the impact of a cyber incident can be transmitted through technological or financial links between firms, such as common software or the interbank market, respectively.

Progress in AI and quantum computing development accelerates the buildup of cyber risk. Besides cyber defense, AI can be deployed in offensive operations such as deepfake-based phishing and advanced attack targeting and automation. Quantum computing has the potential to break classic cryptography, thereby putting data confidentiality and integrity at risk.

Cyber risk requires increased regulatory and supervisory attention to avoid negative systemic implications, considering that cybersecurity is a shared public good necessary for the smooth functioning of the financial system and the broader economy.

2. IMF Work on Cyber Risk Regulation and Supervision in the Financial Sector

Given its mandate to promote the stability of the international monetary system, the IMF has made efforts on many fronts to promote the effective regulation and supervision of cyber risks. This has assisted member countries in strengthening the operational and cyber resilience of their financial systems.

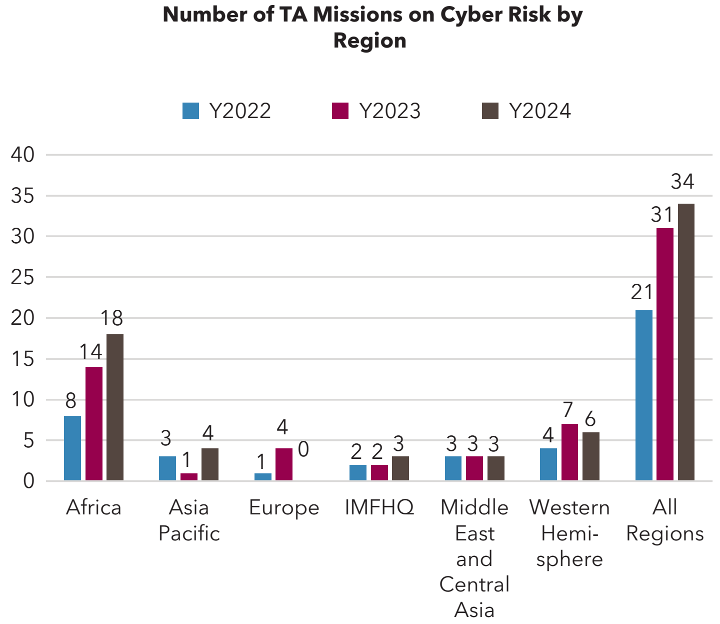
On the surveillance front, formal assessments of cyber risk supervision and oversight have helped monitor developments and strengthen policy frameworks across member countries. In 2019, the IMF began to pilot the assessment of this topic as part of its FSAP. This has mainly targeted advanced and larger emerging market economies, deepening the assessment of operational risks in the banking sector and of FMIs (Table 1). In addition to bilateral surveillance, the topic of cyber risks has also been covered in multilateral surveillance through the IMF's flagship publication, the *Global Financial Stability Report* (IMF 2024b).

Table 1. FSAP Missions with In-Depth Coverage of Cyber Risk

Year	Jurisdiction
2020	Norway United States
2021	United Kingdom
2022	Mexico South Africa
2023	Iceland Republic of Türkiye Sweden
2024	Japan Luxembourg Spain
2025	Canada Euro Area France India Switzerland

Source: IMF.
Note: FSAP = Financial Sector Assessment Program.

Figure 3. Number of TA Missions on Cyber Risk



Source: IMF, TA mission records.
Note: TA = Technical Assistance.

On capacity development, there has been a gradual increase in demand for TA to develop and strengthen cybersecurity regulations and supervisory frameworks. This has largely been tailored to emerging markets and developing economies (Figure 3). TA aims to achieve several outcomes: (1) enact or strengthen, in line with international standards, the legal and regulatory framework underpinning the implementation of regulation and supervision of cyber risk; (2) develop, strengthen, and implement the cyber risk supervisory framework; (3) ensure timely availability of information on cybersecurity threats and incidents to supervisors, who then follow up promptly, appropriately, and comprehensively; and (4) develop sufficient capacity to effectively supervise cyber risk.

To support the achievement of these outcomes in member jurisdictions, the Cyber Risk Supervisory Toolbox was developed by the IMF cyber risk supervision team. The toolbox encompasses eight important elements, including (1) model cyber risk regulation, (2) user guide for model cyber regulation, (3) assessment methodology, (4) user guide for the technology- and cyber-risk-management assessment tool, (5) assessment tool based on the model regulation, (6) supervisory processes, (7) examination guide, and (8) pre-examination document request. In addition to bilateral TA, the IMF has trained officials through regional workshops, hosted annual cybersecurity workshops, and proactively developed online tools[6] to enhance knowledge and skills on cybersecurity.

IMF staff have contributed to key policy developments in the financial sector. Under the leadership of the FSB, staff have contributed to the identification of effective practices in cyber incident response and recovery and to progress in harmonizing the regulatory reporting of cyber incidents, promoting fast response and recovery to safeguard financial stability. Such contributions also cover frontier topics such as

[6] Cyber Risk Regulation and Supervision online course (https://www.imf.org/en/Capacity-Development/Training/ICDTC/Courses/CRS).

AI and Privacy-Enhancing Technologies, which have implications for cybersecurity. Work with international standard-setting bodies such as the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), and the International Organization of Securities Commissions (IOSCO) has helped prioritize operational and cyber resilience across institutions, markets, and infrastructures, establishing expectations for the continuity of critical business services. IMF staff also collaborate with the Bank for International Settlements, International Telecommunication Union, World Bank, and World Economic Forum in the cyber risk area.

A. Cyber Risk Assessments in the FSAP

The FSAP, established in 1999, is a comprehensive, in-depth assessment of a country's financial stability outlook and risks and of the adequacy of the policy framework and tools to address threats to financial stability. It is a key instrument of the IMF's bilateral surveillance. Financial sector stability assessments under the FSAP are mandatory in jurisdictions with financial sectors deemed by the IMF to be systemically important and are expected to take place every five years as an integral part of the Article IV consultation. For all other jurisdictions, FSAP participation is voluntary.[7]

The primary reason cyber risk needs to be scoped into FSAP assessments is its potential to harm financial stability, as discussed in the previous chapter. Until as recently as 2019, FSAP assessments of cyber risks in the financial sector and of their supervision were done as part of the assessments of operational risk and of the resilience and oversight of FMIs, and not on a standalone basis. The latter practice was piloted in the cyber risk assessments in the 2020 Norway FSAP and the 2022 South Africa FSAP before gradually being extended to more countries (Table 1).

Where Does the Cyber Risk Workstream Fit in the Overall FSAP?

Cyber risk assessments can, in principle, align with all three pillars of the FSAP (Table 2). However, thus far, such assessments have covered the regulation and supervision of cyber risks by banking supervisory authorities and FMI oversight authorities, that is, under Pillar 2 of the FSAP, that focuses on the policy framework, oversight,[8] and governance.

Going forward, such assessments could extend to other FSAP pillars, subject to the availability of good-quality data and improvements in quantitative techniques. It is, in general, more challenging to assess the cyber resilience of the financial system compared with financial resilience for several reasons. Financial sector entities are hesitant to voluntarily disclose cyber incidents, fearing reputational damage, which leads to a dearth of reliable data. Cyber incident reporting arrangements vary across regulators, and convergence in this area is a work in progress.[9] Cyberattacks and their impact are unpredictable, and the source and evolution of such threats are wide-ranging, making quantification of risk exposure very challenging. Correspondingly, on the impact side, quantitative measures expressed in monetary value terms—standard for solvency risk analyses of banks—have limited value in providing a meaningful understanding of the impact of the realization of cyber risk and threats.

[7] Further details regarding the FSAP can be found at Financial Sector Assessment Program (FSAP, https://www.imf.org/en/Publications/fssa).

[8] This includes prudential regulation and supervision of FIs and oversight of FMIs.

[9] For international guidance, see FSB (2025).

Table 2. The Three Pillars of the IMF's Financial Stability Assessment Program

	FSAP Pillar 1 Macrofinancial Vulnerabilities/Risk Analysis	**FSAP Pillar 2 Policy Framework, Oversight, Governance**	**FSAP Pillar 3 Safety Net, Crisis Management/ Resolution**
Relevant for cyber risk?	Y	Y	Y
Key elements	Cyber strategy. Macro-level interconnectedness of digital landscape, cyber mapping. Financial stability analysis. Reckoning cyber risk/stress testing with cyber scenario. Cyber resilience stress testing. Threat landscape.	Cyber strategy for the financial sector. Institutional framework/legal framework. Regulations focused on cyber, information technology, business continuity, operational resilience, third- and fourth-party risks, cloud arrangements, digital onboarding, digital banks, incident reporting, information sharing, testing arrangements. Supervisory approach and framework; onsite and offsite supervision. Operational resilience arrangements. Leveraging independent audits and follow-up. Comparison of such arrangements for different sets of institutions, markets, and infrastructure.	Crisis management at the individual institutional level. ICT/cybersecurity arrangements conducive to resolution. Resilience arrangements. Crisis preparedness of the central bank and financial sector supervisory agencies.

Source: IMF Staff
Note: FSAP = Financial Sector Assessment Program; ICT = Information and Communication Technology.

The focus of FSAP assessments on the authorities' approach to cyber risk regulation, supervision, and oversight is based on the hypothesis that strong risk-management requirements, diligent enforcement, and continuous learning and recalibration are all vital contributors to enhancing cyber resilience.

The IMF's FSAP coverage of cyber risk regulation, supervision, and oversight is an invaluable source of identifying good practices in more advanced and large emerging market economies. Transposing them to the broader range of emerging market and developing economies can, nonetheless, be challenging because of significant differences in data availability and institutional and risk-management capacity in the private and official sectors as compared with countries where the FSAP has covered the topic.

B. Cyber Risk Technical Assistance

Recent years have shown an increase in digitalization and innovation within the financial sectors of emerging markets and developing economies. Given the increased use of technology within these financial sectors, there has been an expansion in the attack surface and, therefore, in cyber risk. Consequently, this has accentuated the need for strong cyber resilience within the financial sector of such countries. However, the greatest challenges they face are the lack of expertise, capacity, and resources in the field of cybersecurity. Within this context, the IMF's work program on cyber risk resilience in the financial sector is centered on providing TA to emerging markets and developing economies. Over the past four years, the IMF has delivered 108 TA missions to this group of countries on a wide range of topics, including the following:

- Developing a cyber strategy for the financial sector.
- Developing regulations focused on cyber, information technology, business continuity, operational resilience, third-party risks, and cloud computing.
- Developing cyber incident reporting frameworks.
- Establishing and operationalizing information and intelligence sharing networks.
- Conducting cyber simulations and exercises.
- Reviewing the cybersecurity of, and developing a cybersecurity framework for, central banks.
- Developing a cyber supervisory approach and framework, including onsite and offsite supervision.
- Enhancing operational resilience arrangements and applying the principles of operational resilience within the financial sector.
- Developing cyber testing frameworks.
- Building capacity and expertise of cyber risk supervisors.

Member country requests for TA on the topic of cyber risk have increased significantly over the past few years because countries realize the importance of this topic, and the risk continues to increase globally.[10] In all cases, the IMF teams work with country authorities and subsequently provide a comprehensive report that details the mission's outcome, its findings, and next steps. The TA report sets out the findings from the work, including in-field work with country authorities, and a set of recommendations for the authorities to implement over time. TA may include a review of existing regulations, development of a cyber risk supervisory manual, assistance with authorities' conduct of onsite inspections at commercial banks, and running a cyber risk simulation exercise, among others.

Finally, TA on this topic is not a one-off project or in-field mission but typically constitutes the basis of a longer-term engagement between the relevant authorities and the IMF. Given the increasing importance of cyber risk and its multidimensional nature, building cyber resilience is a long-term endeavor that requires several key building blocks (for example, strategy, regulation, supervision, incident reporting, simulation exercises) to be designed and implemented over a longer-term horizon. In this regard, building cyber capacity takes time and long-term commitment.

Based on the large number of TA missions provided by the authors over the years, several key observations can be made regarding the current situation in, and priorities of, emerging markets and developing economies in this area:

- They have significant work left to do in strengthening their cyber risk regulatory and supervisory frameworks. Although many countries now have strong regulations in place, their capacity to effectively supervise adherence to regulations is lacking, often because of the paucity of resources and expertise available to them.
- Most of these countries do not yet have cyber incident reporting frameworks in place, nor do they have information and intelligence sharing networks among the relevant agencies involved in their financial sector.

[10] The process for TA begins with a formal request to the IMF from the financial authority (for example, the central bank or supervisory authority) seeking assistance on cyber risk. After this request, the IMF undertakes a scoping exercise, engaging with the relevant authorities to better understand the country's requirements, its current regulatory and supervisory framework, and its needs to enhance cyber resilience. After the fact-finding exercise and once the scope is defined, the IMF works with the authorities in person to develop the tools, conduct the assessment, or deliver the required training.

- Most of these countries are yet to conduct cyber risk simulation exercises.
- Most of them are still trying to build a dedicated cyber risk supervision unit that can ensure that there is a comprehensive cyber strategy, robust regulation, and effective supervision.

Consequently, there is significant value in the IMF continuing to work with its membership to assist countries in undertaking a comprehensive, long-term work program to build cyber resilience, systematically building capacity in a structured manner. The work program should include developing a cyber strategy for the financial sector; ensuring there are appropriate financial sector institutional arrangements in place to manage cyber risk; putting in place a cyber regulation; conducting effective cyber supervision; enforcing a cyber incident reporting framework; conducting cyber simulation exercises; and building information and intelligence sharing networks, among other things.

3. Good Regulatory Practices[11]

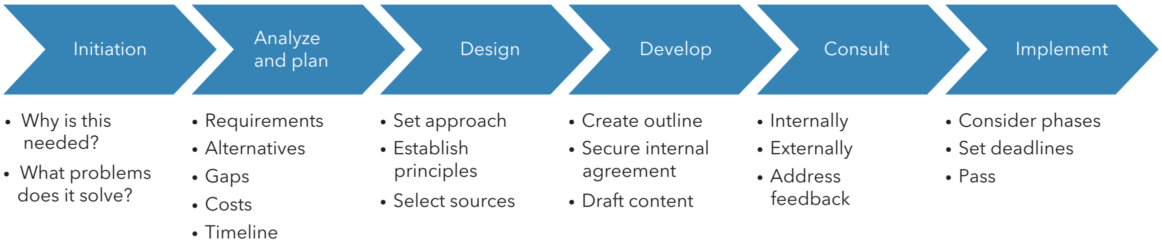
The key objective of cyber-risk-management regulation is to safeguard the confidentiality, integrity, and availability of information and systems within supervised entities. This entails building cyber resilience and responding to and recovering from cyber incidents caused by any threat, such as cyberattacks, technology and process failures, human error, and even natural or man-made disasters.

