FOCUS NOTE

CYBER RISKS IN FAST PAYMENT SYSTEMS

FINANCE FOR DEVELOPMENT

PROJECT FAST
FRICTIONLESS · AFFORDABLE · SAFE · TIMELY · TRANSACTIONS

FEBRUARY 2025

WORLD BANK GROUP

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

1 EXECUTIVE SUMMARY

The global retail payment landscape has undergone significant transformation in recent years. One key development is the enhancement of speed and convenience for users of retail payment services. The demand for (near) real-time retail payments has driven improvements in payment speeds across various jurisdictions. Technological advances, such as internet banking and mobile payments, have further increased the flexibility and convenience of making retail payments.

Since 2010, the number of jurisdictions offering services and systems that enable continuous (near) real-time payments has grown remarkably, with strong prospects for continued substantial growth. Fast retail payment services have been implemented or are in development in many regions. In several jurisdictions, stakeholders in national payment systems are increasingly interested in fast payments, from both the supply side and the demand side, as providers strive to offer better services and users demand more efficient options.

However, the swift adoption of fast payment systems (FPS) brings with it escalating cyber threats, a byproduct of increasing technological reliance. In addition to the risks discussed in detail in the World Bank's focus note *Risks in Fast Payment Systems and Implications for National Payments System Oversight,*[1] cyber risk must be effectively managed to ensure the safe functioning of payment systems in general and fast retail payment services in particular.

Cyber risk, a crucial aspect of operational risk, poses a significant threat to the secure and efficient functioning of the financial sector, as it continues to face a surge of cyberattacks. Of special concern is the systemic nature of cyber risk. Cyberattacks such as distributed denial-of-service and ransomware attacks can disrupt the normal operations of national payment systems, preventing the execution of transactions, affecting liquidity and the availability of funds that could lead to a breakdown in financial intermediation and economic activity. Due to the interconnected nature of financial institutions, a severe attack on a payment system or on a key participant can trigger systemic risk, threatening the stability of the entire financial system.

In addition, FPS are especially attractive targets for fraud, money laundering, and other illicit activities, as cyber criminals try to exploit the speed of these systems to move funds undetected.

The often borderless nature of cyber crime and the interconnectedness of financial systems triggered international standard-setting bodies, including the Financial Stability Board, Basel Committee on Banking Supervision, Committee on Payments and Market Infrastructures, and International Organization of Securities Commissions, to develop cybersecurity guidelines and frameworks that have been adopted by jurisdictions worldwide. The main objective of these initiatives is to strengthen cyber resilience and manage cyber risks more effectively in the financial sector, including within the FPS ecosystem.

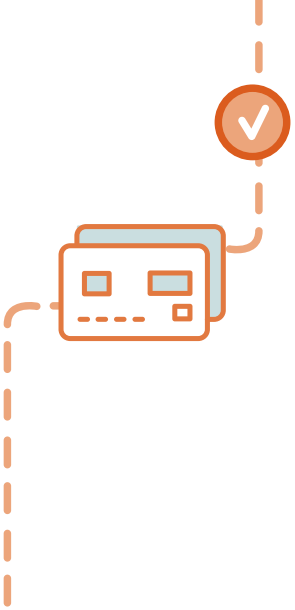
Lessons learned from successful FPS implementations discussed in this note highlight the importance of implementing a robust cyber risk–management framework, supported by a suitable governance structure with clear roles and responsibilities for managing cyber risk. Equally important is the existence of an effective regulatory framework for managing cyber risk. Without sufficient oversight, regulated entities may not be able to identify and mitigate systemic cyber risk that stems from payment systems.

Furthermore, having in place a robust incident-response plan that is frequently tested is another success factor highlighted by FPS operators and participants, along with periodically tested disaster recovery and business-continuity capabilities to resume operations quickly and safely in case of a severe incident. Continuous awareness of the changing threat landscape through relevant cyber intelligence and information sharing arrangements allows these organizations to adjust the security control environment to address emerging cyber risks. The security controls spanning the human, process, and technological layers are frequently tested in these organizations to ensure that they are operating as designed to address cyber threats relevant to the organization effectively. This highlights the importance of implementing preventive, detective, and corrective controls for the mitigation of cyber risk.

Emphasizing the critical need to enhance cyber resilience and manage cyber risks within the FPS ecosystem, this technical note discusses the cyber threats relevant to FPS and provides guidance for participants in the FPS ecosystem to manage these risks effectively. FPS operators and providers should use recognized international cybersecurity standards, frameworks, and guidelines as a starting point to create their cybersecurity programs, tailored to the nature, size, complexity, risk profile, and culture of the organization. The technical note also provides policy considerations for regulators to enhance cyber resilience in their FPS ecosystems.

The *World Bank's Global Payment Systems Survey*[3] shows progress toward enhancing cyber resilience in many jurisdictions, as most respondents have adopted a cyber risk–management framework that follows a homogeneous structure reflecting industry leading practices and international standards that include the identification of critical assets and appropriate means to protect them, as well as detection, response, and recovery procedures. However, there is work to be done in many other jurisdictions, as the survey also shows that, for example, one-quarter of respondents still do not have in place a specific framework to manage cyber risks.

To further support efforts to enhance cyber resilience in the financial sector, the World Bank collaborates with countries to build capacity to protect critical infrastructure and systems, increase cyber awareness, and foster trust, so that people, governments, and businesses can thrive in today's digital landscape.[4]



2 INTRODUCTION

The World Bank has been monitoring closely the development of fast payment systems (FPS) by central banks and private players across the globe. This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit is designed to guide countries and regions on the alternatives and models that could assist them in their policy and implementation choices when they embark on their fast payments journeys. Work on the fast payments toolkit is supported by the Bill and Melinda Gates Foundation through the Finance for Development Umbrella Program.

The toolkit can be found at fastpayments.worldbank.org[2] and consists of the following components:

- The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
- Case studies of countries that have already implemented fast payments
- A set of short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide inputs on aspects of cybersecurity related from an FPS perspective.

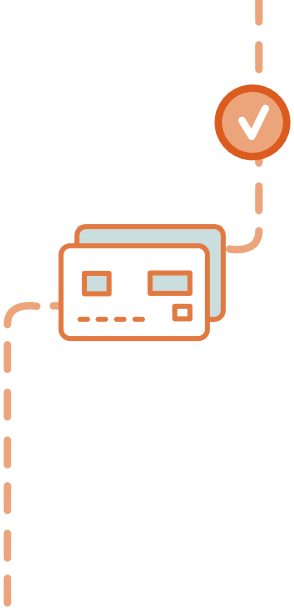
1.1 SCOPE

The scope of the note is cyber risks relevant to payment systems in general and to the different participants of an FPS ecosystem and discusses considerations to manage these risks effectively following recognized international frameworks and guidelines.

These risks and considerations are applicable to FPS under development and existing FPS in all jurisdictions but are particularly relevant to FPS participants in low- and middle-income economies that, due to resource constraints or nascent payment system environments, have not been able to implement appropriate cyber risk–management frameworks.

1.2 INTENDED AUDIENCE

This note aims to provide guidance to the participants of an FPS ecosystem, such as payment system infrastructure operators, payment service providers, and end users, but also partially discusses policy considerations for FPS regulators. The intention of this technical note is not to replicate international frameworks and guidelines but to underscore leading practices that are paramount for managing cyber threats pertinent to the FPS ecosystem.



3 CYBER RISK IN PAYMENT SYSTEMS

Cyber risk is a form of operational risk that poses a significant threat to the secure and efficient functioning of the financial sector. According to the International Monetary Fund (IMF), the financial sector has experienced more than 20,000 cyberattacks in the last 20 years, with operational losses of approximately $12 billion.[5]

According to a report published by FS-ISAC and Akamai Technologies,[6] in 2023 distributed denial-of-service (DDoS) attacks reached new heights of size and sophistication, and the financial sector was the top target across most of the world. Similarly, in 2023 the number of ransomware attacks in the finance industry surged by 64 percent, according to a report published by cybersecurity company Sophos.[7]

Cyberattacks of this nature can disrupt the normal operations of national payment systems. In December 2023, the Central Bank of Lesotho reported a cyberattack[8] that forced it to temporarily suspend the operations of some of its systems. In May 2018, the Central Bank of Mexico reported cyberattacks[9] against participants in the electronic funds transfer system. These types of disruptions can prevent the execution of transactions, affecting liquidity and the availability of funds, and this could lead to a breakdown in financial intermediation and economic activity.

Payment systems comprise financial market infrastructures (FMIs) and are a vital part of the financial sector and the wider economy. The interconnected nature of financial institutions means that a cyber incident at one institution can have spill-over effects, causing other institutions to be unable to settle their obligations. A severe attack on a major financial institution or payment system can trigger systemic risk, threatening the stability of the entire financial system. The impact of such a cyberattack can ripple through the financial system via three critical channels, according to the IMF:[10] loss of confidence, lack of substitutes for the services rendered, and interconnectedness.

A significant breach or service disruption can lead to a loss of confidence in the viability of the targeted institution, resulting in potential runs on other financial institutions, market sell-offs, and broader economic instability. An incident affecting a key institution that is not easily substitutable—such as a ransomware attack against a major bank that participates in payment systems, the failure of key cloud service providers, the hacking of a central bank, or the interruption of operations of an FMI (such as electronic trading systems or clearing houses)—could all cascade rapidly and undermine financial stability. Finally, the impact of a cyber incident affecting a financial institution that is interconnected to others through technological linkages (for example, several institutions using the same cloud infrastructure, data center, platform, or software) or financial linkages (such as settlement systems) could quickly propagate across the financial system.

Cross-border payment arrangements add another layer to the systemic risk for the whole financial sector, as discussed in the World Bank's focus note *Cross-Border Fast Payments*.[11]

Payment systems are considered systemically important if they have the potential to trigger or transmit systemic disruptions. This includes systems that, among other things, make up the sole payment system in a country or the prin-

cipal system in terms of the aggregate value of payments; systems that manage time-critical, high-value payments; and systems that settle payments used to affect settlement in other systemically important FMIs. As a result, in some jurisdictions, payment systems are considered or have been designated as prominently important or systemically important payment systems by regulatory authorities. If the trend continues, the number of these payment systems to be so designated is likely to increase.

The borderless nature of cyber crime and the interconnectedness of financial systems triggered the work of international standard-setting bodies, including the Financial Stability Board, Basel Committee on Banking Supervision, Committee on Payments and Market Infrastructures (CPMI), and International Organization of Securities Commissions (IOSCO), among others. This work led to the development of guidelines and frameworks that have been adopted by jurisdictions worldwide to strengthen cyber resilience and manage cyber risks more effectively in the financial sector.

In particular, *Guidance on Cyber Resilience for Financial Market Infrastructures*[12] from the Bank for International Settlements (BIS) provides guidance for FMIs to enhance their cyber resilience around five primary risk-management categories (governance, identification, protection, detection, and response and recovery) and three overarching components (testing, situational awareness, and learning and evolving) that should be addressed across an FMI's cyber resilience framework. In order to achieve resilience objectives, investments across these guidance categories can be mutually reinforcing and should be considered jointly. In addition, for investments to be effective and yield the desired results, investments in complementary assets, such as user awareness training that supports these activities, are highly recommended.[13]

- **Governance:** Cyber governance encompasses the arrangements that an FMI has established to define, implement, and continually assess its approach to managing cyber risks. Effective governance begins with a well-defined and comprehensive cyber resilience framework. This framework should be informed by a strategic approach to cyber resilience. The framework must also delineate the roles and responsibilities of the FMI's board (or equivalent governing body) and its management.
- **Identification:** FMIs need to pinpoint their critical business functions and the supporting information assets that require protection. This prioritization ensures that these vital components are safeguarded against compromise. The guidance provides a road map for FMIs to identify and categorize their business processes, information assets, system access, and external dependencies.
- **Protection:** Cyber resilience hinges on robust security controls that safeguard the confidentiality, integrity, and availability of an organization's assets and services. The guidance details how FMIs should strategically deploy suitable controls and design systems and processes aligned with leading practices to proactively prevent, mitigate, and contain the impact of any potential cyber incidents.
- **Detection:** An essential capability for FMIs is swiftly detecting anomalies and events that signal a potential cyber incident. At a minimum, detective controls need to be implemented by organizations, especially when relevant preventive controls haven not been deployed or do not function as effectively as intended. Given the stealthy and sophisticated nature of cyberattacks, coupled with the myriad entry points through which compromise can occur, FMIs must deploy advanced monitoring capabilities to thoroughly track and analyze anomalous activities.
- **Recovery:** FMIs should meticulously design and rigorously test their systems and processes to ensure the secure resumption of critical operations following any disruption. In this respect, the existence of corrective controls is essential. The guidance outlines how FMIs should strategically respond to contain, resume, and recover from successful cyberattacks.
- **Testing:** Thoroughly testing the cyber resilience framework is crucial to assessing its effectiveness. The guidance describes the specific components that an FMI's testing program should cover and how the insights gained from testing can inform enhancements to the overall cyber resilience framework.
- **Situational awareness:** Maintaining strong situational awareness significantly bolsters FMIs' ability to anticipate and preempt cyber events. To achieve this, FMIs should proactively monitor the ever-evolving cyber threat landscape. They must also harness actionable threat intelligence to validate their risk assessments, align strategic direction, allocate resources, fine-tune processes and procedures, and fortify controls. The guidance emphasizes active participation in information-sharing arrangements and collaboration with trusted stakeholders both within and beyond the industry.
- **Learning and evolving:** FMIs ought to adopt an agile and flexible cyber resilience framework that adapts along-side the ever-shifting landscape of cyber risks. This dynamic approach enables effective risk management. Moreover, FMIs should foster a pervasive culture of cyber risk awareness, emphasizing continuous reevalua-

tion and enhancement of their cyber resilience posture across all organizational levels.

Well-designed large-value payment systems play a critical role in ensuring a safe, reliable, and efficient financial sector while also facilitating the smooth execution of monetary policy. These systems contribute significantly to overall financial stability. However, it is crucial to recognize that any vulnerabilities in their risk-management framework can give rise to systemic risk, potentially affecting the entire financial ecosystem. Consequently, central banks have long kept a watchful eye on large-value payment systems, often directly owning and operating them within a country's national payment infrastructure. Among the key players in this arena is real-time gross settlement (RTGS), which handles high-value and time-critical payments. The widespread adoption of RTGS systems underscores their pivotal role in mitigating settlement and systemic risks.

For example, the World Bank's Global Payment Systems Survey (2021) shows that 97 percent of surveyed economies are using at least one RTGS system. Some RTGS systems are used by two or more economies (for example, TARGET2 in the Euro area), while some economies use more than one RTGS system (as is the case in Hong Kong). In addition, international standards and leading practices for RTGS systems are increasingly being adopted in all relevant areas, including resilience and business continuity, identification, and detection of and protection from cyber threats. The results of the survey show that SWIFT user groups and proprietary telecommunication networks are the most common means through which direct participants send their payment orders to the RTGS systems.

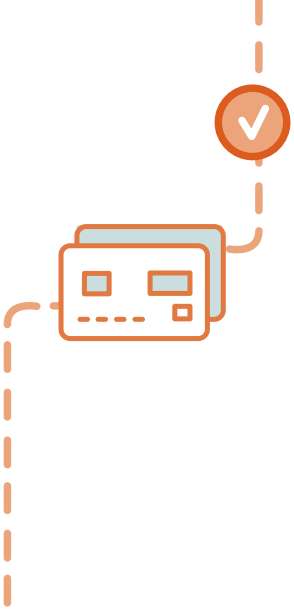
Interestingly, in one of the most notorious cyberattacks in the financial sector, the target was not an FMI but the messaging platform. Such was the case of the Bangladesh Bank heist in February 2016,[14] when attackers successfully passed fraudulent payment messages through SWIFT, a messaging platform used by more than 11,000 financial institutions in more than 200 countries. In this attack, hackers stole credentials from the bank and sent fraudulent transfer requests to the Federal Reserve Bank of New York, which held the Bangladesh Bank's account. Although the New York Federal Reserve could block most transactions (totaling $850 million), approximately $101 million was transferred to foreign bank accounts, and $81 million was later funneled through casinos, making it challenging to track the lost money.

In response to such incidents, SWIFT in 2016 established the Customer Security Controls Framework,[15] which includes control guidelines for its clients to securely manage their SWIFT environment. SWIFT's Customer Security Programme empowers financial institutions to keep their defenses against cyberattacks current and robust, safeguarding the integrity of the broader financial network. Clients assess the security measures they have put in place by comparing them to the guidelines outlined in the framework and then annually affirm their compliance level.

With the exception of a subsequent cyberattack against Banco de Chile[16] in May 2018, SWIFT-related cyberattacks have been less successful, suggesting that the framework has been effective and highlighting the importance of coordinated efforts to improve the preparedness of SWIFT clients.

It has to be noted that progress has been made toward enhancing cyber resilience in the financial sector. For example, the World Bank's Global Payment Systems Survey also shows that cybersecurity laws are now in place in more than half of the jurisdictions surveyed (59 percent). Globally, 80 percent of respondents stated that their economies have a national strategy to address cybersecurity and/or cyber resiliency; 71 percent have a strategy at the financial sector level and 85 percent at the central bank level. Most respondents also adopted a cyber risk–management framework that follows a homogeneous structure reflecting industry-leading practices and international standards that include the identification of critical assets and appropriate means to protect them, as well as detection, response, and recovery procedures.

However, there is work to be done in many jurisdictions, as the survey also shows that one-quarter of respondents still do not have in place a specific framework to manage cyber risks. In addition, comprehensive national or sectoral cybersecurity strategies that effectively incorporate payment systems are often lacking. This is especially true for low-income and emerging economies. Quite frequently, FMIs have not been designated as national critical infrastructure, and as a result, a national-level incident-response plan does not exist for cyber risk–related events that may affect payment systems or are specifically related to FMIs.



4 CYBER RISK IN FAST PAYMENTS

Internet banking, mobile payments, and other technological developments have increased the flexibility and convenience of making and receiving digital retail payments. The number of jurisdictions with services and systems that allow users to conduct (near) real-time payments on a continuous basis has grown impressively.

The accelerated progress in computing technology, coupled with the reduced expenses for technological infrastructure, enhances the practicality of deploying FPS, enabling swift and efficient processing of complete transaction cycles. Initiatives such as the development of digital public infrastructure (DPI) enable nontraditional players to enter the FPS market with innovative solutions that lower the costs, improve the speed of transactions, and increase accessibility. (See box 1.)

However, the swift adoption of FPS brings with it an escalation of cyber threats, a byproduct of increasing technological reliance. The cyber risks relevant to payment systems are further intensified by several intrinsic factors related to the FPS landscape: the relentless pace of digital transformation and innovation, an evolving regulatory framework, the intricacies of a complex supply-chain ecosystem, and the operational demands of round-the-clock service, coupled with the anticipation of instantaneous fund access. Furthermore, the inherent rapidity of FPS makes them prime targets for fraud, money laundering, and related illegal endeavors, as cyber criminals could potentially leverage the systems' velocity to transfer funds covertly.

4.1 TYPES OF CYBER RISKS RELEVANT TO FAST PAYMENTS

FPS participants on both the demand and supply sides are exposed to threats that could lead to cyber risks, such as the disruption of critical services and the compromise of the confidentiality, integrity, and privacy of sensitive data. The relevance of these cyber risks depends on the role that the participant plays in the FPS ecosystem. For instance, actors including FPS operators, regulators, or payment service providers (PSPs) face different cyber risks than the consumers of the services.

Cyber Risks Relevant to FPS Operators and Service Providers

- **Disruption of critical services:** Typically, the most relevant consideration for FPS operators and PSPs is ensuring cyber resilience and the continuous availability of the FPS services, as users expect 24/7 operations and the immediate availability of funds. Cyberattacks such as DDoS or ransomware attacks may make critical systems and services unavailable. Similarly, the disruption of services at a key service provider (for example, the widespread IT outage[17] experienced in July 2024, when 8.5 million Microsoft Windows devices were affected) or in other sectors of the economy (see figure 1) may affect the organization's ability to provide its services as expected. For example, a DDoS attack on the internet service pro-

BOX 1 DIGITAL PUBLIC INFRASTRUCTURE

Digital public infrastructure, often referred to as DPI, represents the combination of networked open technology, effective governance, and innovative and competitive market players that enables the improved delivery of public services via digital channels. Open-source technology acts as a key enabler of DPI. Like other electronic information systems that support critical infrastructure and associated business processes, DPI is not without risk. From a cyber and operational risk point of view, DPI may be vulnerable to cyberattacks in the form of system disruptions, such as DDoS attacks and data compromise.[18] In addition, due to the increased convergence of cyberattacks and some of the more traditional forms of fraud, DPI may be prone to cyber-enabled fraud, especially when considering the provision of payment services that are needed to support the delivery of public services to the general population. In environments where sensitive data is processed and stored, DPI may also be exposed to the risk of ransomware, which may subsequently lead to a disruption of services, as identified above. Therefore, conducting thorough risk assessments that address the specificities of the DPI business model and associated cyber risk is critical. This includes assessing risk that may stem from the various avenues and channels of service delivery within DPI. Since payment systems may form a critical component of DPI, risk assessments need to cover the cyber risk aspect of integrating and offering payment services as a part of DPI. The World Bank's focus note *Open Banking in the Context of Fast Payments* explores the topic of open-source systems, including risk management and the use of open-source technology for the provision of fast payment services.

vider of the FPS that disrupts internet-based processes may render payment services unavailable to consumers.

- **Unauthorized disclosure:** Ensuring the confidentiality of sensitive information is critical for these organizations. The unauthorized disclosure of sensitive information about the organization (such as the board's internal discussions) may lead to serious reputational damage. Similarly, the unauthorized disclosure of privileged IT and business users' credentials in a hackers forum may be used to craft further attacks on the organization or to conduct fraudulent activities.
- **Compromise of data privacy:** A data breach due to unauthorized disclosure of sensitive customer information may lead to serious reputational damage and monetary loss due to noncompliance penalties and increase the risk of fraudulent transactions.
- **Loss of information:** FPS operators and PSPs may lose critical operational information due to ransomware or to the inability to restore information after a cyber incident. This may affect the organization's business continuity.
- **Compromise of data integrity:** Users of the FPS services expect that their transactions have not been modified and are not altered. Protection against data interception, wiretapping, and the alteration of transaction-related messages must be implemented to ensure the integrity of the transactions.
- **Third-party compromise:** FPS operators commonly rely on a complex supply-chain ecosystem that encompasses third parties providing a variety of services, such as cloud infrastructure hosting and data processing, telecommunication channels, software development, and so on. The compromise of a trusted third party may allow an attacker to gain unauthorized access to the organization's network and systems.
- **Access-channel compromise:** A breach in the security of access channels used in the FPS ecosystem, such as QR codes or mobile banking applications, could lead to fraud, identity theft, or compromise of data confidentiality. Scammers may replace a legitimate QR code with a fraudulent one to route payments to a different destination or to lead customers to a malicious website to install malware on the end users' devices or request that customers enter bank account information or log-in credentials. (Please refer to the World Bank's focus note *The Use of Quick-Response Codes in Payments*.[19]) Security vulnerabilities in mobile banking apps may lead to similar risks if exploited by an attacker. This may damage consumers' confidence in the payment system arrangement.

- **Proxy service compromise:** Inappropriate protection of proxy identifiers or aliases database may lead to the registration of fraudulent aliases or unauthorized changes to the aliases, allowing cyber criminals to conduct fraudulent transactions.

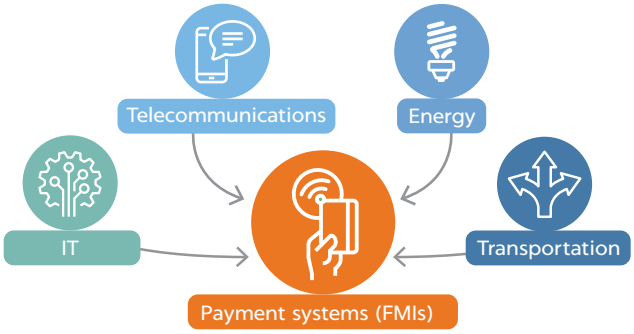
The impact of a cyberattack may span multiple risk domains. These may include other forms of operational risk, such as legal and regulatory risk, or outside the realm of operational risk, the impact may take the form of reputational risk. It is becoming harder to assess the impact of these cyber risks in isolation, or when solely confined to the domain of operational risk. For instance, a cyberattack (such as ransomware) that leads to monetary loss or the disruption of business operations can be linked to operational risk. In addition, the event may also have an impact on legal and regulatory risk if there is a customer privacy breach. However, the organization's reputation may also be harmed if the cyberattack leads to a loss of public confidence or a prolonged disruption of services in a specific financial institution or the whole financial sector. Furthermore, some of the costs of a cyberattack are well understood and can be estimated (for example, regulatory fines, public relations costs, breach notification, protection costs), but some effects may linger for a considerable period of time and are harder to estimate, as they may have an intangible impact tied to reputation damage or loss of strategic assets and competitive advantage.

Cyber Risks Relevant to Regulators

A wide range of challenges and risks need to be considered from a supervisory perspective, including the following:

- **Systemic risk:** The failure of one or more participants in the FPS ecosystem may trigger a chain reaction, causing other participants to be unable to settle their obligations. The interconnectedness of the financial system and the compounding effects of some cyber incidents (when the impact spans multiple risk domains) add complexity to the management of the risk. As a result, a large-scale cyber event associated with FPS, especially if a specific payment system is used by a considerable portion of the population and does not have many substitutes, may have significant implications for financial stability. Figure 2 depicts the impact that various cyber risk–related events may have on financial stability.
- **Unavailability of critical infrastructure:** Some jurisdictions categorize the financial system as critical infrastructure due to how critical it is to the normal functioning of society. Since FPS are a key part of the financial system, a cyberattack against the FPS may have nationwide implications. Therefore, it is vital for national regulatory authorities to assess whether an FPS should be incorporated into national critical infrastructure.
- **Loss of user confidence:** One major cyber incident may undermine user confidence in the system. Amid geopolitical tensions, some cyber criminals may target the FPS ecosystem to undermine its ability to work normally, potentially undermining citizens' confidence in their national agencies.

FIGURE 1 **Critical Dependencies of FMIs (Payment Systems) on Other Sectors of the Economy**



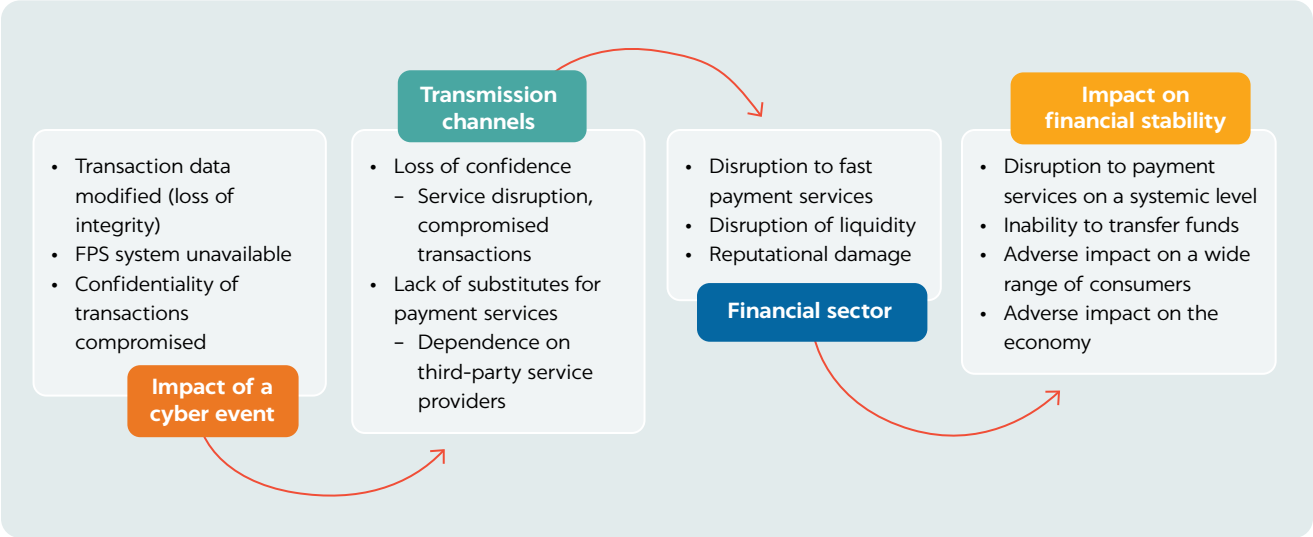
Fast payments require data and privacy protection. As for all digital financial services, breaches of privacy and data security may result in identity theft, harm to financial records, fraud, and other risks. Regulators should set proper legal and regulatory provisions and set up the legal obligations of data controllers and processors.

Establishing a cyber risk supervisory framework is a vital step; however, the core of its effectiveness lies in the comprehensive implementation of the framework, including mitigation of risks associated with payment systems within the jurisdiction. This becomes paramount in environments where oversight is distributed among various supervisory authorities, as this can lead to potential overlaps or omissions in regulatory coverage. Therefore, it is imperative that the implementation of such a framework is meticulously designed to ensure seamless integration and full-spectrum risk management.

Cyber Risks Relevant to End Users

- **Identity theft:** The main cyber risk for consumers relates to the compromise of their identity. Cyber criminals may try to steal personal information, such as usernames or passwords, or compromise personal devices, to impersonate users and gain unauthorized access to their accounts.
- **Fraud:** Cyber criminals may conduct fraudulent activities using compromised user accounts, devices, or access

FIGURE 2 **FPS Cybersecurity and Its Impact on Financial Stability**



Source: Illustration adapted from "Cybersecurity and Macrofinancial Stability: Channels of Transmission" in IMF, *Global Financial Stability Report* (2024).[20]

channels, such as QR codes and mobile banking apps, as previously described. This may lead to the loss of user confidence in the system.

- **Loss of privacy:** Cyber criminals may use compromised personal information, such as usernames or passwords, not only to conduct fraudulent transactions in the system but also to reconstruct the individual's identity or to craft further attacks aimed at acquiring additional personally identifiable information.

4.2 CYBERATTACKS TARGETING FPS

The FPS ecosystem offers a rapidly growing and changing attack surface (see box 2) that is targeted by threat actors.

At the human layer, attackers often exploit consumer cyber illiteracy by targeting the human element and the endpoints and applications they use to conduct fast payment transactions.

At the same time, the continuous digital transformation and innovation seen in the financial industry drive the quick adoption of innovative technologies and transaction channels used for initiating and receiving fast payments (for example, USSD, QR codes, NFC, digital wallets). The software and infrastructure supporting these channels must be deployed securely to protect the confidentiality and integrity of sensitive data. On the other hand, some well-established financial institutions may struggle to support complex back-end legacy systems or outdated supporting infrastructure that could be exploited by threat actors to gain a foothold on their networks. The complexity of information systems associated with payment-related processes can represent a considerable source of cyber risk. Appendix E contains a sample threat checklist that organizations may use to assess cyber threats that can pose a risk to their operations.

FIGURE 3 **Attack Surface Categories**

The attack surface refers to exploitable weakness and vulnerabilities across the following layers:

Network

- Attacks targeting the vulnerabilities of FPS operators' and PSP network, wide area network, and the internet. Examples include DDoS attacks, disruption of communication channels, and different forms of intruder attacks.

Software

- Associated with vulnerabilities in websites, applications, utilities, or operating system code used by FPS operators and PSPs. Special consideration should be given to risks related to the use of vulnerable third-party code (for example, the SolarWinds incident).

Human

- Vulnerabilities that may arise from people, including employees and outsiders. This includes events ranging from human error to social engineering and unauthorized activity that may come from insiders within the organization.

An increasingly complex supply-chain ecosystem may leave FPS organizations exposed to unforeseen attack vectors through their service providers (for example, cloud service providers). Given the 24/7 operations and expectations of immediate fund availability, the reputation of organizations in the FPS ecosystem could be damaged if incidents at the third parties affect the availability of their services. For example, in December 2023, a ransomware attack on a cloud service provider affected the operations of about 60 credit unions in the United States.[21] In addition, if FPS operators and service providers use cloud-based risk-management systems for fraud-detection or cyber risk–prevention purposes, these organizations should closely assess any reputational risk that might arise if the cloud-based risk-management systems are unable to adequately/sufficiently detect fraudulent or cyber risk–related activity.

Threat actors employ different tools and techniques to conduct their attacks against FPS participants. Box 2 describes typical threat actors and their motivation to attack FPS participants.

Cyberattacks Targeting FPS Operators and Service Providers

Cyber criminals, nation-state actors, and insider threats are typically the most relevant threat actors for FPS organizations. The following types of attacks conducted by these threat actors are among the most prevalent:

- **Distributed denial of service:** DDoS attacks flood a targeted FPS server or network with excessive traffic, rendering it unavailable to legitimate users. Critical services (for example, payment gateways, websites) can become inaccessible due to these attacks. This could lead to frustration and inconvenience for FPS consumers, damaging the PSP's reputation, affecting customer loyalty and confidence. DDoS attacks can also lead to direct financial losses for the PSPs.
- **Ransomware:** Ransomware encrypts a victim's files and demands payment (usually in cryptocurrency) for decryption. Data loss, disruption of business operations, and financial losses can occur if an FPS organization falls vic-

BOX 2 THREAT ACTOR CATEGORIES

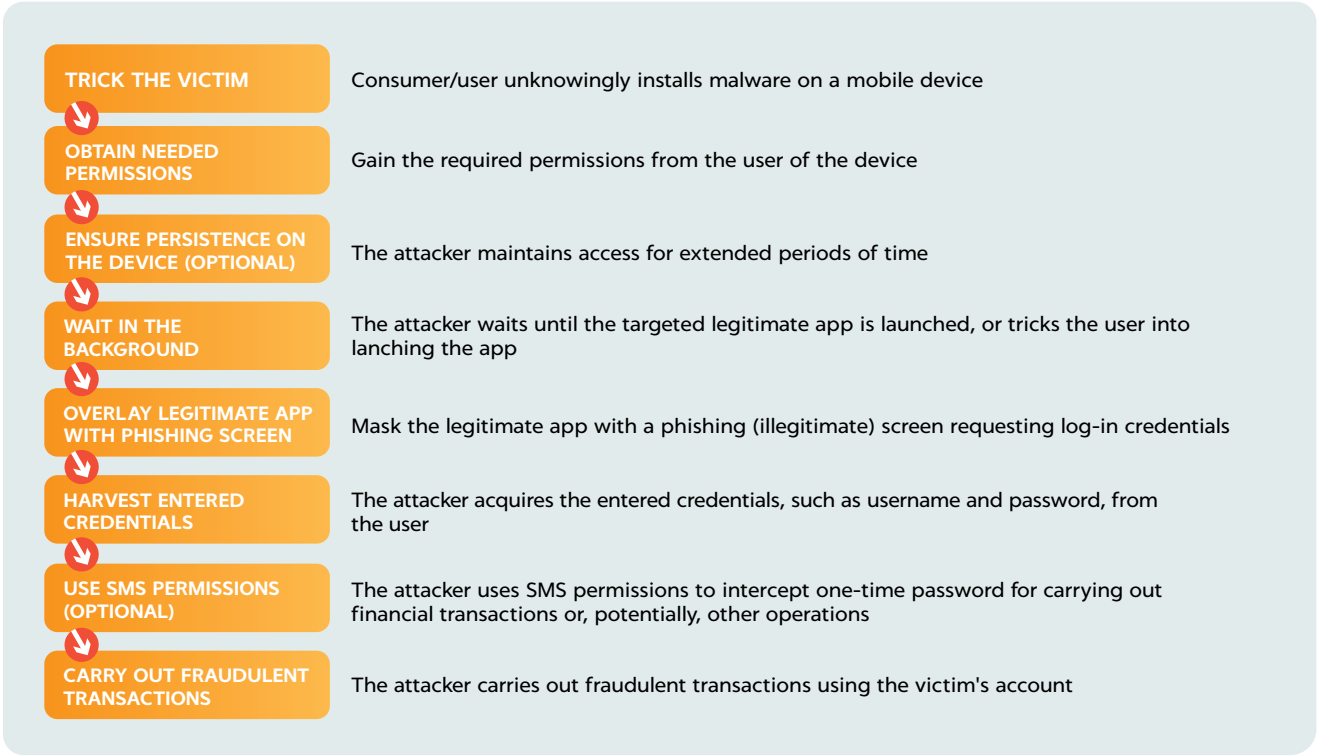
Threat actors are typically categorized into different types based on their motivation and sophistication. The list below ranks them based on their relevance to the FPS ecosystem.

- **Cyber criminals:** Individuals or groups who conduct cyberattacks (for example, ransomware, phishing scams) against FPS organizations mostly for financial gain. FPS targets are especially attractive to cyber criminals, as funds can be moved quickly through the system and identities can be hidden behind an alias.
- **Nation-state actors:** Groups well funded by nation states and governments with the goal of stealing sensitive data or disrupting another government's critical infrastructure. In many jurisdictions, FPS is part of the country's critical infrastructure (even though it may not be officially designated as such) and hence an attractive target for these threat actors.
- **Cyberterrorists:** Individuals or entities that start politically or ideologically motivated cyberattacks that threaten or result in violence. Some cyberterrorists are nation-state actors; others are actors on their own or on behalf of a nongovernment group. Disruptions to the FPS could be used by cyberterrorists to create instability and loss of confidence in the financial system in a targeted country.
- **Insider threats:** Employees of FPS operators and PSPs who intentionally (disgruntled or unhappy employees) or unintentionally (negligent, complacent, or uninformed employee) cause harm to their organization.
- **Hacktivists:** Individuals or entities that use hacking techniques to promote political or social agendas. Hacktivists target individuals, organizations, or government agencies to expose secrets or other sensitive information. They may target FPS organizations that stand for commercial practices they dislike.
- **Thrill seekers:** Individuals who attack computers and information systems primarily for fun or to gain notoriety. Some lack advanced technical skills (script kiddies) but use preexisting toolkits to attack vulnerable systems, primarily for amusement or personal satisfaction. Using these toolkits, they may compromise consumers' devices and credentials.

tim to ransomware. Please see box 3 for more details on the life cycle of ransomware attacks.