The regulatory framework is typically tiered, featuring mandatory requirements and guidance. Mandatory requirements can be enforced using the supervisor's legal powers. Requirements and recommendations whose enforceability is not essential are collectively referred to as expectations. The term "regulation" includes both mandatory requirements and guidance.

A. The Regulation Development Process

A deliberate and structured approach to regulation development helps deliver a set of effective and internally consistent cyber-risk-management requirements (Figure 4).

Figure 4. Example Regulation Development Process Flow



Source: IMF staff.

The key phases under this approach are "Analyze and plan" and "Consult."

In the "Analyze and plan" phase, the development team understands the following:

- What is required from the regulation (as opposed to what requirements the regulation will contain).
- Whether there are alternatives (such as amending an existing ICT-risk-management regulation instead of coming up with a brand-new cyber risk regulation).
- If there are alternatives, then what are the gaps that need to be addressed.
- At what cost and by what deadline can the regulation be developed.
- What costs (and nonmonetary burdens) the regulation will likely impose.

[11] Good regulatory practices outlined here may be equally applicable to FMIs when considered based on their risk profile and specific characteristics.

The "Consult" phase is crucial to ensure buy-in from internal and external stakeholders. Although requirements are ultimately set at the discretion of the regulator (bound by mandate and applicable laws), it is important that the industry is not unduly burdened with overlapping, inconsistent, or overly stringent requirements. Seeking feedback on the proposed regulation is key to achieving this goal.

Success Factors of Cyber Risk Regulation Development

When developing regulations, it is vital that they are clearly written and concise, with sufficient specificity in language and structure to facilitate supervisory assessment. Suggestions for developing regulations that are effective, coherent, and do not put an undue burden on institutions include the following:

- Strive for unified regulation that encompasses all technology risk areas instead of separate ICT and cyber risk regulations.
- Prefer principles-based and outcome-focused regulations. Consider more prescriptive approaches on an exceptional basis, based on the maturity of risk-management practices in the industry.
- Ensure that expectations are outcome-driven and technology agnostic.
- Allow flexibility in how exactly outcomes are achieved. There are often several ways to achieve a given outcome—that is, one size does not fit all. Flexibility is also needed to enable supervisors to follow a risk-based approach using professional judgment.
- Structure expectations according to a risk and control taxonomy (that is, categories of risks and controls) without requiring adherence to any specific cybersecurity or IT control standard. That said, it is beneficial to use a taxonomy that can be easily mapped to well-known standards or frameworks.
- Consider a tiered approach according to the proportionality principle to regulation when the size, complexity, and risk profile of supervised institutions differ significantly. A baseline would apply to all, to which successive tiers applicable for larger, more complex, and riskier entities would bring—gradually—greater and stronger expectations.

Principles-Based versus Prescriptive Regulatory Approaches

A principles-based approach enables the supervisor to establish more future-proof expectations for cybersecurity that can be interpreted to suit the individual circumstances of the FI and changes in the threat landscape or technologies. Principles-based regulation tends to be shorter and easier to maintain but requires a shared understanding of expectations between the regulator and industry. This approach tends to work best in more developed financial systems with mature risk-management practices.

A more prescriptive approach reduces uncertainty by stipulating more detailed expectations that are less open to divergent interpretations. It can benefit less developed financial systems with more fledgling risk-management practices. On the flip side, it leaves less room for supervisory judgment, challenges the implementation of a proportional approach, and may result in more voluminous and difficult-to-maintain regulations.

There is no dichotomy between principles-based and prescriptive approaches, but rather a continuum. Regulators need to strike an appropriate balance, considering the overall financial sector regulatory framework and the maturity of supervised entities. An approach that is primarily principles based is often more beneficial than one that tends toward greater prescription in this area because threats and technologies are fast evolving, and detailed prescriptive requirements tend to become obsolete faster than principles-based requirements.

B. Key Expectations that Facilitate Effective Risk Mitigation

There are many expectations in existing cyber risk regulations. When developing new regulations or amending existing ones, it is beneficial to prioritize those that contribute most to strengthening the cybersecurity stance of regulated entities. In this section, we outline several such requirements, taking a unified approach to ICT and cyber risk regulation. The list is not exhaustive and should be considered in the context of the cyber risk profile of the specific financial system.

Governance and Internal Controls

Arguably, one of the most impactful areas of regulation is governance and internal controls. Just as in the case of financial risk, proper organizational structures, reporting lines, policies, procedures, and the allocation of responsibilities go a long way in instilling an effective cyber-risk-management culture and practice across FIs.

Board of directors. The key roles and responsibilities of the board of directors include the following:[12]

- To possess the requisite experience to understand ICT and cyber risks and principles of risk management.
- To ensure an effective system of ICT and cybersecurity internal controls.
- To set ICT and cyber risk tolerance levels.
- To ensure that an ICT and cyber-risk-management strategy and framework are established and executed.
- To grant senior executives responsible for executing the technology-risk-management strategy sufficient authority and resources.
- To ensure that the risk management and internal audit functions are properly resourced to deal with ICT and cyber risks.
- To regularly review the technology-risk-management strategy and risk assessments.

Policies, standards, and procedures. FIs should establish policies, standards, and procedures and, where appropriate, incorporate industry standards and best practices to manage ICT and cyber risks and to safeguard information assets. Policies, standards, and procedures should be regularly reviewed and updated, considering the evolving technology and cyber threat landscape.

Management of information and ICT assets. FIs should (1) establish information asset management practices, including hardware, software, and data; (2) classify information assets based on their criticality; and (3) designate data owners and custodians with clearly defined responsibilities.

Security awareness. A comprehensive cybersecurity awareness training program should be established to maintain a high level of awareness among all staff, and also covering consultants and third-party vendors.

Budget for cybersecurity. Adequate budgetary provisions must be made to ensure compliance with set risk tolerances. The cybersecurity budget should be independent from the overall ICT budget of FIs.

Audit. The internal audit function should conduct assessments of cybersecurity controls, governance, compliance, and outsourcing processes. The internal audit teams should either possess the requisite qualifications for technical audits or have access to expertise from external service providers. High-risk observations and corrective actions taken should be reported to the board of directors without undue delay.

[12] The board will discharge those responsibilities based on the recommendations of CIO/CISO or senior management.

Technology and Cyber Risk Management

Risk-management framework. The FI should establish a risk-management framework to effectively manage ICT and cyber risks. All identified risks should be assigned to accountable risk owners responsible for implementing and enforcing appropriate risk treatment measures. The risk-management process should be executed on a regular basis. FIs should review the adequacy and effectiveness of their risk-management framework regularly and implement corrective measures as necessary. A summary report on the results of the risk-management process, a risk register, and a remediation plan should be prepared for board approval on a regular basis.

Risk assessment and treatment. FIs should (1) estimate the likelihood of threats exploiting vulnerabilities, (2) estimate the magnitude of the consequences should threats successfully exploit vulnerabilities, (3) assign a risk-level metric to each risk based on these estimations, and (4) develop and implement risk mitigation measures that are consistent with approved risk tolerances.

Risk monitoring, review, and reporting. FIs should institute a process for monitoring changes in risk. Major risks should be monitored closely and reported regularly to the board of directors and senior management.

Project management framework. A project management framework should be established to ensure consistency in project management practices and the delivery of outcomes that meet project objectives and requirements. The framework should cover the policies, standards, procedures, processes, and activities from project initiation to closure. As part of this framework, a stage-gate mechanism should be implemented to validate security adherence at each phase of the project lifecycle, ensuring that risks are proactively identified and addressed before progressing to subsequent stages.

System acquisition and development lifecycle. FIs should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the project's criticality. FIs should establish a framework to manage their system development lifecycle that defines the processes, procedures, and controls in each phase of the lifecycle, including initiation/planning, requirements analysis, design, implementation, testing, and acceptance. Standards and procedures for different phases should be maintained. Security specifications and tooling should be integrated and evaluated consistently across all phases of the system development lifecycle, with strict adherence to established security practices.

ICT Service Management

ICT service management framework. A framework for supporting IT services and operations should be implemented. The framework should encompass governance structures, processes, and procedures for well-defined ICT service management activities, such as asset and configuration management, technology refresh management, patch management, change management, software release management, incident management, and other related activities.

Documentation. Systems and services should be documented in a way that enables skilled substitute staff to run ICT operations with minimal disruption.

Data center (DC) security. FIs should conduct a risk assessment for their DCs to identify potential vulnerabilities, weaknesses, and protective measures to safeguard the DCs against physical and environmental threats. The risk assessment should be reviewed whenever there are significant changes in the threat landscape or in the DCs' environment. FIs must also ensure adequate redundancy for power, network connectivity, cooling, and other electrical and mechanical systems within the DC to minimize single points of failure. DC physical security and environmental controls should be monitored on a 24/7 basis. Escalation and response plans and procedures for physical and environmental incidents at DCs should be established and tested.

Physical and environmental controls. Physical security should cover all physical infrastructure of FIs, including data centers and disaster recovery sites. Controls should include physical access controls, surveillance, and protection against both man-made and natural threats.

Asset and configuration management. FIs should (1) implement a configuration management process to maintain accurate information about hardware and software, (2) review and verify hardware and software configuration information on a regular basis to ensure it is accurate and up to date, and (3) use standardized configurations and software images whenever possible.

Technology refresh and patch management. (1) FIs should avoid using outdated and unsupported hardware or software. A technology refresh plan for the replacement of hardware and software before they reach end of support should be developed. (2) A patch management process should be established to ensure timely implementation of applicable functional and nonfunctional patches (for example, fixes for security vulnerabilities and software bugs) based on the criticality of the patches in relation to the FI's IT systems. Patches should be tested before applying them to the production environment to ensure compatibility and avoid introducing problems to the ICT environment.

Change management. FIs should establish a change management process to ensure that changes to information systems are assessed, tested, reviewed, and approved before implementation. A risk assessment of the change should be conducted before implementing the change.

Incident management. FIs should (1) establish an incident management framework with the objective of recovering affected ICT services or systems to a secure and stable state as quickly and as safely as possible; and (2) maintain a knowledge base that captures lessons learned from resolving incidents, including root cause analyses.

Identity and access management. (1) An identity and access management (IAM) process should be implemented to provision, change, and retire accounts and access rights to information assets. Access rights should be granted according to the "need-to-know" and "least privilege" principles and approved by the appropriate parties, such as information asset owners. (2) Strong password/passphrase controls should be enforced for users' access to ICT systems. At a minimum, multifactor authentication should be enforced for privileged accounts and remote access. (3) Periodic user access reviews should verify the appropriateness of access granted to users. Exceptions noted should be addressed as soon as practicable. Privileged access, such as the use of system administration rights, should be monitored and assessed regularly.

Data security and privacy. (1) FIs should adopt measures to detect and prevent unauthorized access, modification, copying, or transmission of confidential data. Data in motion, data at rest, and data in use should be considered in tandem. (2) The use of confidential production data in nonproduction environments should be restricted. (3) Data on storage media, systems, and endpoint devices should be permanently erased before disposal or redeployment to ensure confidentiality and security.

Cybersecurity Operations

Threat intelligence. FIs should establish a system to collect, process, and analyze cybersecurity-related information for its relevance and potential impact on their business and ICT environments. This should include information from voluntary and collaborative industry and national information-sharing networks, where such networks exist. Active participation in such networks is recommended.

Cyber event monitoring and detection. To ensure timely detection of cyber incidents, FIs should establish a security operations center, obtain managed security services, or at least run cyber incident monitoring, detection, response, and recovery functions.

Cyber incident response, management, and reporting. FIs should establish a cyber incident response and management plan to swiftly isolate and neutralize cyber threats and securely resume affected services. The plan should outline communication, coordination, and response procedures to address plausible cyber threat scenarios and be integrated with wider crisis response and management plans across the FI. Lessons learned from cyber incidents should be used to enhance existing controls and improve the cyber incident management plan. Cyber incidents must also be reported to the supervisor and oversight authority according to prescribed criteria and within specified timeframes.

Response and Recovery

Business continuity management and disaster recovery. FIs should establish a business continuity management process, including (1) business impact analysis; (2) determination of recovery time objectives and recovery point objectives; and (3) development, training, testing, and maintenance of recovery plans for systems and business processes. Plans should be updated and tested after significant changes in ICT systems and business processes, or at least annually, to ensure they remain effective.

Backups. (1) FIs should establish a comprehensive backup regimen, enabling recovery in the event of system disruption, data corruption, or deletion. Data archival for long-term retention should be included in the policies and procedures. (2) Physical and logical access to backup media, especially for write access, should be strictly limited to authorized staff, systems, and processes. (3) To address ransomware risks properly, FIs should consider immutable backups for critical data. (4) Backups of critical data should be redundant (for example, at least in two equivalent copies) and stored in separate secure locations that are unlikely to be affected by the same disaster. (5) FIs should periodically perform test restorations from backups.

Vulnerability Scanning, Tests, and Exercises

FIs should (1) establish a process for regular vulnerability scanning; (2) carry out penetration testing to obtain an in-depth understanding of the effectiveness of their cybersecurity stance; (3) ensure that their external-facing digital services are subject to penetration tests at regular intervals—at least annually—and after significant changes to underlying systems; (4) conduct regular cyber exercises to validate their cyber incident response and recovery procedures, including communication plans. These exercises could include tabletop exercises and attack simulations. In addition, they could be combined with penetration testing and business continuity/disaster recovery testing; and (5) establish a comprehensive remediation process to track and address issues identified through vulnerability scanning, penetration testing, and cyber exercises. The frequency of scanning, testing, and exercises should be commensurate with the criticality of the ICT systems and the security risk.

Independent Assurance

FIs should ensure that independent ICT and cyber risk audits are performed to provide their boards of directors and senior management with objective opinions on the adequacy and effectiveness of their risk management, governance, and internal controls relative to their existing and emerging technology risks. The scope and frequency of the audits should align with the criticality and risk profile of their information assets, functions, and processes. At a minimum, FIs should employ internal audit staff with the competence and skills to develop an annual ICT and cyber risk audit plan and understand the findings and recommendations of specialist external providers.

Outsourcing and Technology Service Provider Management

The outsourcing of functions or the use of technology service providers (TSPs) does not absolve FIs or their boards of their responsibilities. FIs remain responsible and fully accountable for complying with all their regulatory obligations regarding the functions they outsource or otherwise deliver using TSPs.