- **Phishing scams:** This type of attack involves fraudulent attempts to deceive employees into revealing sensitive information, such as log-in credentials, which are then used to get unauthorized access to the organization's network, systems, or information.
- **Malware attacks:** Malware refers to malicious software (such as viruses, worms, logic bombs, trojans, spyware) designed to harm or compromise computer systems. In recent years, mobile banking trojans targeting payment systems have increased.[22] Figure 2 depicts the typical mode of operation of trojans that target payment system–related mobile applications. Employees are tricked into downloading malware by clicking on links delivered via phishing emails or embedded in malicious software on compromised websites or in fraudulent QR codes. This type of attack may lead to unauthorized access to the organizations' infrastructure.
- **Business email compromise:** This type of attack targets employees at the FPS operator or PSP. In an attack, a legitimate sender (usually someone important in the FPS organization) is impersonated by spoofing their email address, imitating the individual's writing style, or using other tactics to trick their victims into starting unauthorized transactions, sending money, or revealing confidential company information through email. Successful attacks can result in substantial financial losses for the operator or the PSP. Business email compromise campaigns can also target the consumers of FPS.
- **Identity theft:** Identity theft refers to attacks that lead to the stealing of system credentials of privileged IT or business users with the purpose of conducting unauthorized or fraudulent transactions on their behalf or using these privileges to craft further attacks. FPS are especially attractive targets for money laundering and other illicit activities, as cyber criminals may want to exploit the speed and anonymity (through aliases) of these systems to move funds undetected.
- **Application or middleware vulnerabilities and misconfigurations:** Unaddressed vulnerabilities or configuration errors in software applications and middleware, such as databases and application programming interfaces utilized by FPS operators or PSPs, may present opportunities for attackers to compromise the organization's infrastructure and gain unauthorized access.

FIGURE 4 Typical Mode of Operation for a Mobile App Trojan Affecting a Payment System



BOX 3 THE LIFE CYCLE OF RANSOMWARE

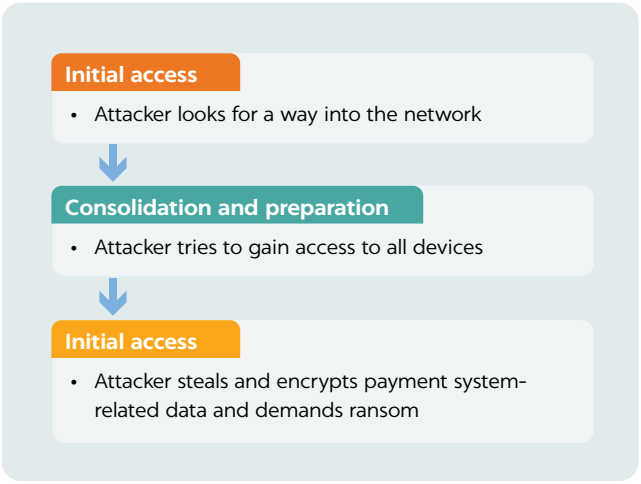
Originally developed by Lockheed Martin in 2011, the cyber kill chain model[23] helps illustrate the various stages of several common cyberattacks and the points where the attack can be prevented, detected, or intercepted. A simplified diagram (figure 3) shows how a ransomware attack against an FPS operator or service provider may unfold.

During the initial phase, an attacker will attempt to gain access to the target's network. This may involve the use of phishing, password guessing, exploiting a technical vulnerability, or sending email. The use of phishing and password guessing may lead to the attacker gaining access to valid credentials, which will lead to the compromise of an internet-facing service. Vulnerability exploitation may also lead to acquiring access to an internet-facing service. If email is used to gain initial access, a document may be sent to the target organization containing malware in the form of ransomware.

During the consolidation and preparation stage, if the attacker gains initial access to the payment system's network, establishing command and control will be the next objective, in order to gain access to specific systems or modules and move laterally within the network. Privilege escalation within the payment system, such as gaining administrative rights, may also be attempted during the consolidation and preparation stage.

During the final phase of the ransomware attack, the attacker will attempt to encrypt or even steal critical or sensitive data that is vital for the operation of a payment system. Then the attacker will seek a ransom to return or decrypt the data.

FIGURE 5 Life Cycle of a Ransomware Event[24]



Figures 6 and 7 present two sample vectors for a ransomware attack. In the first case, the attacker uses email to send a malicious attachment containing ransomware. The email message is intended for an employee of the FPS operator or service provider. If the employee opens the malicious attachment that is contained within the email, the attacker is then able to gain access to the organization's network, establish some level of command and control, move laterally within the network/system that was compromised, escalate privileges within the payment system, and then encrypt critical payment-related data.

In the second example, the attacker uses either a phishing link or password guessing to gain valid credentials to receive access to an internet-facing payment system. The attacker subsequently enters the organization's network, establishes a certain level of command and control over the compromised information system, moves laterally within the organization's information system environment, and then destroys backups.

PSPs could also use attack trees to get a better understanding of how cyberattacks are conducted. Attack trees use a hierarchical representation of the steps needed for a successful attack. Figure 6 shows an attack tree for a cyber incident in which the attacker's goal is to compromise the account used by a consumer to access the FPS. The branches within the figure depict the different methods via which the user account may be compromised. These include such methods as user account compromise, the injection of commands, security policy violations, and other actions. Advanced organizations with complex information systems use threat modelling techniques to better understand the most relevant threat actors and threats that may pose a risk to the most critical assets, so appropriate security controls can be implemented to protect them. Threat modelling exercises could be systematically conducted using comprehensive models (for example, STRIDE, MITRE) or in an ad-hoc manner based on the opinion of a subject matter expert. As resources are scarce, these techniques help organizations focus on protecting the most critical assets from the most relevant threats.

FIGURE 6 Ransomware Attack Example Using Email

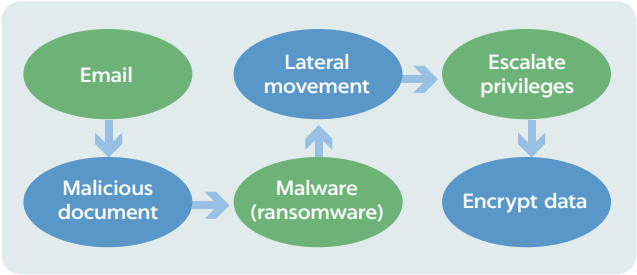


FIGURE 7 Ransomware Attack against a Payment System Using Phishing or Password Guessing

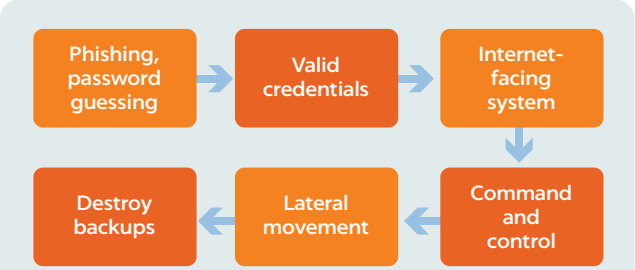


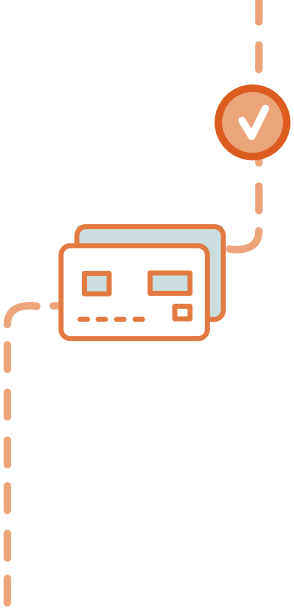
FIGURE 8 Potential Attack Tree for the Authentication of an FPS Operator or PSP System User

Source: Adapted from Stallings and Brown 2014[25]

Cyberattacks Targeting Consumers

An isolated cyberattack on individual customers is unlikely to significantly disrupt the FPS ecosystem unless it affects a substantial number of customers. However, FPS consumers often fall prey to various threat actors, including cyber criminals, cyberterrorists, hacktivists, and thrill seekers, who employ a range of tools and techniques to target them via the following methods:

- **Phishing scams:** Phishing campaigns may also target FPS consumers, with the intent of deceiving individuals into revealing sensitive information, such as personally identifiable information, log-in credentials, or financial details. The attacker can use this information to impersonate legitimate FPS consumers to conduct unauthorized or fraudulent activities.
- **Malware attacks:** Threat actors may also trick FPS consumers into downloading malicious software by clicking on links delivered via phishing emails, embedding the malicious software on vulnerable websites, or redirecting consumers to web pages that they control. Malware can compromise consumer devices, allowing the attacker to steal sensitive information or conduct fraudulent activities. Zimperium's *2023 Mobile Banking Heists Report*[26] finds 29 malware families targeted 1,800 banking apps across more than 60 countries in 2023. The report highlights new capabilities seen in malware, including the Automated Transfer System, a technique that eases unauthorized transfers of money.
- **Ransomware:** Ransomware attacks may also target individuals, as attackers try to collect a ransom from FPS consumers. Ransomware can encrypt critical data stored on a consumer's device, rendering it inaccessible and preventing FPS customers from accessing their accounts, transaction history, and other essential information if they do not pay the ransom. Some ransomware variants steal sensitive information before encrypting files, which could lead to identity theft and financial fraud.
- **Identity theft:** After stealing the system credentials or other sensitive information of the consumer (such as the ID number or bank account details), the attacker may commit fraud or other crimes. Unauthorized transactions, fraudulent charges, and misuse of personal data can result from identity theft.
- **Application vulnerabilities and misconfigurations:** An attacker could exploit unaddressed vulnerabilities or configuration errors in consumer software such as digital wallets and mobile banking applications to install malware or steal users' credentials.
- **Fraudulent access channels:** Scammers may replace a legitimate QR code with a fraudulent one to route payments to a different destination or lead customers to a malicious website to install malware on the end users' devices or ask customers to enter bank account information or log-in credentials. Similarly, scammers may trick unaware users to download unsanctioned applications (for example, mobile banking apps) from fraudulent websites that could allow the scammer to gain control of end users' devices.



5 MANAGING CYBER RISK IN FAST PAYMENTS

A robust cybersecurity program requires the implementation and operation of a comprehensive set of controls across the organization at the human layer (for example, the roles and responsibilities of the chief information security officer), the process layer (such as identity and access management), and the technological layer (firewalls). Internationally recognized frameworks and standards serve as the cornerstone for crafting effective cyber risk–management strategies, particularly within the financial sector. Please refer to appendix A for examples of such frameworks and guidelines.

Documents such as the IMF's working paper *Cyber Risk, Market Failures, and Financial Stability*[27] also provides good guidelines on managing cyber risks in the financial sector.

Similarly, *Cyber Resilience for Financial Market Infrastructures,*[28] published in 2019 by the Financial Inclusion Global Initiative, presents a methodology developed by the European Central Bank (ECB) to operationalize the CPMI-IOSCO guidance on cyber resilience for FMIs. The ECB developed such a methodology in its Cyber Resilience Oversight Expectations for Financial Market Infrastructures. Although the expectations were designed in the context of the European Union and focused on FMIs, they could be used by FPS participants to enhance their cyber resilience following a phased approach, and by supervisory authorities to assess their maturity against cyber resilience requirements. The methodology outlines cybersecurity expectations in three levels of increasing maturity (evolving, advancing, and innovating) across five risk-management categories (governance, identification, protection, detection, and response and recovery).

FPS operators and PSPs are encouraged to adopt these global frameworks and guidelines as foundational elements, tailoring their cybersecurity initiatives to align with their unique attributes, such as organizational scale, structural complexity, inherent risk factors, and cultural dynamics.

Given limited resources, organizations should adopt a risk-based approach to managing cyber risk. This method involves prioritizing security measures based on the potential impact and likelihood of various threats. By focusing on the most significant risks first, rather than treating all risks equally, organizations can allocate their resources more effectively. To do this, organizations need a clear understanding of their critical information assets and the potential threats to these assets. Assessing the impact and likelihood of each threat helps in identifying which risks could cause the most damage. Based on these assessments, organizations can prioritize their security efforts and resources toward mitigating the highest risks first. Once security controls tailored to the prioritized risks are implemented, it is essential to continuously monitor their effectiveness and regularly review the evolving risk landscape. The risk-based approach to cyber risk management also applies to regulatory authorities tasked with the supervision of cyber risk. This implies the identification of critical, high-priority risks within FMIs, such as payment systems operators and providers, and mitigating those risks first, before moving onto less critical risk areas. In addition, organizations with the highest levels of cyber risk should be assessed and examined first, before those organizations that present a lesser risk to the financial system.

A widely used IT risk–management framework that can be applied directly to the management of cyber risk of payment systems is the 4A framework.[29] The 4A framework represents a bottom-up approach toward risk management

FIGURE 9 4A Risk-Management Model

Source: Westerman & Hunter

that is based on addressing the risks of availability, access, accuracy, and agility.

Availability risk consists of all potential scenarios that pose a risk to the organizations' payment systems and associated processes that are linked to systems and processes becoming unavailable or inaccessible. Availability risk is linked to an organization's business continuity–management processes. As an example, availability risk increases when a payment system operator or PSP uses multiple information systems that are not standardized.

Access risk comes from insufficient or inadequate access controls to an organization's information systems. Access risk can arise from insufficient internal controls. This can include such topics as network segmentation that is not implemented properly or unreliable network services, among other things.

Accuracy risk is directly relevant for the data quality–management processes of payment systems. It includes risk that is associated with the storage, use, and processing of payment-related data and information that might be stored in an organization's information systems. Accuracy risk also increases with the complexity of information systems that are being used by payment system operators and PSPs.

Agility risk can be caused by inflexible processes and systems that are difficult to either merge or separate. Poor project-management practices as well as inadequate or insufficient communication and coordination between an organization's business units and IT units can lead to increased agility risk.

This technical note aims not to replicate existing frameworks but to underscore leading practices that are paramount for managing cyber threats pertinent to the fast payment landscape. Subsequent sections will delineate these practices, emphasizing measures that FPS entities should prioritize to bolster the resilience of the payment system, thwart fraudulent activities, and safeguard the sensitive data integral to fast payment transactions.

5.1 CONSIDERATIONS FOR FPS OPERATORS AND SERVICE PROVIDERS

Risk Management

To manage cyber risks consistently and effectively, FPS operators and PSPs should follow a cybersecurity risk–management framework. This framework should be tailored to the nature, size, complexity, risk profile, and culture of the organization. The goal of the framework is to provide guidance both on how to assess cyber risks in a consistent manner (for example, defining likelihood and impact scales) and on risk treatments (that is, avoid, mitigate, transfer, or accept) based on established risk-tolerance thresholds.

Ideally, the cyber risk–management framework should be integrated with the organization's enterprise risk management and leverage a taxonomy to set a common language across the organization when identifying risks from various sources (for example, internal audits, incident reports, vulnerability assessments, penetration tests).

The *World Bank's Global Payment Systems Survey*[30] (chart VIII.2, page 91) shows that most central banks adopted a cyber risk–management framework that follows a homogeneous structure reflecting industry best practices and international standards. However, one-quarter of respondents still do not have in place a specific framework to manage cyber risks. (Nineteen percent are planning or considering implementing one, and 7 percent do not have a cyber risk–management framework.)

The risk-management life cycle consists of several steps, as depicted in figure 10.

Risk and control assessments should be conducted periodically to assess the effectiveness of existing controls to protect against the identified risks. Please refer to appen-

FIGURE 10 Risk-Management Life Cycle

BOX 4 CHARACTERISTICS OF AN IT RISK-MANAGEMENT FRAMEWORK

According to ISACA,[31] an organization's cyber and IT risk-management framework must be:

- **Comprehensive**—thorough and sufficiently detailed
- **Complete**—executed from beginning to end
- **Auditable**—clear, understandable, verifiable, and validated by an independent third party
- **Justifiable**—based on valid reasoning and commensurate with the size and complexity of the organization
- **Compliant**—aligned with relevant standards and legal requirements
- **Monitored**—reviewed and supervised regularly
- **Enforced**—dependable, consistent, and enforceable
- **Up-to-date**—reflecting the current environment of the organization, including processes, systems, people, and external factors
- **Adequately managed**—given sufficient resources with relevant support from executive and senior management

dix B for more details on control mechanisms and control types. Integrating risk scenarios within the risk-management framework empowers FPS operators and PSPs to foster open dialogue and discourse on potential risks. This proactive engagement not only encourages individuals to act against specific risks but also fortifies the link between overarching business goals and the pertinent cyber risks that could potentially prevent their realization.

As the organization evolves and its processes are refined to meet the evolving needs of FPS consumers, the associated risk scenarios will inevitably shift. It is crucial for FPS operators and PSPs to eschew the creation of overly intricate risk scenarios that may become cumbersome to understand and administer. A more effective approach would be to set up an initial foundational set of generic scenarios. This can serve as a baseline from which more nuanced and comprehensive scenarios can gradually be developed as the intricacies of the risks become more apparent.

Weaknesses or gaps found through risk and control assessments should be documented along with proposed corrective actions. Reporting and monitoring mechanisms should be set up to ensure that cybersecurity risks and supporting key risk indicators are periodically communicated to relevant authorities within the organization (such as the board of directors and senior management).

Third-party risk also needs to be managed. Organizations in the financial sector around the world are using outsourced capabilities, such as cloud computing, to run their business more efficiently and better serve their customers. Cost savings, increased scalability, flexibility, and resilience are among the benefits that make this technology especially appealing to PSPs. However, accountability for managing the cyber risks arising from the relationship with third parties stays with the organization. Hence, keeping a comprehensive understanding of key relationships and managing their associated cybersecurity risks are essential for the secure, dependable, and resilient delivery of services. In this regard, contractual agreements should incorporate security and resilience requirements for third parties.

Continuous Monitoring

Given consumers' expectation of (near) real-time availability of transferred funds, FPS operators and PSPs need to be able to promptly detect and prevent a wide array of cyber threats that may affect the continuous and safe functioning of the payment system process. For this purpose, they should establish systematic monitoring mechanisms to detect anomalous activity promptly and understand its potential impact for an effective response. This implies the implementation of relevant detective controls, the aim of which is to discover cyber risk–related events. Considering the close convergence between traditional forms of fraud and cyber-enabled fraud, some of the more common operational risk–related controls, such as the segregation of duties and the use of the four-eyes principle, may also prove to be effective at detecting payment-related cyber risk events. In addition, event logs originated from various sources across the organization's network should be sent to a centralized security information and event management (SIEM) system, where they can be aggregated and correlated for a better analysis of those suspicious activities. These logs should include security events from critical applications, infrastructure, and network components (for example, firewalls and intrusion-detection and intrusion-prevention systems, or IDS/IPS), as well as rel-

evant users' actions, including authentication and authorization events (such as log-in attempts that fail the second step of multifactor authentication, attempts from unusual or unexpected geographical areas, brute-forcing of account passwords, or reports of unexpected account throttling or lockouts).