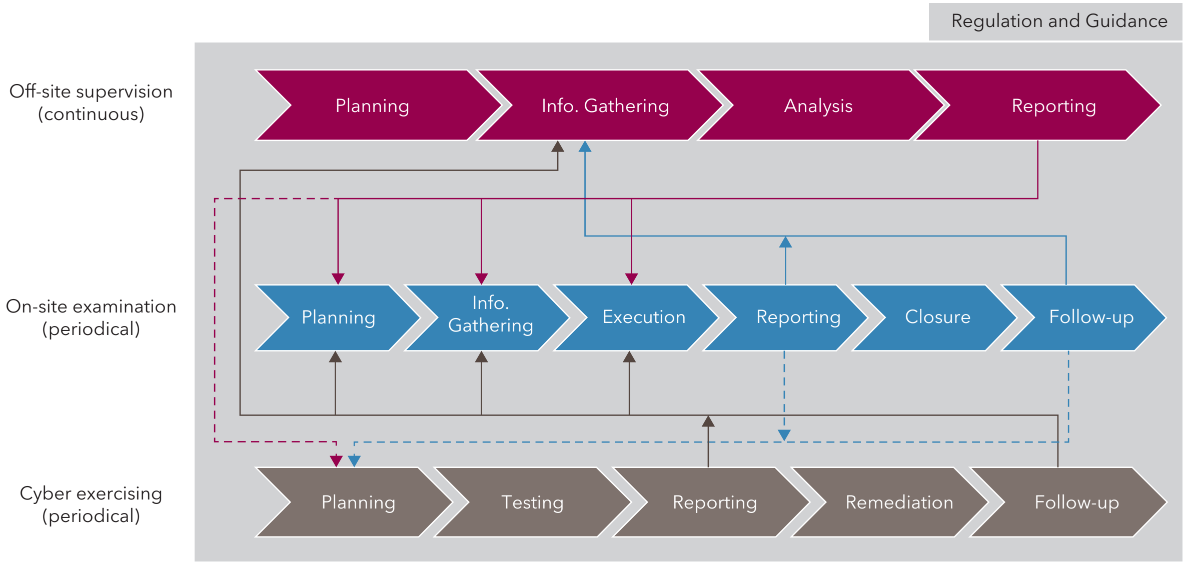
FIs must ensure that the use of TSPs, including for outsourcing, does not result in increased ICT and cyber risks. A risk assessment and a due diligence review should be undertaken before entering into a contract with a TSP. Contracts should explicitly reserve the right for the regulator/supervisor or its designees to audit the TSP to the extent of its involvement in delivering services for the FI. The risk assessment should be regularly updated to ensure accuracy.

4. Good Supervision Practices[13]

Supervision agendas in cyber risk supervision generally focus on four core processes: regulation and guidance development (discussed earlier), offsite supervision, onsite examination (also called inspection), and—increasingly—monitoring of cybersecurity testing. More granular priorities can be established within these processes. For example, an authority might prioritize financial stability analysis and information sharing in offsite supervision or monitor security testing in onsite supervision.

Rather than existing in isolation, these core processes work collaboratively to provide a comprehensive approach. Figure 5 shows a generalized model of the core processes and their interlinkages, reflecting good practice.

Figure 5. Core Supervisory Processes and Interrelationships



Source: IMF.

Supervisors should continually monitor the cybersecurity defenses established by FIs, prioritizing those that are systemically important. This calls for continuous offsite supervision and regular onsite examinations, with the supervisory attention afforded to any given FI being proportionate with its cyber risk profile and systemic importance, as explained in greater detail in section D of this chapter.

[13] Good supervisory practices outlined here may equally be applicable to FMIs when considered on the basis their risk profile and special characteristics. The authors recommend enhanced supervision of FMIs in place of oversight.

A. Governance and Management of Cyber Risk Supervision

Several jurisdictions have adopted the Basel Core Principles for Effective Banking Supervision (BCP), including those related to ICT and cyber risk, albeit supervision authorities exhibit broad variability in their internal governance and in the management of their cyber responsibilities.[14] In this section, we put forward observed practices that contribute most to the effective discharge of relevant supervisory responsibilities as per the aforementioned standards.

BCP 25 on operational risk and operational resilience has been extended to enhance the supervisory focus on the effectiveness of[15] banks' governance, operational risk management, business continuity planning and testing, mapping of interconnections and interdependencies, third-party dependency management, incident management, cybersecurity, and ICT. The Toronto Centre advises supervisory authorities to ensure that their supervisory approaches and practices are sufficiently wide-ranging to cover the revised core principles.[16] Importantly, this includes (1) setting regulatory requirements and supervisory expectations on FIs to put in place arrangements and procedures to enable them to respond to and recover promptly from operational disruptions, in addition to any requirements on FIs to reduce the probability of operational disruptions occurring; and (2) assessing the credibility and likely effectiveness of the plans made by FIs to respond to and recover from operational disruptions, and intervening where these plans are inadequate.

Based on these standards and related guidance, the responsibilities of a prudential banking supervision authority include the following:

- Requiring FIs to have appropriate ICT/cyber strategies, policies, procedures, systems, controls, and processes that are consistent with their risk profile, systemic importance, risk appetite, tolerance for disruption, and emerging risks, and are approved at an appropriate level of management or the board.
- Expecting FIs to identify and protect themselves from threats and potential failures, and to respond to and recover from ICT/cyber incidents.
- Requiring FIs' boards to oversee senior management with respect to implementing the policies and procedures and having the capacity to identify external and internal threats and potential failures in people, processes, and systems on an ongoing basis.
- Expecting FIs to identify their critical operations, mapping the people, technology, processes, data, facilities, third parties, interconnections, and interdependencies required to deliver such operations through disruption.
- Requiring FIs to have response and recovery capabilities.
- Requiring FIs to conduct business continuity exercises under a range of severe but plausible scenarios to test their ability to deliver critical operations through disruption.
- Ensuring FIs have the capacity to compile and analyze ICT/cyber incident data with sufficient granularity and to facilitate appropriate reporting mechanisms to the board and the supervisory authority.
- Ensuring FIs understand the risks associated with third parties and manage them appropriately.

[14] The BCBS amended the BCP in 2024, issued *Principles for Operational Resilience* (2021), *Revised Principles for Sound Management of Operational Risk* (2021), and *Principles for Sound Management of Third-Party Risk* (2025), focusing more on ICT and cyber risks and articulating its expectations for supervisors.

[15] Given the mandate of the BCBS, the principles apply to banks; however, the broader thrust of the principles is equally applicable to FIs in general.

[16] Toronto Centre Note (TCN) on Operational Resilience.

- Requiring FIs to implement a comprehensive, appropriately resourced change management process that includes adequate controls and risk oversight.

In addition, the supervisory authority is expected to identify any common points of exposure across FIs to ICT/cyber risk or potential vulnerabilities arising from the fact that many FIs depend on common service providers, technology, or geographies, and to assess concentration risk-related arrangements that could potentially trigger systemic risks.

Given the wide range of activities to be performed by the FI supervisors, the governance of cybersecurity supervision is paramount. Good practices in this regard are as follows:

- Boards of the supervisory authorities set the agenda for cybersecurity supervision.
- Having a combination of on- and offsite supervision arrangements.
- Providing human, technological, and financial resources in adequate quantity and quality.
- Clearly assigning responsibility and accountability for the supervision and oversight of ICT/cyber risk.
- Integrating cyber risk assessments with the overall enterprise-wide risk management results to obtain a holistic picture.
- Onsite supervision techniques to include the entire range of options, for example, full scope, limited scope, thematic examinations, and short visits.
- Using technology to monitor activities will make the process more efficient and effective. It is useful for monitoring the compliance level.
- Conducting stress tests considering a severe but plausible cyberattack or cyber incident scenario will help make the board more sensitive to cyber risks.
- Cyber resilience testing is an emerging practice contributing to better preparedness.
- Data collection is a key supervisory component—this may include key risk indicators, organizational structure, third-party registers, relevant policies, board agenda items on ICT/cybersecurity, data for mapping, data for preparing dashboards and risk profiles, and incident reporting both at the individual level (beyond a threshold) and at a summary level covering all incidents.
- Capacity building among various stakeholders.
- Facilitating information sharing between financial sector entities.
- Improving coordination among various units within the central bank and other stakeholders (for example, law enforcement and government agencies).

Staffing, Planning, and Resource Allocation

Paucity of resources is a universal challenge because supervisors and overseers seldom get what they desire. However, this challenge is particularly pressing when it comes to emerging risks like ICT/cyber risks, and even more pronounced in emerging markets and developing economies. Resourcing depends heavily on which model is followed for assessing cyber risks. In addition to budget constraints, the issue is exacerbated by the size and quality of the available pool—for example, supervisors may have approved positions but are unable to fill them.

Many advanced economies approach resource management by incorporating cyber risk assessments into specialized risk units within their supervision and oversight authorities. Any general supervisory team that prioritizes assessing the cyber risk of a supervised entity makes a request for resources from this unit. Such arrangements have multiple benefits, including cyber risk assessments being done by specialists; integration of the results into the overall risk assessment; and ensuring that the outcome is beneficial both to the supervisors and the supervised entities.

In countries where setting up a specialized risk assessment unit or a specialized unit for ICT/cyber risk is infeasible, a set of examiners with relevant audit backgrounds is often selected to conduct ICT/cyber examinations and is provided with relevant training and exposure to carry out their duties.

In cases where the supervision department does not have enough skilled resources to conduct such examinations, it is common to leverage the skill set available in other domains—such as information technology, payment systems, risk management, and internal audit departments—within the central bank or supervisory authority. Although this arrangement is useful in the short to medium term, given the direction of digitalization, such capabilities need to be built within supervision departments in the long term.

Cyber risk tends to increase in tandem with digitalization, and given the interconnectedness of the financial system, the focus needs to be on the weakest link. Thus, the approach to risk profiling needs to be nuanced. Further, supervisors are also responsible for sector-wide cyber risks and may need to collect information relevant to identifying risk concentrations and take corresponding remedial action. It is desirable that at least two resources be allocated to ICT/cyber risk assessment, even in smaller jurisdictions, to ensure proper checks and balances and discussions on the pros and cons of various measures.

Although it is necessary to involve specialist technical skills in cyber risk assessments, many governance, risk management, and audit-related aspects can usefully be covered by experienced generalist supervisors. In addition, leveraging external audit firms is a good stopgap arrangement until the required skill sets are built within the supervisory authority.

Background checks on identified cyber risk supervisors are a must, given that they will have access to sensitive information about the financial sector and will deal regularly with FIs and their critical third parties. Upskilling and retention are challenges in this area of specialization. Leveraging technology to automate and analyze supervisory information can make the process more efficient and reduce the demand for human resources to some extent.

Learning and Development

Cybersecurity is a dynamic domain with continuous development. Supervisors and overseers need to pay attention to building capacity to keep abreast of developments and acquire the necessary skills to effectively discharge their responsibilities. Learning and development are important elements in ensuring effective cybersecurity supervision, both for jurisdictions that are strengthening this supervision and for those that are already at a sufficient level of maturity to keep pace with market developments. A notable challenge lies in developing resources who are not only good supervisors but also technically capable. Given this challenge, some authorities select general supervisors and provide them with technical training, and others recruit technical staff and provide them with supervisory training.

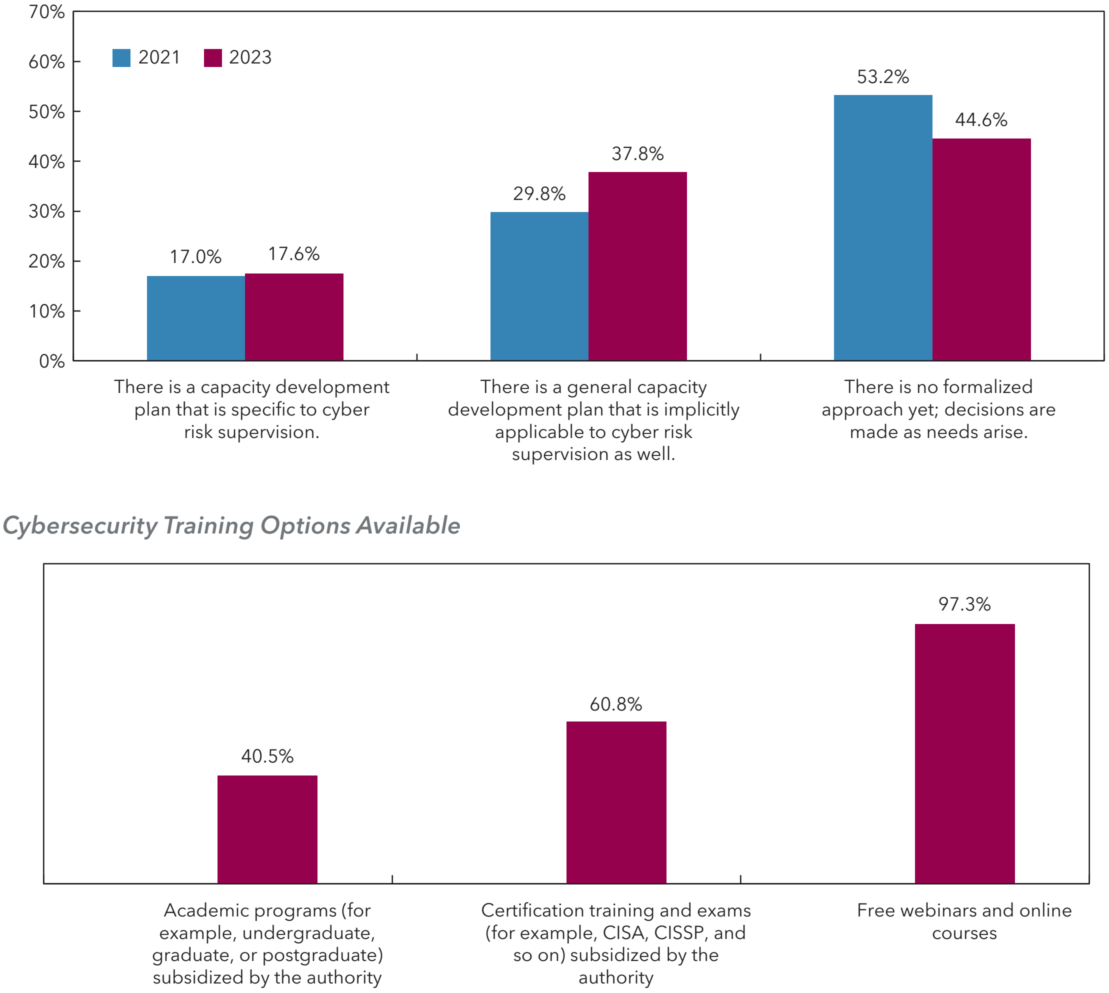
It is good practice to develop an onboarding program for cyber risk supervisors. Such programs ideally should cover the banking and financial structures of the country, technologies deployed by local entities, the current and evolving threat landscape, current levels of maturity of the entities, governance and risk-management expectations from supervised entities, the critical role to be played by the supervisors, and what it takes to do the job effectively. IT and cyber academic qualifications and professional certifications maintained on an ongoing basis help ensure that the right skills are available.