Normal behavior and thresholds should be defined, so alerts can be triggered when suspicious activities are detected. The automated analysis of security events should be supplemented by expert analysis of security events to find potential cyberattacks. FPS operators and PSPs should set up clear roles and responsibilities for the personnel responsible for monitoring events, supported by a framework for the consistent analysis, categorization, and response to alerts.

The integration of AI with technical solutions, such as antivirus software, IDS/IPS, and log-aggregation tools, plays a pivotal role in mitigating cyber risks. AI has revolutionized these systems, offering a new echelon of intelligence and security. Organizations now harness AI's predictive capabilities to proactively identify and neutralize anomalous network behavior, fortifying their defenses against sophisticated cyber threats. More information about the use of AI can be found in appendix C.

Regular testing and auditing of detection processes and technologies are imperative. This practice not only strengthens the organization's control mechanisms but also instills confidence in both supervisors and consumers. Moreover, it is advisable to implement segregation of duties to the greatest extent possible. This separation should be between those conducting the tests and audits and those charged with the oversight and execution of the cybersecurity program.

Incident Response

When it comes to responding to a cybersecurity incident, it is critical for FPS operators and PSPs to have a formalized incident-response plan. In the case of a cyber incident, reacting without a plan once the network has been infiltrated or data has been breached will result in confusion and slower overall response times. Effective plans, procedures, and technologies should be set up and maintained to respond to cybersecurity events and to sustain operations throughout a cybersecurity incident, commensurate with the risk to infrastructure and organizational goals.

The incident-response plan should define criteria for categorizing and prioritizing incidents and provide guidelines on the actions to be followed, such as preparation, identification, containment, eradication, recovery, and lessons learned. An effective incident-response plan would allow the organization to maintain a good reputation and establish trust with all relevant entities. This may be especially important for a fast PSP, due to the organization's business model and the need to be able to process payments in (near) real time.

To the extent possible, a specialized and dedicated team for incident response should be set up and its members trained in the roles and responsibilities corresponding to each incident type. The incident-response plan should also address how and when to notify relevant stakeholders (internal and external) and coordinate joint response activities as needed.

The incident-response plan should be tested, including conducting tabletop exercises with realistic scenarios. Sectorwide crisis-simulation exercises, including live-play exercises, enable organizations and supervisory authorities to identify how potential decisions could affect each other's ability to maintain critical services and enhance the response capability of the sector. The incident-response plan should be updated with lessons learned from such exercises.

Regardless of whether the financial sector is categorized as national critical infrastructure, financial sector supervisory authorities and regulators should work regularly with other relevant national stakeholders to maintain and test nationwide incident-response plans. This will be critical to responding to large-scale incidents that could have a national impact. This work should be aligned with any existing national cybersecurity strategies.

Appendix G presents other considerations regarding the preparation of the incident-response plan.

Resilience and Business Continuity

Business-continuity and disaster-recovery plans are essential components of comprehensive cybersecurity strategies. They ensure that critical functions can resume promptly following a cyber incident. As FPS operators and PSPs increasingly depend on IT for their operational needs, it is imperative that the IT disaster-recovery strategies are seamlessly integrated with organizational business-continuity plans. While business-continuity plans outline the steps necessary to reinstate business functions, disaster-recovery plans provide a detailed blueprint for the prompt recovery of IT systems and the safeguarding of data assets, ensuring minimal disruption to services.

Business impact analysis should often be conducted to determine the information assets (including outsourced systems and services) that support critical business processes and establish and adjust the required recovery objectives. NIST offers a commonly used template for carrying out a business impact analysis.[32] Restoration activities should be coordinated with relevant internal and external parties (for example, internet service providers, vendors, local computer emergency response teams).

FPS operators and PSPs should proactively conduct risk assessments to find and evaluate potential risks that could affect their operations. Organizations in the FPS ecosystem should prioritize threats and threat actors outlined previously but also consider hypothetical risk scenarios that, while not previously experienced, could pose future challenges to PSPs. For instance, the absence of past ransomware incidents does not eliminate the possibility of such attacks occurring in the future. Also, consideration should be given to catastrophic but unlikely events, such as the widespread IT outage experienced in July 2024. Appropriate measures should then be implemented to mitigate the identified risks that could impair business continuity. Those risks should be closely monitored, and business-continuity and disaster-recovery plans updated as needed.

Business-continuity and disaster-recovery plans may become obsolete if they are not tested and updated often. These plans should be tested frequently against a variety of realistic scenarios involving relevant internal and external stakeholders. Scenarios such as extended power outages, DDoS, or ransomware attacks should be tested through tabletop and functional exercises to evaluate the effectiveness of the plans and the readiness of the personnel to respond to an incident. Lessons learned from tests and forensic analysis conducted on real events should be incorporated into the plans to improve the organization's ability to respond effectively and promptly to cyber events.

Testing

Testing should be an integral part of the fast payment organizations' cybersecurity framework. Robust testing programs help to find weaknesses in the control environment that provide useful inputs to the organization's cyber risk–management process.

Systematic testing of all relevant components of the FPS must be conducted to ensure that security controls are running as designed and effectively protecting the organization from cyber threats. Testing could include vulnerability assessments, penetration tests, independent audits, or tabletop exercises within the context of business continuity and incident response.

To reduce the risk of security vulnerabilities being exploited by attackers, FPS operators and PSPs should implement a vigorous vulnerability and patch-management process to find, prioritize, and remediate vulnerabilities. Vulnerability scanning should be conducted periodically and when material changes occur in the operating environment, such as the implementation of new systems, including associated components that may include servers, software, or changes in network configuration. Some organizations perform vulnerability scans quarterly, monthly, or even weekly depending on the criticality of the information assets. Vulnerability scans should be done using tools from reputable vendors and software providers. An added aspect to consider is the regular updating of scan profiles and tools such as the plug-ins that may be needed to scan for vulnerabilities associated with

BOX 5 COUNTRY EXAMPLES

Ensuring the continuity of operations is paramount for FPS operators. In Poland, the FPS operator KIR is certified using the highest cybersecurity standards and is compliant with the European Central Bank's Cyber Resilience Oversight Expectations for Financial Market Infrastructures. Based on the results of business impact analysis, KIR's business continuity–management policy sets up specific recovery-time and recovery-point objectives for payment services.

In the Kingdom of Bahrain, the payment infrastructure is considered national critical infrastructure and must meet a 99.99 percent availability requirement set up by the Central Bank of Bahrain. The payment infrastructure is certified according to the ISO 22301 standard for business continuity. Business impact analysis is regularly conducted to find critical processes and systems and set up business-continuity objectives.

Similarly, Banco Central do Brasil established a 15-minute recovery-time objective and a zero-minute recovery-point objective for the national fast payment service Pix, based on the results of business impact analysis.

In all cases, the business-continuity and disaster-recovery plans are frequently tested to ensure compliance with business-continuity standards and the established resilience objectives. In the Kingdom of Bahrain, the tests include simulation exercises to evaluate the cyber resilience of the financial sector. For example, in 2023 the Central Bank of Bahrain organized a cyber wargame that involved key FPS participants.

payment systems. Organizations should consider scanning all network-connected systems and not just web-facing applications, in support of a defense-in-depth strategy.

To reduce the risk of known vulnerabilities that could be exploited, organizations should ensure that the latest versions of operating systems, databases, middleware, and software in other critical devices are running in the enterprise. As part of the patch-management process, vendor-released patches should be tested in a lower environment before being deployed into production and periodically tested afterward.

Penetration testing and threat-led penetration testing are other powerful types of testing that FPS organizations should consider. Penetration testing is a vital tool to test the effectiveness of controls. Penetration testing could be conducted by internal resources or by a reputable independent party.

As standard penetration tests could become generic in nature and therefore offer reduced value to the target organization, some advanced jurisdictions have implemented assessment frameworks to conduct threat-led penetration testing. In this case, a targeted test is conducted by an authorized third party, based on relevant cyber threat intelligence that applies to the financial sector and the organization assessed. The goal of threat-led penetration testing, also known as red team testing, is to test how current threats can affect an organization's critical business functions. For example, if there is a new form of ransomware attack prevalent in the financial sector, the penetration tester defines targeted scenarios using that threat to test the resilience of the FPS organization against that specific threat.

FPS operators and PSPs should regularly conduct independent information systems audits, including cybersecurity audits. The main goal of these audits should be to ensure the safe functioning of the FPS or any other related process that may have an adverse impact on the payment system that is being assessed. At a minimum, the cybersecurity information system audit should address risks stemming from the confidentiality, integrity, and availability of payment-related data and information. From a different perspective, the independent audit needs to address the risks of availability, access, and accuracy of payment systems. The risk of accuracy is related to data quality management.

Vulnerabilities and weaknesses detected through different types of testing should be analyzed and prioritized based on the potential impact of the vulnerability on the exposed asset and the criticality of the asset.

Information Sharing

The interconnectedness of the FPS and financial infrastructure may expose the financial sector to systemic risk. A localized breach in one of the actors could be propagated to others who are connected to it, triggering a widespread disruption across the entire ecosystem. Similarly, a concerted attack across multiple interlinked payment systems or FMIs in a country may propagate and increase in scale, leading to systemic risk.

The exchange of tactical and technical data, including threat intelligence and insights into recent cyberattack methods, equips organizations with the knowledge to find and adapt to evolving attack trends, thereby enhancing their detection and response mechanisms. Information-sharing and analysis centers (ISACs) serve as pivotal hubs for the collection of cyber threat intelligence, often about critical infrastructure. They facilitate a reciprocal flow of information between private entities and public agencies, such as is the case of the European Union Agency for Cybersecurity.[33]

FPS operators and PSPs should participate in national-level information-sharing initiatives and, if possible, also establish complementary sectoral ISACs that focus on threat intelligence that is relevant to the financial sector. Furthermore, FPS operators and PSPs might also benefit from taking part in or creating a database dedicated to operational risk external losses (an external loss database), which regularly updates stakeholders on incidents related to operational risks, including cyber threats. This proactive approach can significantly contribute to a collective defense strategy against cyber vulnerabilities. Please refer to appendix H for more details on the type of information that is typically shared in an ISAC arrangement.

The *World Bank's Global Payment Systems Survey*[34] (Chart VIII.3, page 91) shows that in high-income economies, the rate of participation of the central bank in cyber threat information-sharing mechanisms reaches 86 percent, compared to 61 percent in lower middle-income countries. Only 12 percent of respondents indicated that they have no plans for participating in such arrangements.

Collaboration among private and public entities and authorities allows for a deeper understanding of the vulnerabilities in the fast payments ecosystem and how they could potentially be exploited by an attacker, leading to the disruption of operations. To that extent, public authorities should find and address impediments to information sharing in the financial sector and the payment system.l

Continuous Learning

As cyber criminals' methods become more advanced, so must the industry's best practices and defensive solutions. It is imperative for FPS operators and PSPs to proactively identify and mitigate cyber threats that could disrupt their operations and cause ripple effects throughout the ecosystem.

BOX 6 COUNTRY EXAMPLES

Informed by up-to-date situational awareness of the ever-changing threat landscape, the FPS operator in the Kingdom of Bahrain adjusts its cybersecurity program and risk-management approach as needed to match changes in the threat and control environment, enhance user awareness, and effectively deploy resources. Similarly, to maintain the required situational awareness, the Polish FPS operator participates in information-sharing schemes established for the Polish financial sector.

In Brazil, potential fraud incidents in the Pix fast payment ecosystem are tracked by Banco Central do Brasil, and relevant information is shared with the FPS participants via an information-sharing arrangement. To ensure that all participants are aware of the threats relevant to Pix, Banco Central do Brasil adopted a full-transparency approach and publicly discloses instances when PSPs are affected by a cyberattack.

This includes preparing for low-probability events that could nonetheless have far-reaching consequences.

To stay ahead of potential threats, cybersecurity strategies and frameworks must undergo regular evaluations and revisions, ensuring that they remain effective against the ever-changing landscape of cyber risks. FPS operators and PSPs must establish a robust process for collecting and analyzing cyber threat intelligence from various facets of their ecosystem, as well as from geopolitical shifts that could precipitate cyberattacks on any part of the network.

In building a resilient control environment, FPS operators and PSPs should not depend solely on actionable intelligence from trusted sources; they must also draw lessons from cyber incidents that have occurred both within their own organization and in the broader industry. By doing so, they can continually refine and strengthen their cybersecurity measures.

Awareness and Education

Organizations operating within the fast payment ecosystem must ensure that both their employees and customers receive cybersecurity awareness and education training that is not only prompt but also pertinent to the evolving digital threats.

Employee awareness is just as critical as the technological safeguards and procedural strategies employed by an organization to mitigate cyber risks. Indeed, elevating awareness levels within an organization often serves as the most effective preventive measure. The conduct of employees plays an essential role in ensuring the protection of computer systems and the integrity of information assets. Industry research indicates that actions taken by employees, whether deliberate (such as malicious intent) or accidental, are significant contributors to operational disruptions and security breaches related to computer systems.[35]

Cyber criminals often target uninformed employees or contractors to access an organization's systems. Earlier on, phishing email attacks were massively deployed through spam campaigns, but phishing attacks are now more targeted (for example, "whaling" or phishing attacks targeting the organization's executives). To counter these types of attacks, FPS operators and PSPs should implement cybersecurity awareness and education programs to equip the workforce with the proper knowledge to conduct their duties in a secure way and prevent becoming victims of cyberattacks that could lead to the compromise of the organization's systems. The content of the awareness and education campaigns should be tailored to target distinct types of users, from IT administrators, developers, and administration staff at operation centers to senior management and executives. (See box 8 for further information on this topic.) The effectiveness of the awareness program should be periodically tested.

The security awareness program should be an ongoing initiative that actively engages all employees through a variety of methods. To send the message effectively, the program can use a range of materials, such as tailored memos, email alerts, informative flyers, eye-catching posters, and other pertinent documentation. Incorporating workshops and training sessions is also a vital part of the program, ensuring that staff members receive hands-on experience. It is crucial that the organization's message is both straightforward and easily comprehensible. The more accessible and pertinent the training materials are, the greater the improvement in security practices will be.

Cybersecurity awareness and education programs not only enhance the level of protection against cyberattacks but also help with improving employee behavior, increasing the ability to hold employees accountable for their actions, mitigating the organization's liability for an employee's behavior, and following regulations and contractual obligations.

Several NIST documents in addition to ISO/IEC 27002:2022 discuss security goals based on an employee's role within the organization. The models described start with aware-

BOX 7 ROLE-BASED AWARENESS

Several NIST documents in addition to ISO/IEC 27002:2022 discuss security goals based on an employee's role within the organization. The models described start with awareness, evolve into training, and then lead to education. This is a role-based approach to information and cybersecurity in terms of the information systems[36] that the employees deal with. The model's foundation is security awareness, which all employees of the organization need to develop and then have. This also includes an overall understanding of policies, procedures, and restrictions. The second level of the model has two layers and is required for staff members who will be using information systems (including data) and need more detailed understanding of existing (and potential) cyber risks, control mechanisms, and other relevant information. The last layer is associated with individuals who have specialized roles revolving around information systems, such as system administrators, programmers, and information security managers. (This list is not exhaustive.)

- Based on the NIST SP 800-16 standard, the four layers of the role-based model shown above include the following:
- **Security awareness:** This is needed for all employees of the organization, no matter what their role is. This layer covers foundational information security concepts for employees and contractors involved with the organization's information systems in any way.
- **Security basics and literacy:** This transitional stage lies between awareness and training. It forms the foundation for later training and consists of foundational security terms and concepts that the employees of the organization need to be aware of.
- **Functional roles and responsibilities:** After the security and literacy stage, the training is a more focused endeavor consisting of specific knowledge, skills, and abilities associated with the employees' roles and responsibilities within the organization. This stage incorporates and uses a differentiated approach to beginning, intermediate, and advanced skills requirements.
- **Education and experience:** This final level of the model emphasizes the development of ability and vision to perform specialized tasks and multidisciplinary activities. It covers and addresses the skills that are needed in order to further the cybersecurity profession and also to keep up-to-date with emerging (evolving) threats and technologies.

The security awareness strategy of the organization has the aim of informing and emphasizing topics that are related to cyber risk and cybersecurity within the organization. This stage of the process aims to achieve the following outcomes:

- Staff members become (or are) aware of what their roles and duties are within the organization. They know what they need to protect and how to protect it.
- Employees understand the role of cybersecurity within the organization and act to protect the organization's information assets.
- Because of the constantly changing threat landscape and evolving technology, management becomes aware of and actively supports cybersecurity management.

ness, evolve into training, and then lead to education. This is a role-based approach to information and cybersecurity in terms of the information systems[36] that the employees deal with. The model's foundation is security awareness, which all employees of the organization need to develop and then have. This also includes an overall understanding of policies, procedures, and restrictions. The second level of the model has two layers and is required for staff members who will be using information systems (including data) and need more detailed understanding of existing (and potential) cyber risks, control mechanisms, and other relevant information. The last layer is associated with individuals who have specialized roles revolving around information systems, such as system administrators, programmers, and information security managers. (This list is not exhaustive.)

For organizations in the fast payment ecosystem, it is also imperative to provide prompt and relevant cybersecurity awareness and education training to their customers. This training would help consumers to distinguish between a legitimate request from their PSP and a dangerous attempt through a phishing email to compromise their user credentials or other sensitive information. FPS operators and PSPs

should use all available channels, from the corporate website and mobile applications to social media postings, to educate their customers on how to prevent identity theft, fraud, and scams.

Fraud Risk Management

Fraud is one of the main categories of operational risk that is closely aligned with cyber risk and also directly relevant for FPS. While not all fraud has a cyber dimension, a large portion of payment system fraud is cyber-enabled. There is also a considerable convergence between cyberattacks and fraud, as illustrated in figure 11. The World Bank has developed a separate focus note on fraud risk titled *Fraud Risks in Fast Payments.*[37] This section overviews fraud risk management as a critical part of cybersecurity.

Cyber-enabled fraud may occur in a multitude of forms. A consumer may have his/her information stolen as a result of a cyberattack, after which the attacker or another unauthorized entity may gain access to the consumer's FPS account and start an unauthorized payment. Conversely, an intruder may compromise or break into the PSP's network, plant malware inside the organization, and then initiate unauthorized payments from within the system. In other cases, intruders may start a DDoS attack to function as a diversionary tactic (setting a smokescreen) while trying to penetrate a payment system and steal funds by electronic transfer.