Periodic debriefing sessions among supervisors in a formalized forum can facilitate the sharing of industry practices and supervisory responses. Rotating supervisors periodically among regulation development, offsite supervision, onsite supervision, incident reporting and response, and testing and exercises could help in achieving all-round development for the team.

A survey on learning and development practices regarding cybersecurity indicates that jurisdictions heavily depend on free webinars and online courses, followed by certification training and exams (for example, CISA, CISSP, and so on), and academic programs (for example, undergraduate, graduate, or postgraduate) subsidized by the authorities (Figure 6(2)). About two-thirds of the authorities mandate an academic degree in IT to become a cyber risk supervisor. Some authorities require cyber risk supervisors, both at the senior level and for all staff levels, to obtain and maintain professional certifications, though such requirements are not mandated by about 20 percent of jurisdictions. In terms of having a capacity development plan, 17 percent had a plan focused on cyber risk supervisors, 38 percent had a general plan focused on all supervisors but not one focused on cyber risk supervisors, and 45 percent addressed capacity development without having any plans (Figure 6(1)).

Figure 6. Continuous Learning and Capacity Development

1. Approach to Strengthening Cyber Risk Supervisory Capacity



2. Cybersecurity Training Options Available

Sources: Survey responses, IMF, and Ravikumar (2025).
Note: CISA = Certified Information Systems Auditor; CISSP = Certified Information Systems Security Professional.

For capacity development among stakeholders, workshops with key stakeholders remained the preferred option. Interviews, speeches, and publications by supervisory authorities also helped build awareness and capacity. Participating in or encouraging public-private partnerships and cooperation with academic institutions was another way authorities built capacity.

B. Proportionality

Proportionality in financial sector supervision refers to the principle that regulatory requirements and supervisory practices are calibrated according to an institution's size, complexity, systemic importance, and risk profile. This approach aims to balance effective supervision with the need for consistency and compliance. For systemically important and complex FIs, the highest standards need to be applied. For smaller, less sophisticated, non-systemic FIs, supervisory expectations may be adapted to align with the institutions' risk profiles.[17]

Proportionality can be applied in the regulatory framework and through supervisory practice. Proportionality allows the supervisor to maintain a single rulebook for all regulated entities that can be applied across the entire industry and be calibrated according to the institution's size, scale, and complexity.

In terms of supervisory practice, applying proportionality means that resources and supervisory intensity can be adjusted to suit the size, scale, and complexity of regulated entities. In this way, supervisors can adapt their approach to align with the risk profile of an FI. For example, the frequency, scope, and depth of onsite examinations can be scaled up for the largest and most important systemic FIs. Supervisors may wish to schedule these FIs on an annual cycle of onsite examinations, dedicating their attention to asking in-depth questions and sample testing. Equally, for FIs with relatively aggressive business models that heavily rely on digitalization, supervisors may target these institutions for more intensive supervision.

Regarding actual IT and cybersecurity controls, proportionality can be implemented by varying the maturity expectations of control procedures in line with the complexity, size, and risk profile of the institution, whereas most control objectives remain the same for all institutions.[18] This means that most controls required by regulations are expected to be operational and effective at all supervised institutions, even as larger and systemic institutions are expected to operate more mature control procedures—for example, by using dedicated systems and automation.

Examples

Penetration testing is an example where supervisors can tailor their expectations using proportionality in the regulatory framework and supervisory practice. Security reviews are crucial for FIs to test their exposure to cyber threats as well as their ability to prevent, identify, respond, and recover. A baseline expectation could be set that all regulated entities undertake security testing at some frequency. For example, a regulation may require that all FIs undertake penetration testing on a regular basis. This is a high-level principle that FIs can interpret based on their risk profiles.[19] For larger and systemic FIs, the best practice is to have penetration testing performed at least annually by an independent and globally recognized third party. For less systemic FIs, the frequency may be adjusted. The third party may be an intra-group function in the case of foreign FI subsidiaries, and the scope of the test could be narrowed. In terms of supervisory practice, at a minimum, the supervisor should receive the executive summary and issues list, track the issues to remediation, and consider them when calculating the supervisory risk rating.

[17] The Basel Framework, which sets minimum requirements for internationally active banks in Committee-member jurisdictions, also allows for a degree of proportionality by providing options to implement simpler standardized approaches.

[18] A suitable maturity model should be used, such as the Capability Maturity Model Integration (CMMI).

[19] Jurisdictions may prefer to issue more specific requirements; however, in such cases, proportionality must be explicitly addressed in the regulation rather than through supervisory practice.

Requirements for organizations to establish a Chief Information Security Officer (CISO) function and position are another area where proportionality may be applied. Many countries stipulate the need for FIs to appoint a senior staff member with responsibilities for oversight of information security and cyber risk. Typically, the requirements are for this to be a senior staff member—part of the senior leadership team—and for the CISO to have a degree of independence. Many countries require that the CISO be considered a second line of defense and, therefore, exhibit a certain degree of independence from the functional responsibilities for technology within the organization. In some circumstances, for smaller FIs, it may not be feasible to assign a senior leadership member to oversee information security. In situations where the local talent pool is scarce, the limitations may prohibit separating staff with responsibility for information security in the functional area of the FI and the second line. In these circumstances, supervisors may adapt the expectations for a CISO correspondingly.

An example of applying proportionality by varying the expected maturity of the control procedure is IAM. All entities are required to control identities (user IDs) and access to systems based on the principles of "need-to-know" and "least privilege." A small institution with few employees may use a manual solution or Active Directory.[20] But complex institutions with a large user base and a heterogeneous system architecture are expected to deploy a dedicated IAM system with proper interfaces to business and HR systems and automation because, without such a solution, they are very unlikely to meet the requirements.

FIs and FI groups are required by their supervisors to have robust corporate governance policies and processes covering, for example, strategic direction, group and organizational structure, control environment, responsibilities of the banks' boards and senior management, and compensation. Supervisors may need to consider proportionality for differentiating qualitative requirements applicable across a range of FIs, particularly those related to corporate governance and risk management.

Board awareness of technology risk and cybersecurity is fundamental to applying corporate governance and asking the right questions. In practice, what has been observed is that boards rarely have sufficient in-depth understanding of technology risk and cybersecurity standards. In many small jurisdictions, boards lack representation of cyber or technology professionals. In terms of proportionality, a tailored approach can be applied to a smaller FI with a simple business model and relatively straightforward technology stack, but ultimately a baseline level of knowledge will be required. The proportional aspect is that in such cases, technological expertise and experience—including with respect to cybersecurity—can be isolated in one board member or an expert the board has regular access to, allowing for accumulation over time.

Proportionality and Nonfinancial Risks

It is less clear how proportionality can be calibrated for nonfinancial risks such as cyber risk, or more broadly, operational risk. Consequently, this involves greater supervisory judgment, which is yet another argument in favor of principles-based regulation. For example, in measuring operational risk under Basel II, although adjusting the metrics for the basic indicator approach is generally straightforward, it is less clear what aspects are tailored in the application of proportionality in the case of operational-risk-management standards. A case in point is the need for business continuity planning and testing. For a globally active bank, it is generally agreed that a full business continuity planning test across the enterprise should be performed at least annually. For non-internationally active banks, the application of proportionality is up for debate—is it the frequency we adjust, the complexity of the test, or both?

[20] Active Directory (AD) is a directory service for Windows systems, which are predominant at smaller institutions. It comprises a central database and a set of services that manage user accounts, computers, and other resources within a network.

Challenges

Challenges remain for jurisdictions that have adopted or are considering adopting proportionality in cyber risk regulation and supervision. These challenges arise during the design of the proportionate approach (for example, how to define the tiering criteria, how to maintain a level playing field, and how to avoid opportunities for regulatory arbitrage) and after proportionality is implemented (for example, how to achieve a net reduction in compliance costs and stress on supervisory resources and constraints). It is important to note that in an interconnected chain, security is as strong as its weakest link.

In conclusion, proportionality helps supervisors closely align expectations of risk management and governance with FIs' risk profiles, complexity, and systemic importance. Through routine engagement, the supervisor can provide guidance to firms about changes in standards and expectations that keep pace with industry developments. This is especially necessary for a technical area where the pace of change is dynamic and industry practices evolve rapidly. Proportionality can be applied across all FIs in a jurisdiction. It can also be applied to different groups of FIs within a jurisdiction—for example, internationally active FIs are required to fully implement all requirements, whereas other, smaller, and simpler FIs are required to implement a limited or simplified set of requirements.

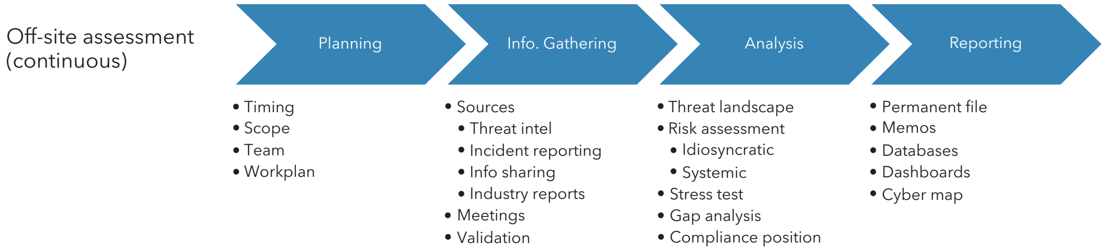
C. Offsite Supervision

Overview

The evolution of supervision has been significantly shaped by technological advances and the increasing complexity of cyber threats facing FIs. Offsite supervision has emerged as a critical component, particularly in the realm of cybersecurity, where continuous monitoring and rapid response capabilities are essential. This supervisory approach enables regulatory authorities to maintain ongoing awareness of FIs' cybersecurity posture without the traditional constraints of physical presence, allowing for more flexible, efficient, and comprehensive risk assessment processes.

Offsite supervision enables supervisors to conduct continuous monitoring of FIs' cybersecurity frameworks and risk-management systems. This approach enables supervisors to track key cybersecurity metrics, analyze threat intelligence reports, and assess the effectiveness of security controls without disrupting daily banking operations. The monitoring capabilities allow authorities to identify emerging cyber risks and vulnerabilities more quickly than traditional onsite examination schedules would permit, creating opportunities for proactive intervention before cyber incidents worsen. Furthermore, offsite supervision facilitates the collection and analysis of standardized cybersecurity metrics across multiple institutions, enabling supervisors to identify industry-wide trends, common vulnerabilities, and best practices that can be shared across the financial sector (Figure 7).

Figure 7. Offsite Supervision Phases



Source: IMF.

Good Practices

Modern offsite supervision leverages advanced technological tools ("SupTech") and secure communication platforms. The use of secure document-sharing systems, encrypted communication channels, and sophisticated data analysis tools enables supervisors to conduct thorough reviews of cybersecurity policies, incident response procedures, and technical security controls remotely. This technological integration allows for more frequent and detailed cybersecurity assessments, because supervisors can access and analyze large volumes of security data and compliance documentation while being less time constrained compared with traditional onsite examinations.

Planning

It is essential to develop an annual offsite cyber risk supervision plan that includes the timing and scope of activities and assigns team members to activities.

Information gathering and sources of information

An effective approach to offsite supervision of cyber risk allows the supervisor to monitor continuously and identify emerging risks early. To achieve this, a predefined set of minimum reporting requirements for both quantitative and qualitative information should be established, allowing the supervisor to review it throughout the supervisory period as part of offsite analysis based on regular reporting of metrics associated with the technology stack. The place to start is the cyber risk tolerance statement. This should form the backbone of supervisory monitoring of regulated entities' compliance with their internal limits and tolerances for cybersecurity and information security writ large. Institutions should be required to submit key documents that form part of the risk-management framework and business strategy, including, but not limited to, business plans, strategic plans, investment plans, operational expenditure, risk registers, and audit reports. Taken together, these documents help the supervisor understand and evaluate cybersecurity holistically.

Annual qualitative information should be submitted for offsite supervision. These documents provide insights into an FI's risk-management framework, governance processes, and the effectiveness of the three lines of defense. Examples include an FI's policies and processes, strategic business plan, technology plan, and technology spending. Key documents that inform an assessment of technological risks and cybersecurity include the following:

- Risk tolerance statement.
- Business, ICT, and cybersecurity strategies.
- Internal audit plan.
- Information security policies.
- Results of tests, assessments, and audits.
- List of material outsourcing service providers.
- Board papers.

In practice, it is often in the planning and preparation phase of an onsite examination when such documents are collected.

Routine regulatory reporting of cybersecurity metrics and data points should be evaluated alongside financial reporting. Just as FIs report financial data on a routine basis (quarterly, semiannually, and annually), nonfinancial data—especially for technology risks and information security—should be regularly reported and included in routine supervisory information. The following are examples of such data points:

- Number of incidents and breaches.
- Key availability metrics of critical and important systems and services (for example, uptime, frequency, and duration of downtimes).
- Key metrics of ICT operations.

Besides regular reports, ad hoc cyber incident reporting is another key source of information. Many jurisdictions have passed relevant regulations and implemented the necessary infrastructure. Common good practice elements are identified as follows:[21]

- There is a secure communication channel and a technology platform for submitting and processing cyber incident reports.
- Monitoring of incoming cyber incident reports is aligned with the operational schedule of the reporting platform (for example, if it is open 24/7, then monitoring is also 24/7).
- All reports are followed up until resolution.
- Trends are identified, and action is taken to prevent or mitigate the impact of further incidents of the same nature, both at the reporting FI and more widely in the financial system.
- Data analytics tools, machine learning, and AI are used to augment incident report analysis.
- There is a defined and tested escalation mechanism to involve senior leadership and other relevant agencies in case of severe incidents.

In addition, it is good practice to consolidate and leverage all information already available to the supervisor—such as previous reports and analyses, documents collected during previous supervisory cycles or onsite examinations—and limit information requests to changes and areas not covered. As a rule of thumb, if cyber risk information is collected, it should be used in the supervisory process; conversely, cyber risk information that the supervisor lacks the capacity to evaluate—or has no capacity to have it evaluated—should not be collected. Examples include in-depth technical security audit reports (request an executive summary and action plan instead) or granular security logs. This applies equally to onsite examinations.