FSP operators and PSPs need to have effective controls to detect and prevent cyber-enabled fraud. This includes, primarily, the development of a fraud risk–prevention policy. The fraud risk–prevention policy should include clear and specific goals, a strategy for achieving the goals, and sufficient detective and preventive controls to mitigate fraud effectively. This may include setting operational limits on transactions, which serves as an effective control that reduces the risk of fraud by enabling the use of the four-eyes principle to review transactions beyond a preestablished monetary threshold. Other effective controls that help in mitigating the risk of fraud include employee trainings and awareness-raising initiatives, in addition to segregation of duties.

In addition, the recent emergence of AI-enabled tools for fraud detection and prevention has offered the ability to automate various tasks associated with fraud prevention. AI and machine learning can enhance an organization's ability to find and then prevent fraud. Various algorithms, such as the k-nearest neighbor or convolutional neural networks, among others, may be used to mitigate the risk of transaction fraud that is inherent to FPS. Both neural networks and more traditional supervised machine learning algorithms can achieve a high level of accuracy in finding fraudulent transactions or other anomalous activity. Figure 12 presents an example of using a machine learning algorithm in the form of a convolutional neural network to determine the accuracy

FIGURE 11 **Convergence between Cyberattacks and Fraud**

Source: Maurer and Nelson 2020[38]

FIGURE 12 **Fraud-Detection Accuracy for a Model Based on a Convolutional Neural Network**

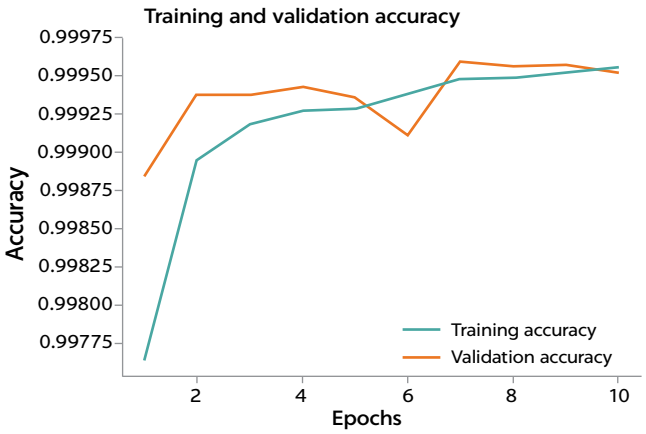
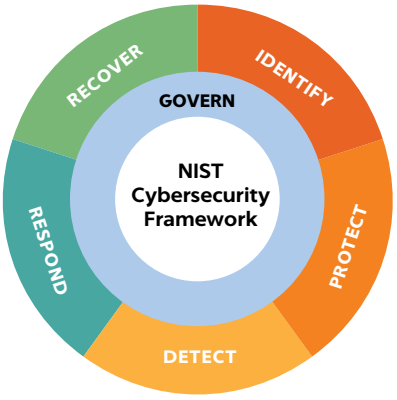


FIGURE 13 **NIST Cybersecurity Framework**



of the fraud-detection model, using 10 individual rounds (epochs) of learning. After the 10 rounds, the prediction accuracy for the training dataset that was used to identify fraud, as well as the data that was used to confirm the results, exceeds 99.9 percent.

Other Considerations

A robust cybersecurity program necessitates the deployment and management of a suite of technical and procedural safeguards. This begins with identifying the critical digital assets that demand protection. Following this, it is essential to implement and manage the necessary controls to safeguard these assets, as well as to detect and address any incidents that could potentially compromise them. While the most pertinent controls have been outlined in the preceding sections of this document, it is also imperative for FPS operators and PSPs to weigh the considerations discussed in the following sections.

- **Cybersecurity Strategy and Framework**
  Organizations that have successfully implemented an effective cybersecurity program typically align it with a cybersecurity strategy and framework that specifies how to identify, manage, and reduce cyber risks, taking into consideration the nature, size, complexity, risk profile, and culture of the organization.

  The strategy should aim at providing cohesion and strategic direction to the organization's cybersecurity activities, organizing them with a purpose under a comprehensive program and helping to align them with the organization's strategic goals.

  Cybersecurity frameworks provide a systematic approach to managing cyber risks, ensuring that measures are comprehensive and well coordinated across the organization. Frameworks such as the NIST Cybersecurity Framework[39] (figure 13) or the National Cyber Security Centre's 10 Steps to Cyber Security[40] (figure 14) provide a good starting point.

While not directly associated with FPS, most of the domains established by the Payment Card Industry Data Security Standard (PCI DSS)[41] could be used by PSPs to secure the network, protect consumers' data, and conduct vulnerability assessments and penetration testing, among other security practices. Please refer to appendix H for more information about PCI DSS.

- **Governance**
  Leading organizations recognize the importance of establishing a governance structure with clear roles and responsibilities, following the segregation-of-duties principle, for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and program.

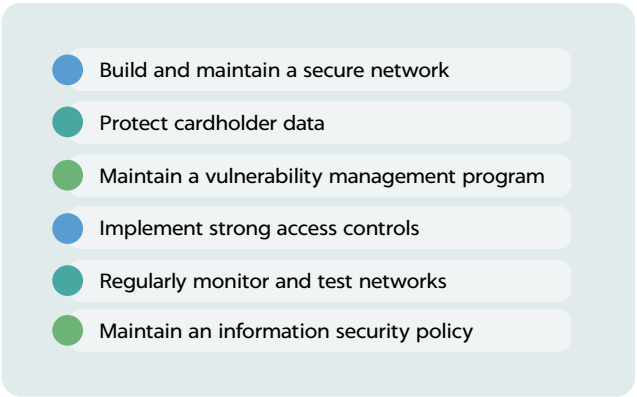
  Mature organizations usually have a qualified individual appointed as chief information security officer who is responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policies. Appropriate lines of reporting should be set up for the chief information security officer to communicate to relevant corporate authority the effectiveness of the cybersecurity program and material cybersecurity risks and events. While smaller organizations may not formally appoint an information security officer, it is important that they make a qualified individual accountable for overseeing the cybersecurity program and provide that person with proper mechanisms to raise cyber risks to the relevant corporate authority periodically.

FIGURE 14 NCSC 10 Steps to Cyber Security

1. **Risk Management**
   - Use a risk-based approach for protecting data and information systems.
2. **Engagement and Training**
   - Engage people within the organization for ensuring security and increasing user awareness.
3. **Asset Management**
   - Identify data and information systems that need to be protected and understand the business needs that they support.
4. **Architecture and Configuration**
   - Design, construct and maintain information systems in a secure manner.
5. **Vulnerability Management**
   - Protect information systems throughout the information system lifecycle.
6. **Identity and Access Management**
   - Control who and what processes can access information systems and corresponding data.
7. **Data Security**
   - Protect data where it needs to be protected.
8. **Logging and Monitoring**
   - Design information systems in such a way that incidents can be detected and investigated accordingly.
9. **Incident Management**
   - Plan incident response to cyber incidents in advance.
10. **Supply Chain Security**
    - Closely work with suppliers and partners.

Source: Adapted from the United Kingdom's National Cyber Security Centre

FIGURE 15 PCI DSS Domains



Source: Williams and Chuvakin 2012[42]

A key part of effective cybersecurity governance is the role of senior management. Senior management in FPS operators and PSPs should set the tone at the top and adopt a top-down approach to dealing with cyber risk. Senior management should have adequate understanding of the cybersecurity risks relevant to the organization, set up the cyber risk–tolerance thresholds, and oversee the design, implementation, and effectiveness of related cybersecurity programs.

The governance structure must be underpinned by cybersecurity policies, standards, and guidelines that should be documented, approved, published, regularly reviewed, and communicated to all relevant stakeholders.

- **Asset Management**

To manage cybersecurity risks effectively, organizations need to identify and prioritize the critical information assets that must be protected from the most relevant threat actors. Without a comprehensive understanding of the information assets (data, physical devices, information systems, software, facilities) that enable the organization to achieve business purposes, it would not be possible to prioritize activities effectively and allocate resources efficiently to address cyber risks. Processes, procedures, and technologies should be established for managing the organization's information assets throughout all stages of their life cycle.

Creating and keeping an asset-management plan is critical from the perspective of cyber risk management. The process can be used to define and find what the

mission-critical assets are that specifically relate to the payment systems. To manage information assets, they must be identified and determined. FPS operators and service providers need to identify the information assets before they can be protected effectively. For example, an information asset may be transaction-related information, in addition to personally identifiable information associated with consumers. Within the context of payment systems, the organizational assets associated with payment systems must be formally identified, prioritized, documented, and inventoried.

- **Identity and Access Management**
  FPS operators and PSPs should develop a comprehensive process for identity and access management. Access to critical information assets must be limited only to the necessary individuals at the necessary times based on business needs. Effective identity and access management is key to managing the risk of unauthorized access to an organization's information assets and to maintaining the confidentiality and integrity of information assets. Appropriate processes, procedures, and technologies should be established to manage the entire life cycle of digital identities and profiles for entities that may be granted logical or physical access to the organization's information assets.

  One of the first steps is to develop a set of goals as to which identities, roles, and users may need access to payment-related data or any other sensitive information that may be linked to the provision of payment services. Deciding who needs access to which resources may be just as important as determining who should not have access to payment systems–related data. For example, access should be granted based upon the specific role or job classification and function. In addition, access requirements for each role should clearly stem from the perspective of payment systems and the relevant components, such as the data resources, that each role may need. The level of privilege within the system should also be defined, which means that regular system users, consumers, and administrators are based on the specific role.

  Another important dimension of identity and access management is deploying multifactor authentication for all accounts being used within the FPS. Payment service operators and service providers should take a risk-based approach when deploying multifactor authentication. User-to-service, user-to-device, and device-to-service authentication methods should be considered in this respect. Furthermore, when it comes to online and web-based services, multifactor authentication should be used. From this perspective, consumers of FPS may potentially be offered a choice of factors to authenticate into the system. The choice of factors may include biometrics, email notifications, or SMS messages. In situations where passwords need to be used, payment service operators and service providers should employ the kind of password policy that considers both usability and password security. Please refer to the focus note *Customer Authentication 2.0: Approaches and Challenges in Fast Payments*[43] for more information.

  Organizations providing payment services may consider the use of password managers and single sign-on methods when reducing the number and complexity of passwords. User credentials should be protected both during transit and at rest.

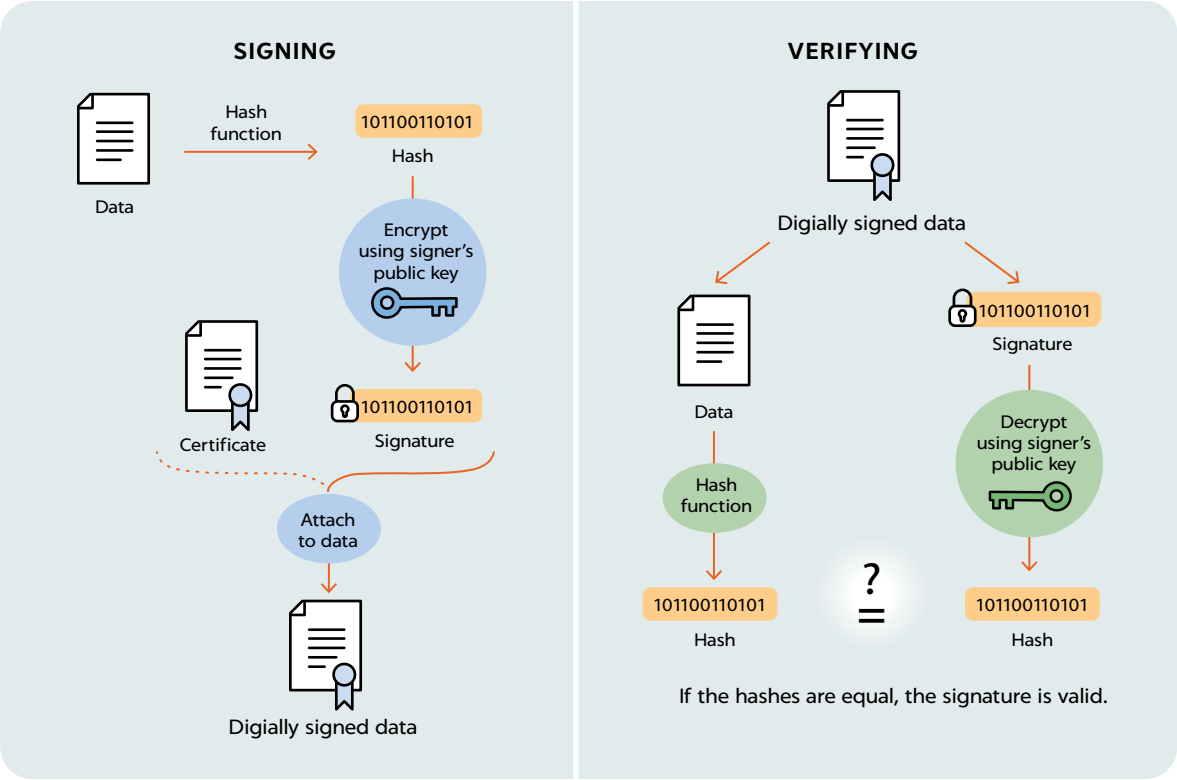
- **Encryption**
  To adequately safeguard the integrity and confidentiality of payment transactions and associated data, information should be consistently encrypted at rest and in transit.

  Encryption protects against passive attacks such as eavesdropping, the aim of which is to gain access to or get a hold of confidential data. A different requirement is to protect against active attacks, which can lead to the falsification or unauthorized alteration of financial transactions and other relevant information. While the confidentiality of payment-related data may typically be secured using symmetric encryption algorithms, the integrity of data is provided using asymmetric encryption. The integrity of payment-related data is of particular concern, since the unauthorized modification of payment information can undermine trust in the fast payment ecosystem, which can also result in systemic operational risk. A payment message, file, or document is said to be authentic if it is genuine and came from the actual source, such as a legitimate payment initiator (that is, the payer).

  Digital signatures are a common method for protecting the integrity of payment-related data. (See figure 16.) For example, when consumers send payment orders via an FPS, the payment orders are digitally signed using the private key that is generated by an asymmetric encryption algorithm. The receiver of a payment transaction can then verify the authenticity of the payment transaction using the public key that has been generated based on the same asymmetric encryption algorithm.

- **Secure Access Channel**
  A breach in the security of access channels used in the FPS ecosystem (for example, QR codes) could lead to fraud, identity theft, or the compromise of data confidentiality. Securing QR codes is a topic of high relevance,

FIGURE 16 Digital Signature Process



Source: DocuSign[44]

as adoption of QR codes has been widespread in recent years, including as part of FPS implementations, owing to the multifold benefits that QR codes provide to both merchants and customers.

As outlined in the World Bank's focus note *The Use of Quick-Response Codes in Payments,*[45] security aspects related to QR codes, including fraud committed by replicating the QR code, identity impersonation, and data protection, need to be carefully assessed. In their efforts to ensure the security of QR codes, PSPs should consider EMVCo specifications[46] that provide a standardized template for the generation of QR codes that will work consistently everywhere to deliver convenient and reliable card- and account-based payments.

Also, PSPs should consider ISO 5201:2024,[47] an international standard on financial services for code-scanning payment security. The standard covers security issues related to code-scanning technologies used for payments and includes an overview, a risk assessment, and minimum-security requirements and extended security guidelines for code-scanning payment, where the payer uses a device to operate the payment transaction. The standard is applicable to cases where the code is both used to initiate a payment transaction and presented by the payer or the payee.

- **Data Privacy**

  High-profile data breaches and privacy regulations around the world emphasize the importance of data privacy. Even though the direct costs associated with these data breaches are already high, most of the time these account only for the known costs (for example, technical investigation and improvements, customer breach notification, and post-breach protection) but fail to consider other less visible costs (such as reputational damage and loss of customer confidence, increased cost to raise capital, increases in insurance premium, and disruption of operations). Privacy regulations in Europe and Asia are further tightening the compliance requirements and will be followed by similar strict requirements in other geographical regions, making it even clearer to organizations processing personal data that protecting the privacy of their personnel and customers is a business requirement.

  A data privacy policy is the first step toward addressing the increased pressure on protecting the privacy of personal data. A data privacy policy should be documented, approved, published, regularly reviewed, and communi-

cated to all relevant stakeholders, setting direction in line with business goals and showing support for data privacy across the organization. The policy should define what personal data is, provide guidance on security controls for protecting the privacy of personal data, and set up roles and responsibilities for protecting the privacy of personal data (for example, data owner, data custodian). The policy must consider legal, regulatory, and contractual data privacy requirements.

Organizations in the FPS ecosystem should deploy technical controls, such as strong authentication and access logging, data masking and encryption, data loss prevention, and integrity-protection mechanisms, to ensure that access to personal data is restricted based on relevant business goals. Similarly, process controls such as periodic impact assessments and breach notification readiness can help reduce potential exposure to this risk.

Beyond the specific requirements established by regulations applicable to its jurisdiction (for example, the European Union's General Data Protection Regulation), organizations in the FPS ecosystem can leverage international standards such as ISO/IEC 27701:2019 to develop their privacy information–management system.

- **Compliance**

  An inability to comply with applicable regulations is a top concern for organizations working in a highly regulated environment such as payment systems. Although multiple different laws and regulations around the world cover payment systems and associated processes, of particular importance is the European Union's Digital Operational Resilience Act, which applies to a wide range of financial institutions, including such FMIs as payment system operators, electronic payment arrangement operators, payment processors, and the associated technological service providers. At the same time, there are some exceptions for small and medium-sized organizations, although the act specifically covers payment institutions. It will go into force in early 2025. There are five foundational pillars within the legislation: management of information and communication technology (ICT) risk, incident management, classification and reporting, operational resilience testing, management and oversight of third-party risk, and information sharing. Figure 17 lists the five pillars of the act. Articles 5–16 relate to ICT risk management; articles 17–23 cover incident management, event classification, and reporting; articles 24–27 address incident management; articles 28–44 relate to the management of third-party risks; and article 45 encompasses information sharing.

  Compliance does not equal security, but there are synergies that should be maximized. The design, operation, use, and management of information systems in the fast payment ecosystem are typically subject to legal, regulatory, and contractual information security requirements.

  So PSPs should have a compliance program in place to avoid breaches of any applicable law, regulations, contractual obligations, or requirements set up in the security policies. To the extent possible, compliance and cybersecurity efforts should be aligned to minimize duplicative efforts (for example, control testing, risk assessments, risk reporting) and help a risk-based allocation of resources to address risks relevant to the organization.

  Compliance with data privacy regulations is a key requirement for PSPs as well, as they manage customers' personal data based on the nature of the business. So they should ensure compliance with data privacy requirements in alignment with relevant legislation, regulations, and contractual agreements. To achieve compliance, organizations should obtain a comprehensive understanding of the data collected and the security controls implemented to meet those privacy requirements.