Analysis

A good approach for effective offsite analysis is to distinguish two components: (1) a comprehensive annual assessment of all material risks, of which cybersecurity and operational resilience are included (often referred to as the Pillar 2 assessment); and (2) ongoing assessment of routine supervisory reporting and other information throughout the supervisory cycle. The combination of these two approaches has been shown to help supervisors identify emerging risks earlier.

Risk analyses cover idiosyncratic risk of specific institutions and systemic risk to the financial system. Key cyber risk indicators can be used for trend analysis and forecasting. Risk level thresholds can be set to trigger warnings when crossed.

Cyber mapping has been a topic of particular interest for supervisors in recent years. A cyber map of the financial system identifies the main technologies, services, and connections between FIs, service providers, and in-house or third-party systems. At a conceptual level, mapping aims to highlight key financial and technological connections between FIs (including FMIs) and between these firms and TSPs. The dynamism and complexity of the financial sector, along with the range of technologies that it uses, can make cyber mapping

[21] Key regulatory requirements regarding cyber-incident reporting are listed in chapter 5. Because of the complexity of the issue, detailed technical requirements are sometimes issued in a separate standard that references the regulation.

a challenging task. Creating detailed maps can be expensive and time-consuming. However, mapping exercises that do not aspire to completeness but rather apply selected criteria and thresholds for inclusion have proven to be a useful tool.[22]

When assessing cybersecurity, supervisors should look at the operational-risk-management and cybersecurity frameworks holistically. This allows the supervisor to recognize strengths and weaknesses enterprise wide. For example, if an FI has weak operational risk management, this may also be reflected in the cyber area. Equally, if they are weak across the board, why would this be different in the cyber area?

Reporting

The results of offsite cyber risk supervision are included in several outputs. Besides regular risk assessments of specific FIs, horizontal analysis reports tackling a specific cyber risk issue across the sector can be created. Stripped of confidential information, such reports can be published and contribute to the supervisor's thought leadership status.

Internally, risks and other relevant data can be visualized on risk dashboards. To this end, data analytics and visualization tools are of great importance.

Collection and storage of offsite reporting should be collated to represent the "permanent file" used as input to the risk rating, which in turn informs the supervisory action plan.

Notifications and permissions

Notifications and permissions form a mechanism to inform supervisors of potential significant changes to an FI's technology stack, supply-chain arrangements, and other material changes. Most supervisors require institutions to notify or seek permission for material changes in operations, such as outsourcing or offshoring. These requirements are predicated on the notion that material changes in processes, systems, or suppliers may alter the inherent risk profile of the entity. Therefore, notifications typically require the supervisor to review, approve, or provide a non-objection. These requirements enable the supervisor to be regularly informed of major developments in the FI's processes and systems and to evaluate those changes as part of ongoing supervision.

Other activities

Offsite supervision also may cater to other requirements, such as pre-licensing activities, mergers and acquisitions, and resolution of FIs. It is good practice to develop checklists and processes to handle such important yet irregular work areas. The checklists and processes should recognize different types of financial sector entities, business and IT strategies of FIs, and the range of digital products and processes being considered.

D. Onsite Supervision

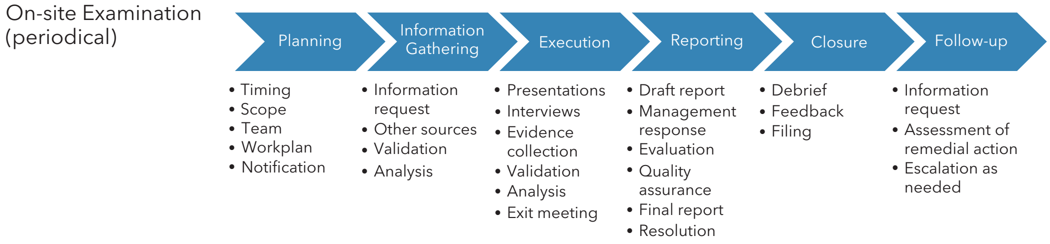
Overview

Onsite supervision is a valuable source of information regarding the actual workings and operations of FIs and provides stronger assurance on the quality of cyber risk management than offsite work. It is an opportunity to deepen the supervisor's understanding of the institution's technology stack, technology services leadership model, governance approach, and cyber-risk-management framework.

Onsite cyber risk examination assignments align with the general rules and regulations of the supervisor, similar to other onsite examinations (Figure 8).

[22] For an example implemented with support from the IMF, see Poljsak (2024).

Figure 8. Onsite Examination Phases



Source: IMF.

Arguably, onsite work is more important in cyber risk supervision than in most financial risk areas. This is because a much larger part of the risk is tied to tangible infrastructure, such as DCs and ICT equipment, the security of which is best assessed during actual visits. Several aspects of the ICT and cybersecurity control environment are also best assessed with onsite procedures, for example, to ensure sample integrity and unfettered access to key ICT personnel.

Good Practices

Planning

Front-loading the effort in onsite examinations pays dividends later because work is time constrained based on a pre-agreed agenda that is difficult to change. Therefore, thorough planning is essential, notably ensuring sufficient resources and focus on pre-examination preparation, especially the comprehensive review of all relevant material available on the target FI. Additional time should also be allocated during the schedule for sample testing to validate the effective implementation of processes, controls, and overall cyber risk management.

The planning of onsite examinations should follow a regular cycle (typically on an annual basis) to facilitate optimal allocation of resources and cover as many FIs as possible with available qualified cyber risk supervisors. Annual planning should be performed before the beginning of the business year, and onsite missions should be distributed throughout the year to align with other supervisory examinations of the same FI. This alignment aims to capitalize on synergies while avoiding overburdening the FIs with multiple examinations of different scopes scattered throughout the year. Exceptions occur, such as unplanned visits because of major incidents or unforeseen issues. It is good practice—although difficult because of work pressures—to reserve a small capacity buffer in the annual plan for such eventualities.

On planning individual examinations, observed good practices include the following:

- Preparing a project plan for the entirety of the onsite examination, that is, one that covers all phases, not just the actual onsite work.
- Preparing an interview plan for the onsite work, detailing all topics to be covered, their respective timeframes, participating supervisors, required bank staff, and any logistical requirements.
- Although the plan is tight, reserving time for internal deliberations of the onsite team and to follow up on open items.
- Preparing a pre-examination information request based on a review of all relevant information available and planned areas of examination so that information already known to the supervisor is not asked for again.

- Transmission of the draft interview plan and information request with the notice to the bank or shortly thereafter to allow sufficient time for the FI to ensure the required participation and prepare the initial return.
- Allocating time within the plan for (1) the review of the initial return and for the FI to make amendments if necessary, (2) an initial risk assessment, and (3) any other preparatory work.
- Fully assigning the team to onsite work, that is, during this time, they are not working on other projects.

The independence and objectivity of the onsite examination team should be ensured: its members must not have direct stakeholder affiliations or be shareholders of the FIs being examined.

The onsite examination team should consist of at least two experts, even for small entities, in order to ensure objectivity and peer support. Generally, the team should include experts with diverse backgrounds and competencies, including ICT GRC (governance, risk, and compliance) experts, to cover all aspects of people-, process-, and technology-related topics tackled during the onsite examination.

Assigning junior supervisors to the onsite examination team facilitates hands-on training and internal knowledge transfer.

The examination team should have counsel assigned from the legal department in case disputes arise with the FI and review legally binding documents before issuance. Although the counsel does not need to accompany the examination team onsite, their availability during the onsite visit is important.

Information gathering and analysis

The most important sources of information for the onsite examination are the relevant documentation collected and maintained during offsite supervision, the return to the pre-examination information request, outputs of offsite analysis, and incident reporting. For more details on what can be included in the offsite information gathering, refer to the section titled Offsite Supervision.

The return should be reviewed and validated, considering (1) reasonableness, given the nature, size, and complexity of the FI; (2) completeness and consistency; (3) compliance with regulatory requirements on governance; and (4) past update and approval dates of strategies, policies, and procedures. Gaps and discrepancies need to be followed up with the FI before starting the onsite work.

Understanding the business model and key features, as outlined in its strategic plan, will help inform and contextualize the analysis of pre-visit information.

A clear understanding of the key features of the technology stack is necessary, including the use of outsourcing and third-party service providers. Examples include the following:

- The enterprise ICT architecture to understand data flows and processing that underpin critical and important services.
- The main technological platforms in use to form an idea of potential weaknesses.
- The age of technology assets such as operating systems and core banking platforms to identify potential obsolescence and end-of-life issues.
- Physical location of the technology infrastructure and whether these are on-premises, located in an external facility managed by a service provider, and similar details for secondary sites.
- Main service providers to the FI, the type of service contracted, and the terms and management arrangements.

Ultimately, the analysis should lead to a preliminary risk assessment that informs the focus areas of the examination. Indicators of potentially higher-risk areas include the following:

- Areas lacking proper documentation.
- Unaddressed internal or external audit findings.
- High risks noted in internal risk assessments without documented and credible mitigation.
- Key cyber-risk-management documentation, strategies, policies, or procedures not updated for too long.
- Obsolescence in the technology stack (for example, use of superseded software versions).
- Major changes in the ICT architecture.
- Budget and time overruns in ICT projects.
- High turnover or prolonged vacancies for key ICT and cybersecurity managerial positions.
- Severity or frequency of reported cyber incidents, especially outages of key systems, above the peer benchmark.
- ICT and cybersecurity staffing or budgets below the peer benchmark.
- Negative media coverage of matters related to the ICT performance and cybersecurity of the FI.

Execution of the onsite examination

Onsite cyber risk examinations are distinct from audits, even though there are several features in common, such as evidence gathering, control testing, and documenting findings and recommendations. Generally, examinations focus more on cyber risk governance and risk management and are less granular. However, it is good practice to adopt the auditors' approach in requiring stronger evidence (for example, firsthand observation of cybersecurity practices and control testing, as opposed to relying on presentations and policy documents provided by the FI). Professional skepticism ("trust but verify") is a key success factor in onsite examinations.

Testing the effectiveness of risk management, for example, through sample testing, needs to be prioritized. The onsite team should take the opportunity to test the application of policies and procedures and evaluate the effectiveness of risk management. Specific issues based on the preliminary risk assessment should be included to validate that policies are effectively implemented.

Ideally, with the preparatory work already done, the first period of the examination can focus on the actual working of frameworks and governance structures and deepening the understanding of the IT architecture and security processes, which can subsequently be followed up with probing and sample-based testing of control effectiveness and finishing with follow-up meetings with the risk owners and second and third lines of defense.

Scheduling a meeting with the board as part of the onsite examination has proved to be a useful mechanism to highlight the role of the board in oversight of cybersecurity, as well as to test board members' awareness of cybersecurity and to communicate supervisory priorities in this area.

All three lines of defense should be included in meetings. The first line is to discuss technology, applications, strategy, investment, timelines, objectives, and priorities. The second line is to discuss risk management, compliance testing, and the institutional risk profile. The third line is to test the scope of the issues covered, identified issues, and how these were/have been addressed. It is important for onsite examiners to meet with the second and third lines of defense independently of the first. Supervisors should also dedicate attention to sample testing during the onsite phase to validate and verify processes, the effectiveness of the control environment, and the application of the three lines of defense.

Examination team members contribute effectively to the discussions by asking probing questions and demonstrating a command of the areas associated with risk management and corporate governance.

Experience shows that undertaking an exit meeting to communicate preliminary observations as soon as possible after the conclusion of the onsite work is of material benefit to FIs and enhances the effectiveness of the overall onsite examination process.

Reporting

As noted earlier, adopting an approach of presenting preliminary findings and communicating the main issues at the conclusion of the onsite examination to key executives—importantly the Chief Information Officer (CIO), CISO, and the senior management team—enhances the effectiveness of the process.

Supervisors should have a standardized approach to managing the report finalization process and apply this approach across all onsite examinations. Findings should be ranked, and deadlines should be set for resolution. It is good practice to implement an approach for segmenting the priorities of identified issues. For example, distinctions can be made between the following:

- **Requirements**—pertains to observations where the FI is not fulfilling its obligations under the regulations. Examples may include not adhering to a specific provision.
- **Recommendations**—typically aligns with observations whereby there is partial compliance, and improvements are clearly in scope regarding processes, risk management, and corporate governance.
- **Suggestions**—observations by the supervisor to strengthen risk management, where the FI is materially in compliance.

Requirements, recommendations, and suggestions should consider the feedback from the FI on feasibility and possible completion timelines without compromising the FI's improvement of its cybersecurity stance. To this end, it is good practice to focus on the desired outcome and let the FI decide the best way to achieve it.

Closure and follow-up

It is essential to diligently follow up on the resolution of findings. First, the FI should be required to submit an appropriately approved action plan that sets out the steps to be taken to rectify matters, including deadlines and the responsible stakeholders. Then, the execution of the plan should be regularly verified, for example, by requiring progress reports, conducting short visits, or having the FI commission independent audits. In some countries, the regulations require FIs to conduct independent assessments (see Box 1 for an example).

In cases where FIs' internal audit is sufficiently independent and capable, follow-up on lower-risk issues can be delegated to them. For example, a management representation letter confirming the remediation, countersigned by the head of internal audit, could be required from the FI, accompanied by an internal audit report. However, supervisors remain accountable for having the FI rectify matters, and therefore, some risk-based validation is advisable in such cases as well. This can be done as part of the next onsite examination.

Remediations past due should be tracked and addressed with priority at the next examination, especially when these have been delayed for too long. High-risk past due items require timely and assertive action from the supervisor, for example, summoning senior management or conducting supervisory visits to convey the importance of the matter, ending with legal enforcement action, if needed.

Lessons learned from onsite examinations should be disseminated broadly among cyber risk supervisors through debriefing sessions. Strengths and weaknesses can be discussed, aiming to continuously improve cyber risk supervision. General conclusions can be shared across the supervisory function in internal training curricula to attune non-specialist supervisors to cyber risk.

Box 1. Australian Prudential Regulation Authority's Supervisory Approach—CPS 234 Independent Assessment

The Australian Prudential Regulation Authority (APRA) maintains a principles-based prudential framework and a risk-based approach to supervision, including technology and cyber supervision. Prior to July 1, 2019, this approach was supported by the 2013 *Prudential Practice Guide CPG 234 Information Security*, which offered guidance while providing regulated entities with flexibility in implementation. Despite ongoing industry engagement, supervisory activities, and educational initiatives, APRA increasingly recognized the need to intensify its supervision with a whole-of-industry intervention to embed nonnegotiable cyber controls across all regulated industries as cyber threats grew in sophistication and frequency.

On July 1, 2019, APRA released a legally enforceable information security standard, *CPS 234 Information Security*, which places obligations on all regulated entities to maintain capabilities and controls to address cyber threats. Other key tenets include an obligation on boards to maintain information security, comprehensive security testing, and response plans. The intent of the standard was to ensure that regulated entities have prevention, detection, and response capabilities to withstand cybersecurity threats.

To "shift the dial" on cyber by ensuring that new information security obligations are embedded, APRA initiated the CPS 234 Independent Assessments (referred to as the CPS 234 "Tripartite" review) as part of its 2020–24 cyber strategy. The assessments required APRA-regulated entities to appoint an independent auditor to assess their compliance with the prudential standard. The assessment results and remediation efforts, conducted over multiple years, drove significant improvements in uplifting cyber practices, including bolstering the board's confidence to direct management to address cyber exposures.

A summary of key findings is presented as follows:

- Incomplete identification and classification of critical and sensitive information assets
- Limited assessment of third-party information security capability
- Inadequate definition and execution of control testing programs
- Incident response plans not regularly reviewed or tested
- Limited internal audit review of information security controls
- Inconsistent reporting of material incidents and control weaknesses to APRA

Since the conclusion of the Tripartite review, APRA continues to reinforce the need for entities to enhance their prevention, detection, and response capabilities; test their preparedness; and work collaboratively with peers, researchers, and government to improve their level of cyber resilience.

E. Thematic Reviews

Overview

Cyber risk supervision needs to adapt to emerging developments, and occasional full-scope examinations based on FIs' risk profiles do not tend to be sufficient. There are situations where supervisors may have common concerns—either across multiple FIs, regarding a particular type of cyber incident targeting specific modes of payment (for example, ATMs or instant payments), or regarding the desirability of better understanding practices of some FIs (for example, business continuity, third-party risk management, or testing). In such situations, thematic reviews, also known as horizontal reviews, can be a particularly incisive supervisory tool.

Thematic reviews may explore either a single ICT/cyber risk-related topic or one of the domains of regulation to get a deeper understanding of the topic to help identify best practices and gaps in risk management. Such reviews do not result in an examination report for individual FIs but in a thematic sectoral report that clearly discusses the exercise's objectives, the methodology adopted, the range of practices observed in managing the risks covered, observed gaps in risk-management practices, and recommendations for the supervision department. Often, the lessons learned from the exercise are shared in supervisory communications, either with all FIs or with specific FIs, with a view to improving their risk management.

Good Practices

- Some of the topics for thematic reviews could be determined early and included in the supervisory agenda set by the board. Supervisory outcomes of the previous or current year may indicate certain weaknesses that are present across several FIs in dealing with specific domains of regulation or in certain focus areas. Supervisors themselves may have specific areas for improvement as outlined in their plans. After considering a range of areas for thematic review, prioritization across topics should narrow the choice to two or three topics that could be taken up consistently with resource availability at the supervisory authority and FIs, the working day calendar in the country, and other relevant factors. Such topics may be included in the supervisory agenda, including a tentative period for conducting the exercises.

- At times, sudden developments like a major cyber incident or a severe service interruption may also necessitate a thematic review, for example, with a view to identifying and communicating lessons learned. Cyber incidents targeting ATM networks in multiple FIs in a short period may warrant a better understanding of the root causes. Similarly, cyberattacks targeting SWIFT messaging-based payments across multiple FIs within a short window may require supervisors to gain a better understanding of the issues. In some cases, a major internal ICT incident at an FI that exhibits weaknesses in risk management may prompt the supervisor to review the practices at other/similar banks regarding the same issue. Such thematic reviews cannot be planned. It is, therefore, necessary to leave some slack in the resource envelope and working day calendars to conduct one or two need-based thematic reviews in the annual supervisory program.

- Thematic reviews produce better results when their objectives and methodologies are thought through in advance. They are deep-dive exercises in a focus area, requiring appropriate skill sets for successful execution. Identifying a team of specialists that can visit the covered FIs within a short period will facilitate a consistent approach and better results because they will be able to compare practices. If sending the same team is infeasible, selected teams conducting such reviews across the FIs under scope need to be thoroughly briefed about the objectives and methodologies to achieve good results.

- Thematic reviews can be conducted onsite, offsite, or in hybrid format, depending on the topic. For instance, DC preparedness of banks is better assessed using onsite examinations. Assessment of cybersecurity policies or organizational structures managing ICT/cyber risk can be done offsite by gathering relevant information. A tabletop supervisory review of the business continuity and disaster recovery arrangements could be done offsite. In other areas where policies, processes, and practices are to be examined, a hybrid approach may be useful. For instance, cyber resilience stress testing carried out by the European Central Bank (ECB) in 2024 had both onsite and offsite components.

- Thematic reviews are a very useful tool in the hands of ICT/cyber risk supervisors. Such reviews contribute to a better understanding of individual FIs while also offering benefits from a cross-sectoral perspective. As the objectives of such reviews are targeted, the outcome is often very useful and thus result-oriented by design. They are also less resource-intensive on the output front—there is no need to prepare FI-wise reports, and the discussions are held with preselected FI officials who are well versed in the subject. Thematic review reports also receive better attention from senior management because of their cross-sectoral views and policy input. Such reviews often result in either amendments to the supervisory expectations or supervisory actions.

- An illustrative list of focus areas for conducting thematic reviews is given hereunder:

  - Governance structure in managing ICT/cyber risk.
  - Range of practices followed by FIs, incorporating the three lines of defense model.
  - Review of internal audit effectiveness.
  - Practices in identifying critical business services and setting tolerances for disruption/risk appetite.
  - Board reporting practices.
  - Practices relating to maintaining asset inventory registers and third-party vendor registers, and cyber mapping.
  - Management of incident reporting, escalation, resolution, follow-up, and lessons learned.
  - Response and recovery capabilities.
  - IAM practices and data-leak prevention practices.
  - Building awareness and capacity among stakeholders.
  - Data center management.
  - Security Operations Center management.
  - Business continuity and disaster recovery arrangements.
  - Testing practices and remediation of vulnerabilities.
  - Source and accuracy of offsite information.
  - Compliance management practices relating to ICT/cyber.

F. Monitoring of Cybersecurity Testing

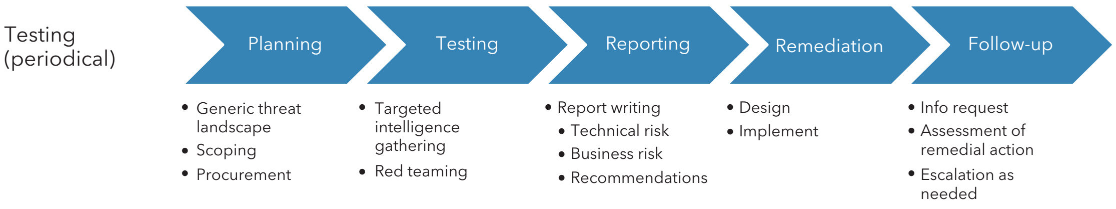
Overview

Cybersecurity testing significantly contributes to a realistic understanding of security vulnerabilities, cybersecurity defenses, and response and recovery preparedness. Also called penetration testing or red teaming, the frequency and scope of such testing are determined by the criticality of the FI/FMI and their ICT systems.

Major jurisdictions have established requirements and frameworks for penetration testing to enhance the cyber resilience of their financial sectors.[23] As noted earlier in the paper, authorities should consider implementing cybersecurity testing proportionally—that is, simpler requirements for smaller FIs and advanced testing for systemically important FIs and FMIs.

An advanced form of penetration testing is the so-called threat-led penetration testing (TLPT). A TLPT is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors based on targeted threat intelligence and focuses on an entity's people, processes, and technology, with minimal foreknowledge and impact on operations (Figure 9).

Figure 9. TLPT Phases



Source: IMF staff.

Note: TLPT = threat-led penetration testing.

The exercise typically involves three teams—the *White Team* (facilitators), the *Red Team* (threat actors), and the *Blue Team* (system defenders). During the exercise, the White Team enforces the rules, observes the exercise, addresses any issues that may arise, receives all requests for information or questions, and ensures that the test is executed in the intended manner. The Blue Team is responsible for defending an entity's use of information systems by maintaining its security posture against a group of simulated threat actors (that is, the Red Team). The Red Team is authorized and organized to emulate potential actions of a threat actor or exploitation capabilities to test an entity's security posture.

Supervisory authorities are increasingly assuming an active monitoring role in cybersecurity testing, most often the TLPT variety. Some authorities perform penetration testing themselves, which can be a risky endeavor, given the concentration of highly sensitive information readily usable to breach FIs that inevitably builds up over time. Such testing is best left to specialist providers unless the risk appetite is backed by validated confidence in a highly capable, stable, and vetted technical expert pool, along with tight operational security at the agency.

Good Practices

Supervisors in the TLPT do not directly engage in testing; instead, they oversee the entire testing engagement. They set the framework and expectations and assess the results.

Planning

Typically, TLPTs are conducted on critical live systems. Therefore, strong risk management is imperative to reduce the risk of any adverse impact of testing on entity data, damage to entity assets, and disruption to critical services and operations at the entity or in the financial sector. TLPT requires qualified third-party service providers to perform the Red Team roles to ensure an independent and professional view. The FI's White Team plans every aspect of the exercise, whose scope should be based on an assessment of the entity's critical functions and services, which in turn inform decisions on the test's duration and inclusions and exclusions.

[23] Examples include the United States, the United Kingdom, and the European Union.

If not predefined in regulatory expectations, an agreement must be reached on the classification of vulnerabilities discovered during testing, as well as on indicators that demonstrate the breach of the FI's cybersecurity.[24]

FIs are generally responsible for procuring threat intelligence and penetration testing services. Authorities may mandate the use of approved external threat intelligence and penetration testing providers, based on a validation of their expertise by accreditation and certification providers. To maintain a consistently high-quality testing regimen, requirements for service providers may be set regarding professional credentials, references, and experience.

Key challenges encountered in practice include insufficient testing capacity and inconsistent performance of testers, even with the aforementioned requirements in place. Therefore, emphasis should be placed on procurement (for example, thorough due diligence) and quality control procedures, which should be explicitly addressed in the plan.

Testing

Developing threat intelligence for the FI is an important task that precedes the actual test within the TLPT exercise. Threat intelligence providers use reconnaissance techniques focused on the entity to create credible threat profiles. These profiles, which accurately reflect real-life cyber threat actors, are critical in defining the scope of testing activities. The threat profiles contain cyber threat scenarios that help the Red Team develop test plans, used during the penetration testing phase. Based on such threat intelligence, the Red Team prepares detailed plans for the penetration testing.

Based on the scope, sufficient time must be allocated to the actual testing procedures to allow the Red Team to conduct a realistic test in which the cyber threat scenarios are executed. The Red Team is typically responsible for (1) producing a penetration test plan, aligned with the scope and risk-management processes, which clearly sets out the scenarios to be followed during the test; (2) conducting the test in accordance with the cyber threat scenarios generated from the output of the threat intelligence provider; and (3) drafting and issuing the final penetration test report to the entity. The White Team is responsible for (1) coordinating and facilitating test activities, (2) maintaining continuous dialogue with the Red Team and providing additional support where necessary, (3) overseeing and monitoring the Blue Team, and (4) applying effective risk-management controls (including halting the test at any point, if deemed necessary).

Relevant authorities may observe the test alongside the White Team.

Reporting

On conclusion of the test, the Red Team is expected to deliver a penetration test report. This report should include details of the approach taken for testing, as well as the findings and observations from the test. The report should address both technical and business audiences (the latter, at a summary level) and clearly spell out the vulnerabilities arising from the weaknesses discovered during the test and set out recommendations for corresponding corrective action. It is good practice to require the provider to focus on the business risk and avoid technical jargon and deeply technical details in the body of the report. These should be included in the annexes. This way, the report can be more useful beyond the cybersecurity function of the FI—for example, to senior management of the FI.

Supervisors should exercise restraint in collecting full technical details on how the FI's cybersecurity was compromised, because this is not very relevant to their objectives with the TLPT, which is to ensure that weaknesses are found and remediated. To this end, assuming that the testing framework was properly

[24] Such indicators are often linked to gaining privileged access to certain systems or data, which are referenced as "flags," hence the expression "capturing the flag," meaning that the Red Team has achieved its objective. The flags are initially set in the planning phase but can be modified later based on the threat intelligence and as the test evolves.

adhered to, a brief description of the weaknesses and a remediation plan are sufficient. Therefore, it is good practice for supervisors not to collect and store detailed technical information from penetration tests, because this can unnecessarily increase their attractiveness as targets for cyberattacks.[25] If the supervisor wishes to ascertain the level of detail and quality of the work based on the full report, then they can always consult it at the premises of the FI.

Remediation

The FI should be made responsible for undertaking the following steps in the remediation process: (1) distributing findings to appropriate stakeholders using agreed-upon secure delivery methods, (2) arranging post-test workshops with relevant stakeholders to discuss findings and identify potential mitigation solutions, and (3) formulating and executing a full remediation plan. The remediation plan should include milestones and timelines for corrective action. The remedial actions need to be carefully designed, considering the constraints posed by the ICT architecture and the capabilities of the FI.

Follow-up

Supervisors are responsible for engaging with the FI, agreeing on the remediation plan, and subsequently overseeing the execution of the remediation plan as part of their normal supervision. The first step in this regard is gathering the TLPT report (however, see the caveat above regarding excessive technical details) and its recommendations from the FI. Given their active monitoring of the test, supervisors should have sufficient background to understand the test report and its recommendations. They must also independently assess the remedial action plan, considering feasibility, appropriateness, and timelines. Prioritization of the remedial actions based on the criticality of functions also needs to be evaluated. Supervisors need to ensure that the FI takes the planned remedial action and, in the interim, puts appropriate compensatory controls in place.

[25] Even large and supposedly well-secured supervisory authorities can be hacked. For a recent example, see https://www.bloomberg.com/news/articles/2025-04-10/us-bank-regulator-didn-t-have-safeguard-on-hacked-email-account. This can happen to penetration-test providers as well, but (1) their main business is cybersecurity, so it is less likely, and (2) they typically are not a monopoly, so there is less concentration of highly sensitive information about systemic FIs within a jurisdiction.

5. Cyber Simulation Exercises

A. Overview

To better understand the scope and nature of interdependencies within the financial system and between FIs and relevant third parties, as well as the ability of FIs to respond to and recover from incidents, it is important that both public and private financial sector entities develop and implement their cyber incident response and recovery plans. This is mostly done through cyber simulation exercises, often referred to as "cyber war games" or "cyber tabletop exercises." These exercises simulate real-world cyberattack scenarios, allowing participants to practice their response strategies and identify potential vulnerabilities in a controlled environment.