- **Secure Design Principles**

  When discussing internal controls and protection mechanisms, there are no foolproof techniques. Therefore, it is critical to develop relevant protection mechanisms that are based on different controls that the organiza-

FIGURE 17 **The Five Pillars of the Digital Operational Resilience Act**

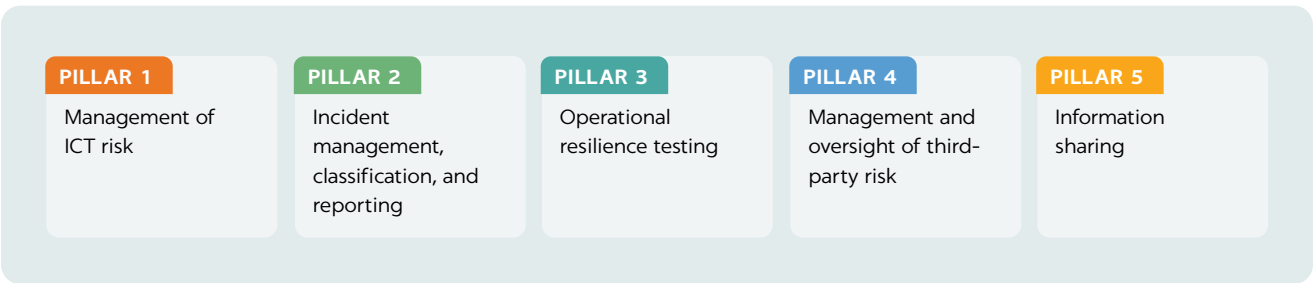
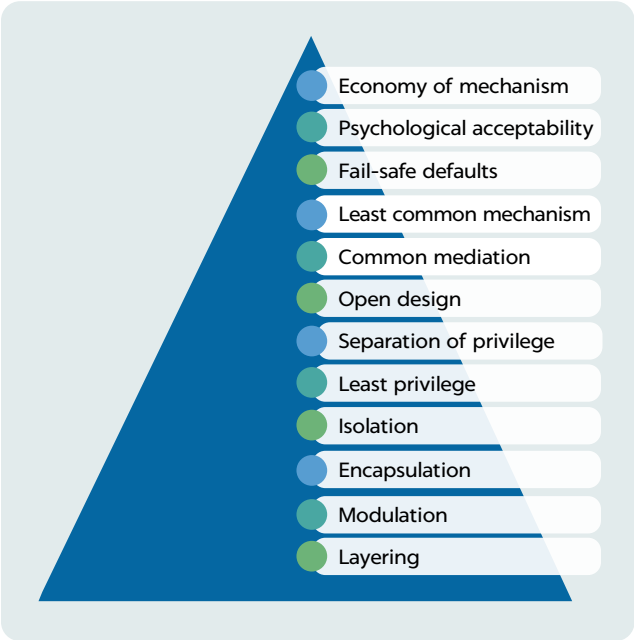


FIGURE 18 Fundamental Secure Design Principles



tion may implement to secure its information systems. This includes payment systems. The U.S. National Centers of Academic Excellence in Cybersecurity list 12 baseline security principles that should be followed for developing relevant protection mechanisms.[48] These mechanisms are depicted in figure 18. Appendix D provides an expanded description of these principles.

5.2 CONSIDERATIONS FOR REGULATORS

The safe and continuous operation of payment systems and other FMIs is essential to the stability of the financial system and the global economy. Cyber incidents disrupting the ICT that supports these activities can have systemic consequences. Naturally, cyber resilience continues to be a top priority for the financial services industry and a key area of attention for payment system supervisors. Payment system supervisors in most jurisdictions have developed regulatory frameworks to deal with cyber risk.

A suitable regulatory framework for the operation of payment systems promotes the adoption of leading cybersecurity practices that enhance operational resilience, transparency, and cooperation. The absence of such a regulatory framework may expose the FPS ecosystem to significant cyber risks, with PSPs working in isolation and without proper guidance on how to secure the critical components of the payment system.

Regulators in jurisdictions with a certain level of cyber resilience maturity typically leverage existing related regulations on cybersecurity or operational risk and provide a principle-based regulatory framework that provides the payment system operators and participants with high-level expectations on how to achieve cyber resilience. In other jurisdictions, regulators opt for a more prescriptive approach, with detailed requirements that the FPS operators and PSPs must meet to be allowed to take part in the FPS ecosystem. The former approach offers flexibility on how the payment system providers can achieve the cyber resilience goals, and the latter incorporates tailored guidance with clear and specific requirements.

To offset the danger of having too much rigidity in the regulation, which may hamper innovation or set an undesired compliance mindset in the sector, some regulations combine broad cyber resilience principles with a set of baseline requirements for PSPs.

A trend has been seen in recent years where regulations take an "assume breach" mentality and focus on providing financial institutions and authorities with specific tools to improve cyber resilience. Requirements on cyber incident reporting, threat intelligence sharing, and cyber resilience testing are typically covered in these regulations. Requirements to effectively manage cyber risks arising from dependencies and connections with third-party service providers are also common.

Several regulatory frameworks have been successfully implemented around the world. Some jurisdictions continue to enhance their frameworks to address the ever-changing threat landscape. For example, the European Union set up the Digital Operational Resilience Act, which aims to strengthen the IT security of financial entities in Europe and ensure that the European financial sector is able to stay resilient in the event of a severe operational disruption. However, as there is no "one size fits all" approach, the legal framework must be tailored to the characteristics of the financial sector in each jurisdiction to ensure that it can be enforced.

The cost of implementing and maintaining a comprehensive cybersecurity program is normally high, and the quantification of the investment varies significantly from jurisdiction to jurisdiction. Implementing a cybersecurity program that meets the regulators' requirements could be daunting for FPS operators and participants in many jurisdictions, especially in low- and middle-income economies where advanced cybersecurity products and services and a skilled cybersecurity workforce may be in short supply. This may lead to a suboptimal control environment that drifts away from requirements over time, exposing the FPS participant to higher cyber risks.

It is also important to consider the separation of functions such as payments oversight, supervision and operations. While, on the one hand, the FPS operator, such as a central bank, may also be the supervisor of PSPs, it is important to separate the functions into different structural units within the organization. In addition, the operation of a payment system requires the implementation of relevant internal control mechanisms, such as those that are preventive, detective, or corrective in nature. Supervision of payment services, on the other hand, will likely include the evaluation of the control mechanisms in question.

However, establishing the legal framework is not the only tool that regulators can use toward the goal of strengthening cyber resilience in the FPS ecosystem. Supervisors can also play a pivotal role in helping FPS participants achieve the cybersecurity and resilience objectives through the following key initiatives, which go beyond establishing cybersecurity requirements and technical guidance (Legal Framework for Cybersecurity in the Financial Sector: A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity, 2022):

- **Offering financial incentives:** Regulators can introduce incentives such as tax breaks, grants, or subsidies to encourage financial institutions to invest in cybersecurity measures. These incentives can make it financially viable for PSPs, especially smaller ones, to implement robust security systems. Additionally, offering low-interest loans specifically for cybersecurity projects can be an effective way to ensure that financial institutions have the necessary resources to enhance their defenses.
- **Facilitating multistakeholder partnerships:** Regulators can facilitate the coalition of actors from various communities to increase cooperation and support innovation. Multistakeholder partnerships can occur at operational levels, such as computer emergency response teams, which provide rapid response and coordination in the event of a cyber incident. At the strategic level, these partnerships can involve cross-sector collaborations to develop comprehensive strategies and frameworks for cybersecurity, fostering a unified approach.
- **Creating procurement frameworks:** Developing standardized procurement frameworks can help financial institutions streamline the process of acquiring cybersecurity solutions. These frameworks can include templates for requests for proposals, evaluation criteria, and contract templates. Regulators can also provide detailed guidelines on the types of cybersecurity products and services that financial institutions should buy. This includes specifying standards and certifications that products must meet to be considered secure.
- **Facilitating access to trusted vendors:** Regulators can maintain a list of vetted and trusted cybersecurity vendors. This can help financial institutions make informed decisions and reduce the risk of procuring substandard products.
- **Facilitating information sharing:** By creating platforms for sharing information, such as ISACs, regulators can help institutions stay informed about the latest cyber threats and best practices. Regular updates and alerts can empower FPS participants to address vulnerabilities proactively. Encouraging open communication and collaboration among financial institutions, technology providers, and government agencies can lead to a more resilient cybersecurity environment.
- **Mandating cybersecurity investments:** Regulators can require FPS participants to allocate a specific percentage of their budget to cybersecurity. This ensures that institutions dedicate adequate resources to protecting against evolving cyber threats. Such mandates can be tailored to the size and risk profile of the institution, ensuring that the investment is proportional and effective.
- **Supporting training and education:** Providing resources for cybersecurity training and education programs helps FPS participants build a knowledgeable workforce capable of managing cyber risks. Regulators can develop and offer certification programs, workshops, and continuous learning opportunities. Ensuring that employees at all levels are aware of cybersecurity best practices and emerging threats is crucial for maintaining a secure environment.
- **Encouraging collaboration:** Promoting collaboration between financial institutions, government agencies, and cybersecurity experts can lead to more effective security strategies. Joint initiatives, such as threat intelligence sharing and joint exercises, can help institutions prepare for and respond to cyber incidents. Encouraging a collaborative approach can foster innovation and improve overall cybersecurity resilience.
- **Implementing liability regimes:** Liability regimes can enable stakeholders to claim compensation in case of defects or incidents, holding FPS participants accountable for their cybersecurity practices. This can incentivize institutions to adopt stringent security measures to avoid potential liabilities. By defining clear policies and procedures for liability, regulators can ensure that FPS participants prioritize cybersecurity to protect their customers and stakeholders.
- **Conducting audits and assessments:** Regular audits and assessments can help identify vulnerabilities and

ensure that FPS participants comply with cybersecurity standards. Regulators can establish audit frameworks and guidelines that financial institutions must follow. These assessments can provide valuable insights into the effectiveness of current security measures and highlight areas for improvement.

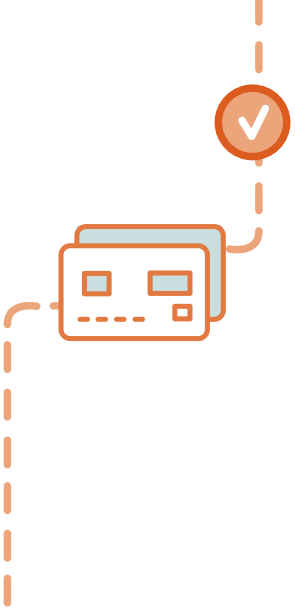
Supervisory authorities must find ways to ensure that PSPs adhere to the regulations and effectively meet cybersecurity and resilience requirements. This is a significant challenge for most supervisory authorities working with resource constraints in an FPS ecosystem with many participants. To address this issue of limited resources, supervisors should consider implementing a risk-based approach for cyber risk supervision following the proportionality principle, by which the resources are efficiently allocated to address the areas of greater risk. This is fundamentally different from a compliance-driven approach, where the supervisor is expected to check that all the supervised entities meet the regulatory requirements.

In addressing the systemic risk, supervisory authorities should also consider other factors that could expose the FPS infrastructure to cyber risks, including dependencies with other industry sectors, such as IT, power or telecommunications, that could affect the availability of operations (figure 4). Supervisory jurisdiction authorities should map critical economic functions in their financial systems as part of their risk and control assessments to find single points of failure and concentration risk.

5.3 CONSIDERATIONS FOR END USERS

Users of fast payment services must also follow good cybersecurity practices, usually referred to as cyber hygiene, to protect themselves from cyberattacks. Among other things, consumers should follow the following good practices:

- **Use strong authentication:** Consumers should avoid using easily guessable information, such as birthdays, or often-used words, and they should forgo reusing passwords for multiple applications or services. Passwords should be changed often, without weakening the strength of the password. For an extra layer of security, consumers should enable two-factor authentication. The focus note *Customer Authentication 2.0: Approaches and Challenges in Fast Payments*[49] provides more details on this topic.
- **Avoid using public Wi-Fi:** When it is impossible to use only secure networks, consumers should use a virtual private network to keep their credentials and financial data safe.
- **Update antivirus software regularly:** To protect against malware and other similar cyber threats, consumers should install and periodically update antivirus software on all of their devices.
- **Monitor transactions closely:** Transactions should be reviewed regularly to detect potential unauthorized activity. Any suspicious activity should be promptly reported to the PSP and corresponding authorities.
- **Beware of phishing scams:** Phishing scams use deceptive emails, texts, or websites to obtain sensitive information. Consumers should be extremely cautious of unsolicited messages and avoid clicking on suspicious links.
- **Keep software and hardware updated:** Consumers should rely only on trusted digital wallet providers and keep the digital wallet application up-to-date to minimize security risks.
- **Back up the digital wallet properly:** Secure backups of the digital wallet data should be created, and recovery phrases or keys should be stored in a safe place, separate from the digital devices.
- **Increase awareness:** Consumers should familiarize themselves with the fast payment arrangement that they are using, understanding its stakeholders, ecosystem, and how it is set up. They should keep abreast of existing and new cyber threats to avoid becoming a victim of cyber criminals.



6 COUNTRY EXAMPLES

6.1 BRAZIL

Within the Brazilian fast payment ecosystem, Banco Central do Brasil (BCB) created Pix, a fast payment scheme that enables its users—people, companies, and governmental entities—to send or receive payment transfers in a few seconds at any time, including on non-business days.

BCB is the scheme owner of Pix. As such, BCB handles the Pix rulebook and is responsible for the supervision of Pix (that is, guaranteeing that participants follow the Pix rulebook). BCB handles the management and operation of the Pix operational platforms, whose messages flow through the National Financial System Network (RSFN), which consists of the following platforms:

- Transaction Accounts Identifier Directory (DICT): A database that links aliases and users' account information and stores and shares antifraud information
- Instant Payments System (SPI): An RTGS infrastructure that settles transactions between different institutions in a few seconds

The criteria for taking part in Pix are broad and flexible, focused on the scheme's safety and efficiency, to foster competition within the ecosystem. In this sense, participation in Pix is open for all financial and payment institutions licensed by the BCB that offer transaction accounts.

Cyber risk is a top priority for the BCB. To manage the risk, BCB has in place a cybersecurity program and technical control environment to protect the confidentiality, integrity, and availability of the DICT and SPI platforms.

It is worth mentioning that Pix is not categorized as critical infrastructure in Brazil.

For BCB, the most important aspects of cyber risk are preventing fraud, protecting the confidentiality of sensitive information, and ensuring cyber resilience. To do so, BCB's cyber program aims at preventing cyberattacks, effectively responding to cyberattacks when they occur, and resuming operations in a prompt and secure fashion as per business-continuity requirements.

Among other technical controls to prevent fraud, BCB tracks transactions and provides near real-time information that PSPs use to decide if the requested transaction can be approved or if it looks fraudulent. Currently, BCB is not using AI capabilities to help with the detection of fraudulent transactions, nor does it use AI and machine learning algorithms for anomaly detection associated with cybersecurity, although the bank might consider using the technology in the future.

To protect the confidentiality of the transaction, data is encrypted while in motion through the fully redundant private links between PSPs and the Pix operational platforms.

Regarding business continuity, BCB has set up a 15-minute recovery-time objective and a zero-minute recovery-point objective.

The Pix operational platforms and communication channels are monitored 24/7 by the BCB security operations center.

Fraud incidents in the Pix ecosystem are tracked by BCB, and relevant information is shared with its participants via an information-sharing arrangement.

As the regulator of the financial sector, BCB has set up a principle-based regulatory framework for cybersecurity. BCB has also published specific cybersecurity requirements for Pix to ensure that the PSPs run their solutions in a secure fashion.

Among other requirements, encryption and mutual authentication must be set up in the communication between the participants and the Pix application programming interfaces, and the messages transmitted within the system must be digitally signed. Security requirements for payment initiation are also set up in the regulation. In addition, PSPs must keep audit logs to provide traceability of messages and transactions conducted in Pix.

The BCB allows PSPs to use different technologies in support of innovative solutions, as far as they meet the Pix cybersecurity requirements. The BCB periodically reviews these requirements to address changes in technology and the cyber threat landscape.

The PSPs self-attest compliance with the cybersecurity requirements. In the few cases of successful cyber incidents affecting the Pix ecosystem, BCB found that they were related to PSPs' failure to comply with the cybersecurity requirements.

The BCB prioritizes transparency when it comes to operational incidents. BCB adopted a full-transparency approach to reputational risk. As a result, the BCB publicly discloses instances in which PSPs are affected by a cyberattack.

6.2 POLAND

Poland is one of the early adopters of FPS. The country implemented the Express Elixir System in 2012. Express Elixir is owned and run by Krajowa Izba Rozliczeniowa S.A. (KIR), a key technology and infrastructure institution that provides clearing and settlement services for the financial system. The owners of KIR are the National Bank of Poland, the Polish Bank Association, and the biggest commercial banks.

KIR published certain conditions (requirements) that the participating entities must meet before being allowed access to the system. These conditions include minimal technical specifications and IT requirements to be adhered to by the participants. Only banks can take part in Express Elixir, as they have settlement accounts with the National Bank of Poland. However, the system enables instant person-to-person mobile transfers via overlay services such as BLIK, where mobile phone numbers can be used as aliases. The BLIK mobile payment service was launched in February 2015 by Polski Standard Płatności, which was set up by six commercial banks.

Express Elixir was developed as a stand-alone payment system. In light of the importance of FPS, risk management forms a vital part of Express Elixir's operations. KIR is certified using the highest cybersecurity standards and also complies with the European Central Bank's Cyber Resilience Oversight Expectations for Financial Market Infrastructures. From a risk-management perspective, KIR adheres to the Principles for Financial Market Infrastructures introduced by the BIS.

According to KIR, contemporary cyber risks potentially affecting FPS include the risks of service disruption due to DDoS attacks, phishing campaigns, malware, and ransomware attacks. The Business Continuity Management Policy sets up specific recovery-time and recovery-point objectives for critical services.

From the perspective of risk mitigation, KIR has implemented various tools to deal with different cyber risk scenarios. These include an array of preventive, detective, and corrective controls, such as business-continuity management, incident handling and response, and participation in information-sharing mechanisms related to the financial sector. There is also considerable emphasis on the security of payments, which implies the use of relevant cryptographic mechanisms. The organization conducts regular audits of information systems to achieve compliance with corresponding standards.

6.3 BAHRAIN

Fawri+ is a near real-time electronic fund transfer service introduced under the near real-time Electronic Funds Transfer System (EFTS) in the Kingdom of Bahrain. EFTS, the FPS, interconnects with all retail banks in Bahrain and also offers a deferred net settlement fund transfer service (Fawri) and an electronic bill presentment and payment service (Fawateer).

Through Fawri+, a customer of a participating bank can make account-to-account fund transfers in Bahrain dinar (up to BD 1,000 per account per day) to a customer of the same or another participating bank within 30 seconds and is available 24/7 365 days a year. The request-to-pay transactions can be started through BenefitPay, the national e-wallet.