Jurisdictions around the world are increasing their focus on cyber simulation exercises, which can be conducted by regulatory and supervisory authorities and by market participants. Based on IMF TA and FSAP assessments, several key benefits of these exercises have become apparent (Table 3).

Table 3. Key Benefits of Cyber Crisis Exercises

Benefit	Examples
Improved incident response	▪ **Faster decision making:** Participants get to practice decision making under pressure, honing their ability to make quick and effective responses in a real attack. ▪ **Coordination among teams:** Exercises help test and improve coordination between different teams, such as IT, security, communications, and legal teams, ensuring a more unified response during an actual attack.
Identifying gaps in security	▪ **Uncover vulnerabilities:** Simulations can expose weaknesses in security infrastructure, policies, and procedures that might not be immediately apparent. ▪ **Test backup systems:** They can also help identify whether backup systems, incident response plans, and recovery procedures work as intended.
Enhanced preparedness	▪ **Training for employees:** Simulations provide employees with a chance to practice their roles during an incident, especially those in non-technical roles who may not regularly engage with security issues. ▪ **Scenario customization:** Organizations can create custom scenarios that accurately reflect their specific risks, ensuring training is directly relevant to their environment.
Better risk management	▪ **Evaluate potential impact:** Simulations allow teams to assess the potential impact of different attack vectors (for example, phishing, ransomware, insider threats), helping prioritize defensive measures. ▪ **Cost-effective risk assessment:** They offer an opportunity to test various risk-management strategies without the financial and operational consequences of a real cyberattack.
Strengthening communication and collaboration	▪ **Internal communication skills:** Cyber simulations help refine internal communication strategies, ensuring that everyone, from the IT department to C-suite executives, understands their roles and can relay information efficiently. ▪ **Cross-departmental collaboration:** Effective cyber defense often requires input from various parts of an organization, IT, Human Resources, legal, and others. These exercises promote cross-department collaboration and foster stronger inter-team relationships.

(continued)

Benefit	Examples
Reinforce cyber hygiene and awareness	▪ **Education on best practices:** Participants gain firsthand experience of the importance of cybersecurity hygiene, such as secure password management, phishing prevention, and software updates. ▪ **Awareness of threats:** Simulations raise awareness of emerging threats and common tactics used by cybercriminals, such as social engineering attacks, which often bypass technical defenses.
Meeting regulatory requirements	▪ **Testing compliance procedures:** Simulations can assess how well an organization is adhering to regulations, such as data breach notification laws.
Continuous improvement	▪ **Actionable insights:** After a simulation, a debriefing session allows organizations to analyze the effectiveness of their responses and pinpoint areas for improvement. By conducting regular simulations, organizations can track their progress over time and refine their incident response strategies.
Boosted confidence	▪ **Organizational confidence:** Regular participation in cyber simulations can increase confidence that the organization can handle cyber threats effectively and minimize damage. ▪ **Stakeholder assurance:** It demonstrates to stakeholders (customers, clients, and investors) that the organization is prepared and resilient against cyber threats.
Adapting to new threats	▪ **Simulation of novel attacks:** As cyber threats evolve, organizations can tailor simulations to replicate new attack methods, such as APT or state-sponsored hacking attempts. ▪ **Proactive defense strategies:** Simulations allow organizations to stay ahead of the curve by continuously testing their defenses against the latest TTPs used by cyber adversaries.

Source: IMF Staff
Note: APT = advanced persistent threats; IT = information technology; TTPs = tactics, techniques, and procedures.

In summary, cyber simulation exercises are a powerful tool for strengthening cybersecurity. They improve response capabilities, identify vulnerabilities, and enhance communication and preparedness, ultimately leading to a more resilient organization in the face of ever-evolving cyber threats.

B. Good Practices

There is a broad range of different cyber simulation exercises, and the IMF has observed jurisdictions around the world applying some or all of the following:

- Phishing exercises to test the awareness and training of an organization's employees.
- Tabletop exercises or drills/walk-throughs of cyber incident response and recovery plans or playbooks involving incident responders and incident management teams to build muscle memory.
- Live tests or simulations such as basic and threat-led penetration tests, bug bounties, cyber ranges, and adversarial attacks (DDoS, ransomware) to enhance actual technical response and recovery capabilities.
- Executive-level crisis management exercises to stress decision making under simulated conditions, senior management involvement, and communication proficiency. This could include developing challenging scenarios, such as dealing with no-win situations, uncertainty, and imperfect information, or requiring the prioritization of the timing of recovery of competing systems and business lines.

- Sector-wide exercises to allow financial sector participants to practice cyber incident response, recovery coordination, and communication in the event of a large-scale cyber incident.

Although exercises can be driven by regulatory and supervisory authorities or by market participants, good practice is for authorities to drive exercises in their financial sectors, reflecting their convening power and broader financial stability mandate. Authorities should, therefore, consider developing an exercise program that follows a cyclical approach, including exercises, evaluation, improvements, and repetition.

Simulation exercises can build on earlier ones in a phased approach: (1) enabling the organization to progressively enhance its cyber preparedness by tackling increasingly complex risk scenarios; (2) developing key risk indicators and metrics on improvements to the incident management process and procedures; (3) ensuring a common understanding of priorities, threats, and risks; and (4) validating or benchmarking incident recovery capabilities.

Effective cyber simulation exercise program management typically includes (1) stakeholder engagement, (2) multiyear preparedness priorities, and (3) improvement planning.

Stakeholder Engagement

Stakeholder engagement is a crucial first step in establishing and maintaining a successful exercise program because it secures the support of key individuals within the organization. Stakeholders play a vital role in guiding the program, setting priorities, and ensuring long-term sustainability. There are two primary types of stakeholders in a simulation exercise: (1) program-level stakeholders, who oversee and influence the entire program, ensuring alignment with organizational objectives; and (2) simulation-exercise-specific stakeholders, who are involved in individual exercises within the program.

Identifying stakeholders early enhances the effectiveness of the program by ensuring that simulation exercises are prioritized appropriately. A key strategy in this process is conducting an ecosystem scan, which helps planners assess interconnections among companies and identify interdependencies, such as with third-party service providers. By understanding these relationships, planners can include the most relevant stakeholders.

For effective coordination, FIs can establish a joint committee to oversee and deliver the simulation exercise program. This collaborative approach enhances communication, ensures consistency, and strengthens stakeholder involvement. In addition, a lead stakeholder holding a senior position should be appointed to “own” the program, with responsibility for securing resources, driving organizational commitment, and maintaining momentum for a multiyear simulation exercise program. This lead stakeholder would also play a key role in determining the risks that the program should address.

In summary, strong stakeholder engagement, clear roles, effective coordination, and stability are good practices that contribute significantly to a successful and sustainable simulation exercise program.

Multiyear Preparedness Priorities

A well-structured multiyear simulation exercise program ensures that insights gained from past exercises are carried forward and integrated into evolving priorities. Observed good practices include the following:

- Incorporating Lessons Learned
  - A structured program helps transition lessons from one system or exercise to another.
  - It enables authorities to update priorities based on past experiences.

- Risk-Based Planning Approach
  - Programs should be based on risk assessments and approved multiyear priorities set by authorities, stakeholders, and senior leadership.
  - Priorities must be clear, concise, measurable, realistic, and directly linked to risk assessments.
- Risk Assessments and Organizational Threats
  - Risk assessments evaluate vulnerabilities, threats, and mitigation strategies affecting the financial sector.
  - Risks may stem from external dependencies connected to the financial sector through logical or physical dependencies.
  - In interconnected sectors like finance, an ecosystem scan can help identify risks arising from external dependencies.
- Cybersecurity Considerations
  - Cyber threats evolve rapidly, requiring frequent reassessment of multiyear priorities.
  - However, authorities should be cautious when making updates to avoid disrupting the ability to track long-term improvements in incident response.
- Budget and Resource Constraints
  - When setting long-term preparedness priorities, financial and resource limitations must be taken into account.

In summary, multiyear simulation exercise planning is a strategic approach that enhances sector resilience by continuously refining risk management and preparedness efforts. By integrating lessons learned, adapting to emerging threats, and aligning with risk-based priorities, authorities can improve the incident response capabilities of the financial system as a whole.

Improvement Planning

The primary goal of conducting a simulation exercise is to identify areas for improvement in responding to and recovering from cyber incidents. An after-action report plays a crucial role in this process by documenting the simulation exercise assessment results and issuing specific recommendations for improvement. Once areas needing enhancement are identified, it is good practice to link these to measurable corrective actions, with designated responsible parties and target implementation dates.

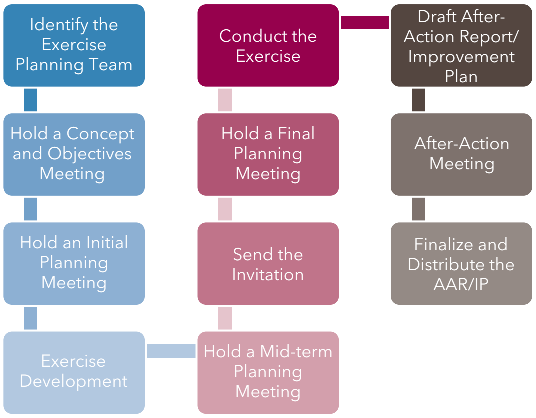
Process for Conducting an Individual Exercise

When planning and executing an individual cyber simulation exercise, it is good practice to follow a structured approach focused on preparation (Figure 10).

The simulation exercise design phase defines the type of exercise, participants and their roles, objectives, alignment with a multiyear plan, and scenario details. Each exercise may have unique objectives and assessment criteria, which should be clear, measurable, achievable, and tied to risk assessments. Participant selection is crucial, involving a diverse range of experts, including technical, legal, communications, and law enforcement professionals.

Scenarios should be based on risk assessments and threat intelligence, with complexity tailored to the purpose of the simulation exercise. More complex exercises may require additional training and planning. Clear communication protocols are essential to avoid confusion between exercise activities and real events.

Figure 10. Cyber Crisis Exercises Step by Step


Identify the Exercise Planning Team
Hold a Concept and Objectives Meeting
Hold an Initial Planning Meeting
Exercise Development
Hold a Mid-term Planning Meeting
Send the Invitation
Hold a Final Planning Meeting
Conduct the Exercise
Draft After-Action Report/ Improvement Plan
After-Action Meeting
Finalize and Distribute the AAR/IP

Source: IMF.

Simulation Exercise Design and Development

Planners should anticipate deviations from the simulation exercise plan and use scenario injects to steer the exercise back if needed. Regular planning and educational sessions ensure all participants understand the exercise. Any identified gaps should not be prematurely addressed but rather presented to system owners for action, ensuring the exercise accurately reflects potential real-world challenges.

Simulation Exercise Conduct

The conduct of an exercise depends on its type, the number of participants, and their roles. It is crucial to secure logistics, such as location, technology, communication, and safety, for all exercises. Materials should be provided in advance, and briefings organized, especially when multiple jurisdictions are involved.

To avoid disruption, confusion, or panic, planners should take the following actions:

- Clearly label simulation exercise communications.
- Choose a date, time, location, and delivery method that minimize impacts on operations.
- Distribute materials outlining roles, responsibilities, and communication plans.
- Notify external parties about the exercise.
- Allow participants to exit if needed to respond to real events.

Assessment

The simulation exercise assessment aims to identify areas for improvement in policies, procedures, operations, and systems, while enhancing future exercise proficiency. It involves comparing results against objectives and analyzing recorded events to pinpoint weaknesses.

Effective assessment criteria measure how well the objectives are met, highlight gaps, and recognize successful strategies. Participants should not be incentivized to “pass” the exercise artificially, because genuine issues must be addressed for meaningful improvements to occur. A critical component of the assessment is the “hotwash” or “hot debrief,” a post-exercise discussion to gather immediate feedback, shaping the improvement planning process.

Assessors should evaluate the following:

- Whether participants correctly identified the issue.
- Whether their actions aligned with policies and procedures.
- The effectiveness of their responses.
- Their awareness of others' roles and actions.
- These factors form the foundation for creating an improvement plan that strengthens future exercises and overall preparedness.

In conclusion, authorities are increasingly focusing their attention on cyber simulation exercises because these are highly useful tools to raise awareness within the financial sector, improve the overall resilience of the financial system, and strengthen the crisis preparedness of the public and private sectors to a potential systemic cyber incident. The IMF has facilitated several exercises as part of its TA program and, in all cases, has noted significant areas for improvement in institutional governance arrangements, crisis communication protocols, incident reporting, information sharing, and response and recovery arrangements. Simulation exercises have reinforced the importance of these core areas and have often catalyzed further initiatives to drive improvements.

6. Monitoring and Mitigating System-wide Cyber Risk

Although adequate capital and liquidity are necessary buffers for financial resilience, operational resilience does not simply result from a strong balance sheet. Instead, it requires focused operational preparedness, demanding skilled resources, lifecycle management, and adequate budget to strengthen defenses. Achieving robust operational resilience requires alignment among people, processes, and technology. Each forms a strand supporting critical services. The synergy of trained personnel, clear and tested processes, and adaptive technology ensures readiness for both routine and extraordinary disruptions.

To illustrate the breadth of supervisory responsibilities, consider digital products across the financial sector, including mobile banking apps, e-wallets, real-time payments, automated lending, and digital asset management tools. Supervisors must fully understand what it takes to deliver these products. This includes essential software, hardware, and the interplay among fintech firms, third-party providers, people, processes, networks, and infrastructure such as power supplies. This holistic view enables supervisors to identify dependencies and vulnerabilities at every stage of the delivery process.

To clarify, supervisors should (1) identify and map the most critical third parties underpinning digital offerings. These parties include system integrators, core banking solution providers, and essential software or hardware vendors; (2) assess for concentrations that might create systemic risks, such as dependence on a single provider, data center clustering, or technology monopolies; and (3) document where these concentrations occur, whether in software platforms, hardware suppliers, service providers, or operational sites. This helps identify and manage single points of failure and guide focused risk mitigation strategies.

A. Key Pillars for Resilience and Stability

Effectively monitoring and mitigating systemic cyber risks in the financial sector demands a multilayered, proactive approach.

- At the foundation lies continuous surveillance of cybersecurity preparedness across all industry participants. This ensures the sector remains robust against emerging threats.
- A comprehensive cyber incident reporting framework is essential. It must capture granular data for timely detection, swift response, and informed policymaking.
- Mapping the web of interconnections and interdependencies is crucial—not just between institutions but also with third-party service providers. These external entities often form critical links in the operational chain. Including third-party dependencies in these mappings reveals potential propagation channels for cyber incidents. This highlights vulnerabilities requiring attention. Critical third-party service providers whose operations underpin essential financial functions must be rigorously identified, monitored, and supervised to prevent single points of failure.
- Financial stability analysis must include scenarios of severe yet plausible cyberattacks. These scenarios evaluate sector-wide impacts and guide contingency planning (Khiaonarong, Korpinen and Islam, 2025).
- Creating a cybersecurity strategy for the financial sector establishes a clear vision and policies for resilience. Stress tests using payment system data under simulated attack conditions reveal weaknesses and guide improvements.

- Leadership plays a pivotal role. Top management must set the agenda and promote a culture of cybersecurity awareness through impactful speeches and advocacy.
- International collaboration and cooperation are vital to ensuring cybersecurity of the sector—particularly regarding convergence in regulatory practices, well-articulated supervisory practices, threat intelligence and information sharing, supervisory colleges focusing on nonfinancial risks, emerging threat landscapes and modus operandi, emerging practices regarding mapping and quantification of cyber risk, and factoring cyber risk into financial stability analysis. Testing and exercises are another area where such collaboration might be useful.

It is therefore critical that all stakeholders commit to implementing these measures and collaborate to build a more resilient and trustworthy financial sector for the digital age.

Given the key role of financial sector supervisors in safeguarding financial stability, it is important that at the board level, the supervisory authorities (1) appreciate the potential systemic impact of cyber risk, (2) set clear expectations for cyber risk regulation and supervision, and (3) monitor progress against defined benchmarks. Cyber risk should be regarded as a cross-cutting issue, and all its dimensions—people, process, and technology—addressed. Each institution or infrastructure will remain prepared, and the sector overall resilient, only if these actions are consistently applied. Supervisors should clearly articulate their cybersecurity strategies, develop proactive policies, and foster an environment where best practices are not just adopted but continually improved throughout the financial ecosystem.

Ultimately, the effectiveness of these strategies depends on supervisory agencies' commitment to allocate sufficient human, technical, and financial resources to fulfill their mandates. Supervisory bodies must (1) invest in skilled personnel, (2) adopt advanced technology, and (3) secure sustained funding. Taking these specific actions now will ensure frameworks succeed and the sector achieves the resilience and stability needed in the face of digital transformation and complex systemic risks.

B. Financial Market Infrastructures—Systemic Players

Distinct from prudential and conduct supervision, central bank oversight is holistically concerned with the safety of the financial system (Box 2). In observed practice, central bank cyber risk oversight focuses on payment systems and other FMIs. Its activities are often a subset of those in cyber risk supervision, with a less intrusive approach. For example, it is rare for this function to perform onsite examinations, with the bulk of institution-specific work resembling offsite supervision. However, given the criticality of FMIs, some central banks have adopted oversight frameworks that follow the same approach and intensity toward cyber risk as advanced prudential supervisory authorities or explicitly state that FMIs are subject to both oversight and prudential supervision.

Box 2. Supervision versus Oversight: Key Differences

The concepts of supervision and oversight are distinct but complementary. Supervision focuses on the safety and soundness of individual FIs (prudential supervision) and how FIs protect the interests of customers, investors, and market participants (conduct supervision). Oversight, typically conducted by central banks, is about ensuring the safety and efficiency of a financial system with emphasis on the interconnections between participating institutions. Supervision and oversight are complementary because they both contribute to safeguarding financial stability.

The three key activities of oversight include monitoring, assessment, and inducing change.

Monitoring involves identifying and obtaining sources of information to improve the understanding of a system's design and operation. The sources of information could include system documentation, reporting on system activity, internal reports, self-assessments, bilateral contacts, multilateral meetings, onsite inspections, expert opinions, and customer feedback. Powers to obtain such information, perform onsite inspections, and induce change help ensure effective oversight.

Assessment occurs at two levels. At a general level, assessments take a more holistic view, analyzing contributions to monetary and financial stability objectives. At the system level, assessments determine whether the relevant policy requirements and standards are met. A balance is often struck between self-assessments by regulated entities (for example, a payment system) and external assessments (for example, by the central bank).

Inducing change arises when policy requirements or standards are not being met. The tools to induce change vary significantly, including (1) moral suasion, (2) public statements, (3) voluntary agreements and contracts, (4) participation of the central bank in systems (as part-owner or official observer), (5) cooperation with other authorities, (6) statutory power to require change, and (7) enforcement and actions.

Source: CPSS 2005.

The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks—such as liquidity dislocations and credit losses—or major channels through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, a key element of an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy. The systemic importance of FMIs accentuates the need for their robust oversight.

In analyzing cyber risk associated with systemically important FMIs, the IMF applies the CPMI-IOSCO Guidance on Cyber Resilience of FMIs (Cyber Guidance) among other international standards. The Cyber Guidance is informed by five key principles of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), including Principle 2 (Governance), Principle 3 (Framework for the comprehensive management of risks), Principle 8 (Settlement finality), Principle 17 (Operational risk), and Principle 20 (FMI links). The analysis of operational risk also considers the application of Annex F (Oversight expectations applicable to critical service providers), which includes expectations on information security. To further examine cyber risk supervisory and oversight practices, the five major areas of responsibility of central banks, market regulators, and other relevant authorities for FMIs are referenced.

Using information specific to FMIs obtained from IMF FSAP and TA work, including in-field assessments, key findings, and recommendations against the components of the Cyber Guidance (Table 4) and associated with authorities' responsibilities under the PFMI, where relevant (Table 5), are presented in the following section. These highlight the need for continuous improvements in strengthening the cyber resilience of FMIs and the broader FMI ecosystem.

Table 4. Recommendations to Strengthen FMI Cyber Resilience

Component of Cyber Guidance	Issue of Concern or Identified Gap	Recommendation, Action, and Comments
Governance	▪ Cyber strategy	▪ FMI oversight authorities should keep developing their cyber strategies, both in their own mandates as well as in joint functions, for the financial sector and FMIs, with a clear vision and objectives, clear articulation of roles and responsibilities in operationalizing the strategy, initiatives and tools required to operationalize the strategy, road map for implementation and timelines, and estimates of resources and investment required to achieve the strategy.
	▪ Independence	▪ The oversight division should be given enough independence and resources to conduct effective oversight of the FMI.
	▪ Board of directors	▪ Ensure that the board of directors has a member with appropriate skills and knowledge to understand and manage cyber risks. Ensure regular training of the Board on cyber resilience matters.
Identification	▪ Concentration risk	▪ The FMI should maintain a specific database of third-party service providers of systemically important financial entities and FMIs, and conduct analysis to identify critical third-party service providers and determine whether there is concentration risk in the financial system.
Protection	▪ Attack surface documentation	▪ Document a comprehensive attack surface for the FMI and critical systems, covering business operations, IT systems, infrastructure, people, and interconnections.
Detection	▪ SOC operational hours	▪ Enhance 24/7 Security Operations Center operations to cover all perimeters, internal systems, and applications after business hours.
Response and recovery	▪ Cyberattack scenarios in FMI business continuity plan	▪ Continue upgrading FMI business continuity plan with a range of cyber-specific extreme-but-plausible scenarios that are regularly tested.
Testing	▪ Testing with participants and FMI links	▪ Consider conducting cyber exercises or simulations (for example, tabletop exercises) for FMIs with relevant parties (for example, FMI participants and other FMI links) to strengthen the responses to potential cyber incidents that could have material impacts on broader payment and settlement systems.
	▪ Penetration testing	▪ Expedite penetration testing on FMIs and all critical systems and network infrastructure more regularly and after significant system changes.
	▪ Cyber stress testing	▪ Conduct cyber stress tests to make quantitative assessments of the impact of cyberattacks on systemically important FIs and FMIs, business continuity arrangements, and financial stability.

(*continued*)

Component of Cyber Guidance	Issue of Concern or Identified Gap	Recommendation, Action, and Comments
Situational awareness	- Information sharing	- Establish formal information-sharing arrangement between financial authorities, the cybersecurity agency, and FMI participants.
Learning and evolving	- Cyber resilience metrics	- Develop cyber resilience metrics for FMIs to measure, track, and improve their cyber resilience posture.
	- Benchmarking	- Strengthen supervisory and oversight expectations of bank and FMI response and recovery by using metrics for cyber resilience benchmarking, including recovery time objectives for critical functions such as payment, clearing, custody, and settlement.

Source: IMF.
Note: FMIs = financial market infrastructures; IT = information technology.

Table 5. Recommendations to Strengthen FMI Supervision and Oversight

Authorities' Responsibility	Issue of Concern or Gap or Shortcoming	Recommendation Action and Comments
Responsibility A (Regulation, supervision, and oversight of FMIs)	- FMI oversight	- Strengthen the oversight approach on cyber resilience for FMI.
	- FMI oversight	- Supplement the CPMI-IOSCO guidance with more detailed expectations on cyber risk oversight of FMIs.
	- FMI supervision	- Increase offsite and onsite supervision of FMIs.
Responsibility B (Regulatory, supervisory, and oversight powers and resources)	- Resources	- Further increase/enhance the skills and expertise of FMI overseers regarding cyber to address the changing cyber threat landscape surrounding the overseen FMIs.
	- Oversight powers	- FMI authority should develop and issue regulatory requirements, based on the CPMI-IOSCO guidance and its cyber strategy, for the FMIs under its oversight mandate.
Responsibility D (Application of the principles for FMIs)	- Consistent application	- Monitor the observance of the CPMI-IOSCO Guidance on Cyber Resilience by all systemically important FMIs to ensure ongoing efforts to adapt, evolve, and improve cyber resilience.
Responsibility E (Cooperation with other authorities)	- Authorities' cooperation	- Enhance coordination and cooperation to strengthen supervisory and oversight approach on cyber for commonly supervised/overseen FMIs.

Source: IMF.
Note: CPMI = Committee on Payments and Market Infrastructures; FMIs = financial market infrastructures; IOSCO = International Organization of Securities Commissions; IT = information technology.

7. Conclusions

Given its mandate to promote the stability of the global financial system, the IMF has made efforts on many fronts to promote effective regulation and supervision of cyber risks. The cyber risk work program, in effect since 2017, has assisted IMF members in strengthening the operational and cyber resilience of financial systems.

Key elements of the IMF cyber risk work program include FSAP cyber risk regulation and supervision assessments and TA on a wide range of topics, such as developing cyber strategies, cyber risk regulations, incident reporting frameworks, and testing frameworks; conducting cyber simulations and exercises; reviewing the cybersecurity of central banks; and building capacity and expertise of cyber risk supervisors. The breadth and intensity of this work program have enabled the IMF to develop a unique ability to observe cyber risk regulation and supervision worldwide, which has been leveraged in this paper to identify good practices.

Effective regulatory frameworks are tiered, featuring mandatory requirements that can be enforced using the supervisor's legal powers, complemented by guidance that reflects desirable outcomes but is not enforceable. A deliberate and structured approach to regulation development helps deliver a set of effective and internally consistent cyber-risk-management requirements. Key elements are (1) a unified regulation that encompasses all technology risk areas instead of separate ICT and cyber risk regulations; (2) outcome-driven and technology-agnostic expectations; (3) application of proportionality; and (4) balancing a principles-based approach with prescriptiveness, based on the maturity of risk-management practices of FIs and FMIs. Cyber risk regulatory expectations that effectively facilitate risk mitigation are usually structured according to a risk and control taxonomy that is easy to map to an internationally accepted standard. However, verbatim adoption of one is not necessary and can be counterproductive.

When it comes to good practices in supervision, the approach that is probably the most consequential in improving the cybersecurity stance of the financial sector is the presence and thoroughness of the supervisor—almost irrespective of the regulatory framework. Appropriate presence and thoroughness can compensate for weak regulation, and deficiencies in this area can make strong regulation with strict requirements largely ineffective. Although such a conclusion could have been intuitively inferred from observations on financial regulation and supervision in general, an empirical, evidence-based argument can be made that, going forward, the lion's share of the improvement effort should be spent on practices—that is, skills, people, and processes.

Assuming that the basic elements are covered, implementing or improving specific expectations should focus on cybersecurity testing, crisis simulation exercises, and third-party risk management. Generally, supervisors should avoid conducting cybersecurity tests themselves and instead take an oversight role. Requiring TLPT should be considered in a proportional manner. It is not advisable to collect full technical details of the vulnerabilities and exploits used to breach FIs and FMIs. Key aspects to focus on are adherence to the established testing framework, risk management of the process, remediation, and follow-up. Authorities should promote and drive cyber simulation exercises, especially those with broad sectoral participation. Expectations need not be mandatory initially, but the trend is toward requiring systemic FIs and FMIs to regularly participate in such exercises. Although authorities should take a more active role in exercises compared with cybersecurity tests, the focus areas—adhering to an established framework, remediation, and follow-up—are largely similar (risk management is much simpler because the exercise remains at the tabletop simulation level). Finally, the risks posed by the extraordinary growth and reliance on third-party technology services should prompt jurisdictions to bring critical providers under a cyber risk oversight framework.

References

Committee on Payment and Settlement Systems (CPSS). 2005. "Central Bank Oversight of Payment and Settlement Systems." CPMI Paper No. 8, CPSS, Basel.

Financial Stability Board (FSB). 2023. "Cyber Lexicon." https://www.fsb.org/uploads/P130423-3.pdf.

Financial Stability Board (FSB). 2025. "FSB Finalizes the Common Format for Incident Reporting Exchange (FIRE)." https://www.fsb.org/2025/04/fsb-finalises-the-common-format-for-incident-reporting-exchange-fire/.

International Monetary Fund (IMF). 2024a. "Artificial Intelligence in Capital Markets." In *Global Financial Stability Report, October 2024*. Washington, DC: IMF.

International Monetary Fund (IMF). 2024b. "Cyber Risk: A Growing Concern for Macrofinancial Stability." In *Global Financial Stability Report, April 2024*. Washington, DC: IMF.

International Monetary Fund (IMF). 2024c. "The Last Mile: Financial Vulnerabilities and Risks." In *Global Financial Stability Report, April 2024*. Washington, DC: IMF. https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024.

Khiaonarong, T., K. Korpinen., and E. Islam. 2025. "Using Simulations for Cyber Stress Testing Exercises". Working Papers WP/25/85, IMF. https://www.imf.org/en/Publications/WP/Issues/2025/05/02/Using-Simulations-for-Cyber-Stress-Testing-Exercises-566489

Poljsak, Borut. 2024. "Cyber Mapping as a Tool for Monitoring Cyber Risk." Bank of Slovenia Discussion Paper. https://www.bsi.si/en/publications/research-publications.

Ravikumar, Rangachary. 2025. *Strengthening Cybersecurity: Lessons from the Cybersecurity Survey*. Washington, DC: IMF.

PUBLICATIONS

Good Practices in Cyber Risk Regulation and Supervision

ISBN 9798229026185

9 798229 026185