EFTS, including Fawri+, is run by the BENEFIT Company with the authorization of the Central Bank of Bahrain (CBB). BENEFIT was set up in November 1997 and is currently owned by 11 commercial banks; BENEFIT also runs the national ATM and the point-of-sale switch.

The EFTS directive from CBB provides the regulatory requirements, including the eligibility criteria for licensed banks and non-bank PSPs to take part in the EFTS, while the CBB Rulebook provides the overall regulatory require-

ments, conditions and process of licensing, and regulation and supervision of licensees that provide regulated financial services in the kingdom. Currently, 28 financial institutions are taking part in the FPS.

In 2021, CBB introduced cybersecurity requirements within the CBB Rulebook mandating compliance across the financial sector. This rulebook is aligned with the NIST Cybersecurity Framework and customized to meet the specific needs of Bahrain's financial sector. The CBB Rulebook and directives provide the needed flexibility for EFTS participants to adopt innovative technologies. CBB continuously monitors the environment to decide if other directives, regulation, or clarification are required for innovative technologies used in the FPS.

The CBB Rulebook requires all licensed financial institutions, including those that are taking part in the FPS, to have a formal cybersecurity function with clearly established roles and responsibilities. CBB also requires licensed financial institutions to have comprehensive information-security policies, standards, practices, measures, and controls to ensure the confidentiality, integrity, and availability of data and information systems involved in the fast payment service.

BENEFIT has implemented a robust cybersecurity program with a proactive approach to managing cyber risks such as ransomware, data breaches, fraud, and service disruption due to DDoS and other types of cyberattacks.

The cybersecurity program is anchored by a proper governance structure, in which cyber risks are periodically reported to the board and the CEO through relevant risk committees. There is special emphasis on continuous improvement of the cybersecurity posture and security governance. This includes addressing human aspects of cybersecurity as well as third-party and supply-chain risks. Identity and access management is an added dimension of the overall cybersecurity strategy.

To manage cyber risks, BENEFIT keeps a variety of technical and procedural controls. These include deterrent, detective, and preventive controls on the organizational, human, physical, and technological levels{~?~EDITS OK?} to respond to cyber events and recover in case of an incident.

Informed by up-to-date situational awareness of the ever-changing threat landscape, the cybersecurity program and risk-management approach are adjusted as needed to match changes in the threat and control environment, enhance user awareness, and deploy effective resources.

The EFTS infrastructure is periodically scanned for vulnerabilities that are prioritized and patched accordingly. Security controls and processes are regularly audited, and penetration testing is conducted as well.

BENEFIT pays special attention to reducing the attack surface by limiting connections to the EFTS system only to private links. BENEFIT runs the public key infrastructure used for digital signature and encryption of data processed through the FPS. The public key infrastructure is one of the main components for ensuring the confidentiality and integrity of data, including financial transactions that are processed by the system.

In general, humans can be a weak link in the line of defense against cyberattacks if not managed, so BENEFIT places significant emphasis on raising cybersecurity awareness, not only for its employees and third-party providers but also for consumers of the fast payment services.

EFTS is considered critical national infrastructure and must meet a 99.99 percent availability requirement set up by CBB. The IT disaster-recovery and business-continuity plans are tested periodically and updated with lessons learned from those tests. Business-continuity tests are conducted annually. In 2023, CBB organized a sectorwide cyber wargame exercise to evaluate the cyber resilience of the financial sector. This exercise involved the participation of CBB, BENEFIT, and five systemically important banks in Bahrain. The primary focus was on assessing the potential impact of cyberattacks on EFTS, including fast payments. The simulation specifically targeted an attack on the EFTS system to gauge response and mitigation strategies.

EFTS is certified according to the ISO 22301 standard for business continuity. Business impact analysis is conducted regularly to find critical processes and systems and set up business-continuity objectives. BENEFIT has implemented prevention capabilities as well as high-availability infrastructure, with the goal of achieving zero downtime in case of a cyberattack.

As BENEFIT leverages services from third parties, relevant business-continuity requirements are set up in the contract with these service providers and periodically tested through tabletop exercises.

Significant emphasis is placed on the verification of user identity at the time of registration and onboarding of users to the access channel (BenefitPay) also managed by BENEFIT. BENEFIT shares relevant information with FPS participants to enable the detection of potential fraudulent transactions. There is ongoing cooperation among BENEFIT, CBB, and other relevant national agencies to combat fraud in the payment system, with a focus on raising cyber awareness among the users of the system.

AI is incorporated in the identity-verification process of BenefitPay, as well as in analyzing network events for any active threats.

From their experience implementing Fawri+, BENEFIT's cybersecurity team recommends that adopters of FPS implement a cybersecurity program from the beginning. This will enable the development and adoption of a clear set of goals for the implementation of a functional cybersecurity strategy.

6.4 MEXICO

The Central Bank of Mexico (Banco de México) has developed and implemented a cyber risk–management framework for the management and supervision of cyber risk. Banco de México has dedicated units within the organization for both the management of internal cyber risk and the supervision of cyber risk of financial institutions, including FMIs. Cybersecurity has been a relevant topic for Banco de México since it began to extend the use of information technologies in its processes. Banco de México safeguards cybersecurity, including the confidentiality, integrity, and availability of its information, with a holistic approach that encompasses personnel, processes, and technology, based on international standards and principles. Likewise, these standards and principles are reflected in the regulations issued by Banco de México to supervised entities and in the recommendations it makes to financial system participants. The Cybersecurity Directorate of the central bank is responsible for defining and implementing Banco de México's cybersecurity strategy, through relevant processes and people.

Banco de México supports the automation of financial services, which provide the public with accessibility, mobility, and lower costs, always closely ensuring that the development of these services is secure and that the information and resources of clients are protected.

Within the context of the financial system, Banco de México's cybersecurity strategy includes the following objectives:

- Issue and update the cyber risk framework of Bank of Mexico, so that it incorporates the best practices of cybersecurity and cyber resilience, based on international standards and principles
- Strengthen compliance with cybersecurity requirements
- Monitor compliance with cybersecurity regulations and requirements of supervised financial institutions and sanction any noncompliance that is detected
- Promote collaboration and cooperation with authorities
- Promote, within the scope of the powers of Banco de México, coordination between authorities of the financial system and national security for the prevention and response to incidents, as well as for the prosecution of crimes
- Strengthen cyber resilience within the financial sector
- Perform periodic exercises to measure the cybersecurity and cyber resilience capabilities of the institutions that make up the financial system, in coordination with other authorities and organizations
- Manage incidents in the financial sector
- Strengthen collaboration between institutions and authorities to respond promptly to cybersecurity incidents that occur in the financial system

Within the context of payment systems, Banco de México operates SPEI, a large-value RTGS fund transfer system. SPEI was launched in the second half of 2004. Multiple different participants use SPEI, including banks, pension fund management firms (*Afores*), brokerage firms, foreign exchange firms, insurance companies, non-bank financial entities (*Sofoles*), and investment firms.[50] To ensure the security of transactions, a number of controls have been implemented. These include data encryption, two-factor authentication, and continuous monitoring to detect anomalous or suspicious transaction-related activity, among others.[51] Furthermore, SPEI is regulated by Banco de México, which sets the rules and requirements for the operation of the payment system. The process covers the supervision of the financial institutions that are members of SPEI.

In 2018, the Mexican financial system was subjected to a series of cyberattacks that affected payment systems. In May 2018, Banco de México warned banks to upgrade their existing security mechanisms following a series of fraudulent transactions that amounted to approximately $15 million.[52] The fraudulent transactions occurred in five financial institutions that were connected to SPEI. While the cyberattacks did not directly target SPEI, the central payment system, the attacks were aimed at violating the systems for the generation and transmission of payment transfer orders. Specifically, attackers used a vulnerability in third-party software that was connected to SPEI to access the system and initiate fraudulent transactions, which were subsequently cashed out by the criminals.[53]

To carry out the attacks, the hackers took advantage of the functionalities and expedited processing capabilities that were implemented within the national payment system, in such a way that the automated processing of the illegitimate payment transfer orders could be carried out before they were detected in time by the financial institutions from which they originated. Consequently, the cyberattack was not intended to render SPEI inoperative or

penetrate the defenses and internal control mechanisms of Banco de México.[54]

During the attacks, different techniques were used to insert, into the flow of operations that the compromised institutions process in their systems, simulated transfer orders that were not generated by the clients' account-management systems, so they were not referred to any of these accounts. The account holders' resources were not affected, since only the financial institutions' transfer order–sending systems were accessed and charged to the concentrator accounts that they maintain for the processing of all transfers made by the centralized payment system. Furthermore, the attackers used valid beneficiary accounts to retrieve funds. The illegitimate transfers were generated by specific amounts. The recipients of the funds were also valid entities within the system. Consequently, the transfers were settled in accordance with the payment system's procedures.

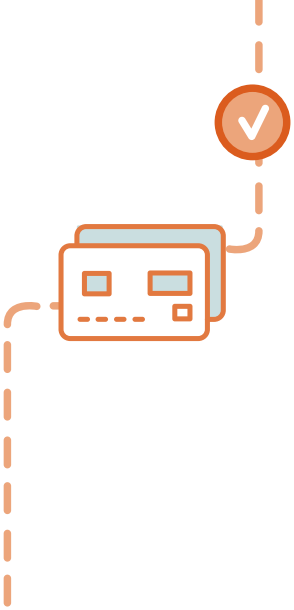
The cyberattacks that took place in Mexico used well-known techniques, such as credential theft, privilege escalation, lateral movements between servers, insertion of files or execution of instructions, and the deletion of logs. Based on the subsequent forensic analysis that was conducted,[55] risk-mitigation measures were implemented to avoid similar attacks and to strengthen the interaction of Banco de México with the institutions that participate in the payment systems that it operates.

6.5 LESSONS LEARNED

Other organizations concerned about cyber risk in FPS could benefit from the following lessons learned by FPS operators and providers in Brazil, Poland, Bahrain, and Mexico:

- The safe and continuous operation of payment systems and other FMIs is a top priority for FPS regulators such as central banks. To enhance the cyber resilience of the financial sector, regulators in these countries opted for principle-based cyber regulatory frameworks, in some cases supplemented by specific requirements for the secure operation of FPS. Regulators highlight the importance of establishing a cybersecurity regulatory framework that provides flexibility for FPS participants to adopt innovative solutions. To deal with risks introduced by emerging technologies, regulators periodically review and update the rulebooks or supplement them with specific requirements.
- Ensuring the cybersecurity and resilience of the FPS is also a top priority for FPS operators. Similarly, effectively managing cyber risk is a business imperative for FPS providers and a key goal in their strategies.
- A key success factor for these organizations was implementing a robust cyber risk–management framework from the beginning, supported by a suitable governance structure with clear roles and responsibilities for managing cyber risk.
- The organizations leveraged international guidelines, such as those established by the BIS in the Principles for Financial Market Infrastructures. Then they based their cybersecurity programs on internationally recognized cybersecurity standards and frameworks, such as the ISO/IEC 27002:2022 standard and the NIST Cybersecurity Framework. Following these standards and frameworks, they implemented a comprehensive set of technical and procedural controls at the human, process, and technological levels, tailored to the nature and culture of their organizations and environment.
- These organizations acknowledge the importance of keeping continuous awareness of the changes in the technological and threat landscapes and accordingly adjust the security control environment to address emerging cyber risks. Maintaining situational awareness hinges on threat intelligence capabilities and information-sharing arrangements where participants across the financial sector share relevant information about threats and incidents.
- The cyber risks that consistently appeared at the top of their risk registers are fraud, compromise of confidentiality of sensitive information, and disruption of critical services. As such, these organizations pay special attention to protective and detective controls that deal with DDoS attacks, ransomware, malware, and phishing campaigns. The effectiveness of the security control environment is periodically tested through penetration tests and other types of assessments.
- To deal with cyber-enabled fraud, FPS operators either implement near real-time fraud-detection capabilities or provide relevant and prompt information to FPS participants to find potentially fraudulent transactions. Special attention is paid to user registration and onboarding, as well as user authentication.
- These successful FSP operators also recognized the importance of consumer cyber literacy, so they regularly implement campaigns to raise cybersecurity awareness continuously among users of the FPS.

- Acknowledging that, regardless of all the preventive and detective controls in place, they may be affected by a successful cyberattack, these organizations implement mechanisms to resume safe operations within expected recovery objectives that aim at providing uninterrupted fast payment services. They periodically conduct table-top exercises and crisis-simulation exercises to test the effectiveness of the business-continuity and disaster-recovery plans.
- These FPS operators consider that a key element of protecting the reputation of the organization and the whole FPS is to exercise transparency in disclosing cyber incidents when they occur. The disclosure of cyber incidents is accompanied by the measures taken to prevent their recurrence.



7 CONCLUSION

Financial institutions place extensive reliance on ICT to provide electronic financial services, including payment-related services. Internet banking, mobile payments, and other technological developments have increased the flexibility and convenience of payment systems. The number of jurisdictions with services and systems that allow users to conduct (near) real-time payments on a 24/7 basis has grown notably. However, the technological developments that help accelerate the implementation of the FPS also introduce cyber risks and, potentially, increase the attack surface.

FPS are especially attractive targets for fraud, money laundering, and other illicit activities, as cyber criminals try to exploit the speed of these systems to move funds undetected. The convergence between cyber risk and fraud merits considerable attention. Cyber incidents that disrupt FPS could severely affect economic activity. Such disruptions could originate from outside the financial sector, given the critical dependencies of FPS and other FMIs on other sectors of the economy, such as IT, telecommunications, and energy. As an example, a DDoS attack that brings down the internet service provider of the FPS operator or a PSP may make the fast payment service itself unavailable to consumers, despite the fact that neither the operator nor the PSP were attacked directly. These types of incidents could also trigger systemic risk if they cause spillovers to other financial institutions in the jurisdiction. Therefore, operators, service providers, and regulators should consider systemic risk implications closely within the context of FPS.

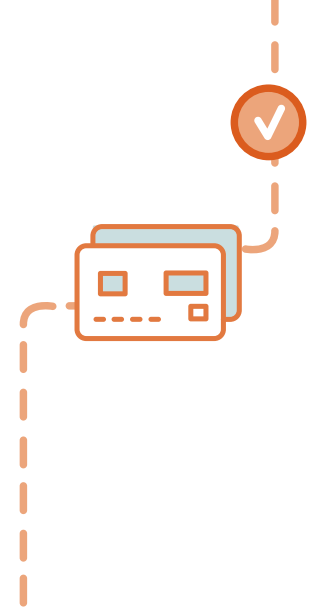
FPS are such a key part of the financial system that some jurisdictions have designated them as systemically important payment systems. Furthermore, national jurisdictions may also need to assess whether FPS (or potentially other payment systems) constitute national critical infrastructure based on their nature, size, and complexity. Ensuring the cybersecurity and resiliency of the FPS is a vital part of central banks and regulatory authorities' efforts to strengthen cyber resilience in the financial sector. At the same time, regulatory authorities face challenges in this regard. The regulation of cyber risk is not uniform across the various jurisdictions. Cyber risk for payment systems is a topic that is not always prioritized by supervisory authorities. In certain cases, a cyber risk regulatory framework for payment systems may be missing. In jurisdictions where multiple regulatory bodies are responsible for supervising cyber risk, close coordination and communication is vital between the different regulatory entities in order to avoid ineffective supervision and a false sense of security that cyber risk is being sufficiently addressed in the system. To summarize, managing cyber risk in an effective manner has become imperative for FPS operators and providers.

A robust cybersecurity program requires the implementation and operation of a comprehensive set of controls across the organization at the human, process, and technological layers. Several recognized international frameworks and guidelines provide guidance on how to address the challenge of effectively managing cyber risk and could be

used by FPS operators and providers as a starting point to create their cybersecurity programs, tailored to the nature, size, complexity, risk profile, and culture of the organization.

Preventing fraud, protecting the confidentiality and integrity of transactions, and ensuring the availability of critical services are paramount for FPS operators and providers. Hence, their cybersecurity programs focus not only on preventive controls, such as strong authentication and encryption of transaction channels, but also on real-time capabilities to detect potential fraud and frequently tested, effective plans to respond to incidents and safely resume critical services in case of a cyberattack. Leading payment system organizations also recognize the importance of end user cyber literacy and implement tailored programs to raise cybersecurity awareness among consumers of the fast payment services.

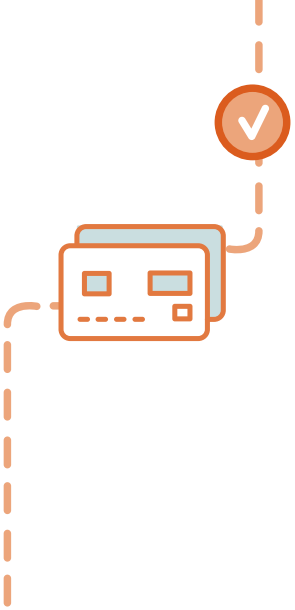
FPS operators and PSPs must adopt an effective cybersecurity risk–management framework that offers flexibility to deal with the ever-evolving threat landscape looming over an industry that continues developing innovative payment services and leveraging emerging technologies. This cannot be done in isolation, so supervisory authorities should encourage and facilitate the prompt sharing of actionable cyber threat intelligence among actors in the fast payment ecosystem to increase situational awareness and strengthen cyber resiliency.



8 ACKNOWLEDGMENTS

Organization	Contributor
World Bank	David Papuashvili (primary)
	Marcelo Roldan (primary)
	Harish Natarajan
	Dorothee Delort
	Guillermo Galicia Rabadan
	Holti Banka
	Nilima Ramteke
	Thomas Piveteau
	Andrea Monteleone
	Kiyotaka Tanaka

The authors would like to thank Ghislain de Salins, Goran Vranic, Hunt La Cascia (all World Bank), for their valuable comments during the peer reviewing process.



APPENDIX A

INTERNATIONAL FRAMEWORKS FOR MANAGING CYBER RISK

Informed by the organization's nature, size, complexity, risk profile, and culture, organizations in the FPS should leverage existing recognized international standards and guidelines to manage cyber risks effectively. Among others, the following frameworks and guidelines provide good starting points:

NIST Cybersecurity Framework:[56] This framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk-management processes. The framework consists of three parts: the framework core, implementation tiers, and framework profiles. The framework core incorporates concurrent and continuous functions: govern, identify, protect, detect, respond, and recover. Using profiles, the framework will help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The tiers give a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

ISO/IEC 27002:2022 (Information Security, Cybersecurity and Privacy Protection):[57] ISO/IEC 27002 is an international standard that provides guidance for organizations looking to set up, implement, and improve an information security management system focused on cybersecurity. While ISO/IEC 27001 outlines the requirements for an information security management system, ISO/IEC 27002 offers leading practices and control objectives related to key cybersecurity aspects, including access control, cryptography, human resource security, and incident response. The standard serves as a practical blueprint for organizations aiming to safeguard their information assets against cyber threats effectively. By following ISO/IEC 27002 guidelines, companies can take a proactive approach to cybersecurity risk management.

ISO 22301:2019 (Security and Resilience—Business Continuity Management Systems):[58] ISO 22301 is the international standard for business continuity management systems. It provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents. This standard is crucial for organizations to enhance their resilience against various unforeseen disruptions, ensuring continuity of operations and services. It helps in identifying risks, preparing for emergencies, and improving recovery time.

ISO/IEC 27701:2019 (Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management):[59] ISO 27701 specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a privacy information management system in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

ISO 5201:2019 (Financial Services—Code-Scanning Payment Security):[60] ISO 5201 provides an overview and risk assessment of, and minimum security requirements and extended security guidelines for, code-scanning payment

in which the payer uses a mobile device to operate the payment transaction. This document is applicable to cases where the payment code is used to initiate a mobile payment and presented by either the payer or the payee.

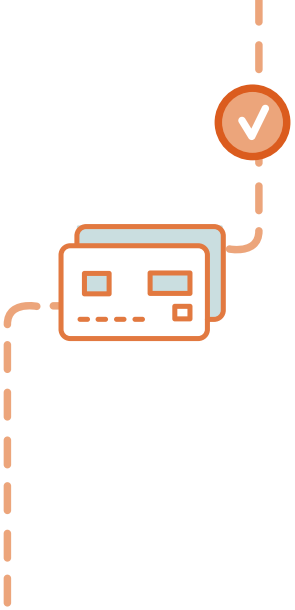
ISACA Control Objectives for Information Technologies (COBIT):[61] COBIT is a framework of the best practices for IT governance. It is a set of best practices and procedures that help the organization to achieve strategic objectives through the effective use of available resources and minimization of IT risks. COBIT interconnects enterprise governance and IT governance. This connection is realized by linking business and IT goals, defining metrics and maturity models to measure the achievement of objectives, and defining the responsibilities of owners of the business and IT processes.

Payment Card Industry Data Security Standard (PCI DSS):[62] PCI DSS defines security controls and processes for entities involved in the payment ecosystem, as well as requirements for developers and solution providers to build and securely manage payment devices, software, and solutions for the payment card industry. PCI DSS is a standard for developing a robust process for securing payment account data, including prevention, detection, and proper reaction to security incidents.

National Cyber Security Centre's 10 Steps to Cyber Security:[63] This guidance aims to help organizations manage their cybersecurity risks by breaking down the task of protecting the organization into 10 components. Adopting security measures covered by the 10 steps reduces the likelihood of cyberattacks occurring and minimizes the impact on the organization when incidents do occur.

ECB Cyber Resilience Oversight Expectations for Financial Market Infrastructures:[64] In June 2016, the CPMI and IOSCO published *Guidance on Cyber Resilience for Financial Market Infrastructures* (see below), which requires FMIs to take the necessary steps to implement it to ensure that they enhance their levels of cyber resilience. The cyber resilience oversight expectations provide FMIs with detailed steps on how to operationalize the guidance, provide overseers with clear expectations to assess the FMIs, and establish the basis for a meaningful discussion between the FMIs and their overseers.

CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures:[65] This document provides supplemental guidance to the CPMI-IOSCO Principles for Financial Market Infrastructures related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities. Like the ECB document, this guidance outlines cyber resilience expectations around such domains as governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving.



APPENDIX B

INTERNAL CONTROLS

The effective management of cyber and IT risk, as a part of the overall operational risk-management framework, depends on the adequacy of internal controls. Controls, within the context of managing risk for FPS, may be used to mitigate the inherent level of risk associated with the operational environment. In general, controls can be grouped into the following two broad categories:

- Time-based controls
- Qualitative controls

A control can fall into both categories at the same time, and the two categories mentioned above are not mutually exclusive. This means that a time-based control can also be a qualitative control. Time-based controls are either preventive, detective, or corrective. Table B1 briefly defines each type of time-based control.

Qualitative controls can take various forms. They can be administrative or directive in nature but can also be technical or physical. Table B2 provides a list of qualitative controls with brief descriptions.

TABLE B1 Time-Based Controls

CONTROL TYPE	CONTROL DESCRIPTION	EXAMPLES
Preventive	Prevention of event or incident	Access controls for applications, IPS, firewalls, locks, and so on
Detective	Warning or notification mechanisms that warn the organization about the occurrence of an event	Anomalous activity reports, logs, IDS, video cameras
Corrective	Control type that reduces the impact of an event	Business-continuity plan, incident-response plan

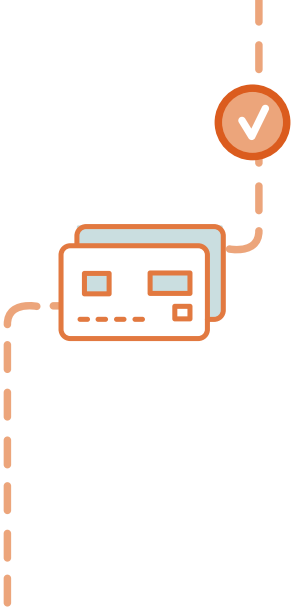
TABLE B2 Qualitative Controls

CONTROL TYPE	BRIEF DESCRIPTION	EXAMPLES
Administrative/ directive	Control type, based on management expectations, that mandates what actions are allowed and not allowed and also in line with the organization's risk appetite	Fraud-prevention policy, information-security policy, business-continuity policy
Deterrent	Control type that either warns or dissuades threat agents from accessing the system	Warning banners and log-in screens
Technical	Application (program) or device control that prevents unauthorized activity	Data leakage prevention system, firewall, and the like
Physical	Device that prevents physical access to an information asset	Biometric controls, locks, fences, and doors

Network Controls

Fast payment service operators and providers typically need to protect their networks over which payment services are sent and processed. Some controls needed to protect the network include a firewall and IDS. When it comes to firewall implementation, the firewalls may be installed at each internet connection point and between the demilitarized zone and the internal network zone.

In addition, network diagrams that clearly find all connections between fast payment service operators and service providers and other networks offer an effective method for finding the channels via which specific threats and risks may arise. It is also important to map data flows associated with payment system processes.



APPENDIX C

CYBERSECURITY AND AI

Since FPS depend on (near) real-time availability of funds for the payee, PSPs need to be able to detect and prevent a wide array of cyber threats that may affect the continuous, safe functioning of the payment system process. The use of technical solutions (for example, antivirus, IDS/IPS, log aggregation) leveraging AI can be important when faced with different scenarios associated with cyber risk. AI has recently appeared as an effective tool for creating potentially smarter and safer security systems that allow organizations to predict and detect suspicious network activity. PSPs can deploy solutions leveraging machine learning and deep learning algorithms to mitigate cyber risk. These solutions may offer many benefits. One of the potential benefits of AI is the ability to analyze substantial amounts of data and information quickly, compared to other methods. As a result, cyber threats may be identified with greater speed.

Before AI algorithms, threat detection was widely based on rules and signatures. The process was commonly used for the detection of viruses and other forms of malware. One of the downsides to using methods based on rules and signatures was its rigidness in finding and preventing evolving threats. In addition, limited levels of automation and a lack of real-time analysis posed considerable challenges when dealing with dynamic and evolving cyber threats.

AI can improve the detection and prevention of cyber risk–related events. AI is based on machine learning algorithms that can be incorporated into the organization's risk-management processes to allow prompt detection (and prevention) of both existing and emerging cyber threats. This can be done by implementing various machine learning algorithms designed for detecting anomalous events. It must be mentioned that both traditional machine learning algorithms, such as decision trees and nearest-neighbors, as well as some of the more advanced neural networks and deep learning algorithms can be used for the detection and prevention of cyber risk–related events.

The advantages associated with AI also include behavioral analysis, pattern recognition in large datasets, and reduced false positives. Therefore, machine learning, which is a subset of AI, can be deployed for malware detection and classification, network traffic analysis, and even vulnerability management. Adversarial models associated with machine learning also offer the potential benefit of generating realistic cyber risk–related events and scenarios against which risk-management systems can be trained to detect newly emerging threats that have not been faced before. For example, adversarial models can be used to generate authentic-looking fraud events and other cyber threats to try to evade detection, which can be used by the organization to train its own systems and improve the accuracy rate of both detection and prevention.

Another significant benefit of using AI-based models is in incident management. PSPs can use AI-based models to analyze a vast array of data, ranging from logs and endpoint data to network traffic and payment systems, offering the ability to detect and prevent threats in real time.

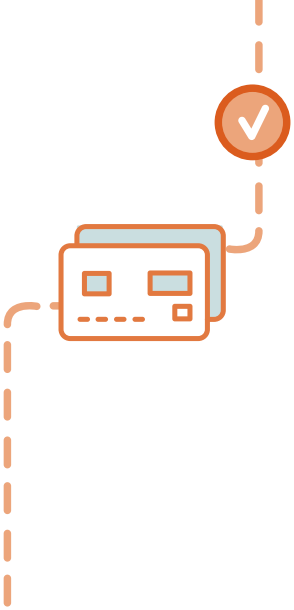
The adoption of AI also poses a few challenges to organizations, including PSPs. One of the main drawbacks to using

AI-based models is the specialized knowledge that is needed to develop, implement, and configure such systems. In addition, data quality is a significant issue that is associated with AI-based models. The quality of the threat detection and prevention is directly proportional to the data used to train the AI model. If the model does not use data that has been evaluated for consistency and accuracy, the accuracy (and reliability) of the system will be lower than intended and the model itself may be challenged. The quality of cyber risk–related data and operational risk data in general may differ from organization to organization and even from system to system. The lack of uniform taxonomies and data-classification schemes may pose an added challenge in gathering high-quality data for training AI-based models.

Furthermore, AI-based models are complex, which can make them difficult to understand and analyze.

Another significant aspect worth considering when adopting such systems is the lack of explainability. AI algorithms may not explain how the system decided to block a specific payment transaction that was classified as suspicious.

Overall, AI and machine learning offer considerable benefits for the effective detection of cyber threats associated with FPS. This is especially relevant when dealing with real-time processing of payments. Simultaneously, the challenges and risks associated with AI (and machine learning) must be weighed carefully.



APPENDIX D

SECURE DESIGN PRINCIPLES

The U.S. National Centers of Academic Excellence in Cybersecurity list the following 12} baseline security principles that should be followed for developing relevant protection mechanisms:[66]

Economy of mechanism: Economy of mechanism refers to the fact that security measures, such as control mechanisms that are implemented in both hardware and software, should be as simple and small as possible. Simple and small designs are usually easier to test and verify in detail. When the security design is complex or difficult to understand, there are more opportunities for an adversary to discover subtle weaknesses to exploit that may be difficult to find in advance. In general, the more complex the security mechanism, the higher the probability (likelihood) that the mechanism may have security flaws and vulnerabilities. Again, simpler mechanisms are likely to have less exploitable weaknesses and require less maintenance. In addition, because configuration-management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process. In practice, this is one of the most challenging principles to implement. In most organizations, there is a constant demand for new features in both hardware and software, which complicates the security design task. The best that can be done is to keep this principle in mind during system design, to try to eliminate unnecessary complexity.

Fail-safe default: The fail-safe default implies that access decisions need to be based on permission, as opposed to exclusion. This means that the default situation should be a lack of access, and where the protection scheme of the organization finds the conditions necessary for access to be granted. This approach is characterized by a better failure mode than its alternative, which grants access even in cases when something might go wrong. A design or implementation mistake in a mechanism that gives explicit permission tends to fail by refusing permission, a safe situation that can be quickly detected. On the other hand, a design or implementation mistake in a mechanism that explicitly excludes access tends to fail by allowing access, a failure that may go undiscovered for long periods of time during normal use. For example, most file-access systems work on this principle, and all protected services on client/server systems work this way.

Complete mediation: This part refers to the fact that every access must be checked against the access-control mechanism. Systems should not rely on access decisions retrieved from a cache. In a system designed to run continuously, this principle requires that, if access decisions are remembered for future use, careful consideration should be given to how changes in authority are introduced into local memory. File-access systems represent an example of a system that follows this principle. However, typically, once a user has opened a file, no check is made to see if permissions change. To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control. This resource-intensive approach is rarely used.

Open design: The idea behind open design is that the security mechanism should be open, instead of secret. For example, when looking at the way encryption may be

implemented, while the encryption keys that are used to encrypt data need to remain secret, the encryption algorithm that is used should be open to scrutiny and review by outside experts.

Separation of privilege: Separation of privilege is often defined as a practice that includes the use of several privilege attributes that are needed to achieve access to a restricted resource. Day-to-day operations are executed in a lower privileged-access regime. A prime example of separation of privilege includes two-factor authentication. Multifactor authentication requires several (at least two) authentication techniques, such as a password and biometrics, to authorize a user. Separation of privilege can also be used to refer to any task that is divided based on specific privileges. For example, administrative tasks may be restricted to a separate account, while everyday activities are conducted with low-privilege accounts.

Least privilege: The concept of the least privilege is associated with the idea that every process or task and every user of a specific system should function with the least set of privileges that are necessary to conduct the task. Role-based access control is an access-control principle and method based on the concept of least privilege. Each role is assigned only the permissions that are needed to perform specific tasks.

Least common mechanism: The idea of the least common mechanism refers to the fact that the design should minimize the functions that are shared by different users, the end result of which is to provide mutual security. The principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, making it easier to verify if there are any undesirable security implications.

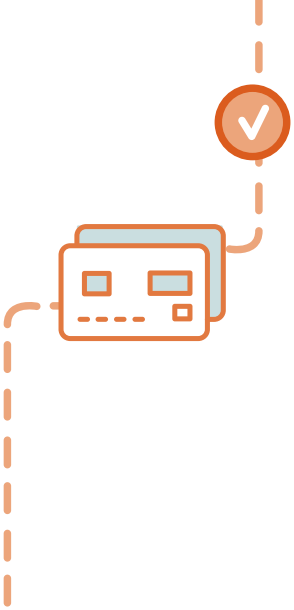
Psychological acceptability: One of the most important concepts of a secure design is psychological acceptability. This means that the control mechanisms that are implemented should not interfere excessively with the everyday operations of users and the organization itself. The mechanisms implemented should not hinder the organization's functioning. If the internal control mechanisms are considered excessive and unusable by the staff, employees might choose to ignore the controls wherever this might be possible. As a result, the cyber risk associated with such practices might increase. It is also worth noting that the implemented security controls should make sense to the employees and fit the mental model of the users. In short, these mechanisms should not be too burdensome. In addition, if the control mechanisms do not make sense to the employees, the chance of making mistakes also increases.

Isolation: The concept of isolation has three parts. In general, public access systems should be isolated from the more sensitive or critical systems that hold sensitive data, processes, or other assets of the fast payment service operator or service provider. For some of the more sensitive information systems and assets, physical isolation of the critical systems may be considered. In other cases, a defense-in-depth approach, using logical security controls, may be implemented. The second aspect of isolation refers to the fact that processes and files of individual users should be isolated from one another except where access is specifically needed. All modern operating systems offer the capability to provide separate space for individual users, with relevant protection mechanisms for the prevention of unauthorized access. The third part of isolation deals with the need to isolate security mechanisms, such as internal controls, in such a way that prevents unauthorized access to the security controls.

Encapsulation: Encapsulation is typically a form (subset of isolation) that is founded on object-oriented functionality. Security is provided by encapsulating or enclosing a collection of procedures as well as data objects in a separate domain in such a way that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated entry points.

Modularity: The use of modular architecture is one of the key components of secure design. This principle implies the use and adoption of a modular architecture and the development of security functions as separate, protected modules. For example, functions associated with the encryption of data and information should use common security modules or services. Security modules should be portable to newer technologies in an easy manner without too much (excessive) effort.

Layering: As noted in some of the earlier guidance, operational risk stems from people, processes, systems, and external events. Security controls (that is, internal control mechanisms) should be developed to ensure a defense-in-depth approach. This applies to, among other things, payment system processes. Control mechanisms should be designed and implemented to ensure overlapping protection addressing the operational risk factors mentioned above. This means that if one control mechanism fails, there are other overlapping controls that will not leave the system unprotected.



APPENDIX E
SAMPLE THREAT CHECKLIST FOR PAYMENT SYSTEMS

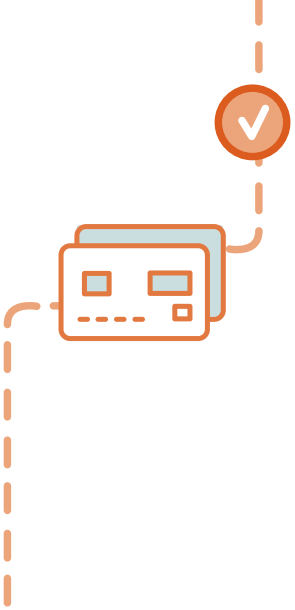
The following is a sample threat checklist that has been modified for payment systems and is based on the risk-management threat checklist model developed by the German organization IT-Grundshutz.[67] It is not exhaustive but intended to guide fast payment service operators and providers in finding the threats that they may face.

	THREAT CHECKLIST		
	Instructions: Risk managers and other risk analysts can use the following checklist to find cyber and IT threats that are relevant for FPS. The checklist is divided into three main categories: integrity, confidentiality, and availability of data, information, and processes.		
	CATEGORY		
1	**Integrity**		**Applicable (Yes/No)**
	1.1	Payment-transaction stream could be intercepted.	
	1.2	Faulty programming associated with the FPS could (inadvertently) modify data.	
	1.3	Electronic (or other) copies of transactions or reports could be diverted to unauthorized or unintended persons.	
	1.4	Data could be entered incorrectly.	
	1.5	Intentional incorrect data entry.	
	1.6	Use of outdated programs could compromise the integrity of information.	
	1.7	Faulty hardware could result in inaccurate data entry and analysis.	
	1.8	Third parties could modify transactional data.	
	1.9	Files could be accidentally deleted.	
	1.10	Hackers could change data associated with fast payment transactions.	
	1.11	Internal users could launch unauthorized programs to access and modify transactional data.	
	1.12	Reports could be falsified.	
	1.13	Internal theft of information by employees.	
	1.14	Network sniffing could intercept user passwords and allow unauthorized modification of information.	
	1.15	Information could be outdated.	

1	**Integrity,** *continued*		**Applicable (Yes/No)**
	1.16	Hackers could obtain unauthorized access into networks to corrupt system resources.	
	1.17	Physical intrusion by unauthorized persons.	
	1.18	Documents could be falsified to appear as official company documents.	
	1.19	Information could be misinterpreted due to language barriers.	
	1.20	Fraudulent programming could affect data integrity.	
	1.21	Computer viruses could modify data.	
	1.22	Information could be misdirected.	
	1.23	Transactions could be intentionally not run or misrouted.	
	1.24	Newer or upgraded software could cause corruption of documents or files.	
	1.25	Non-standard procedures could cause misinterpretation of information.	
	1.26	Unauthorized persons may use an unattended workstation.	
	1.27	Information to and from third parties could be corrupted in transmission.	
	1.28	Account information may be shared.	
	1.29	A power failure could corrupt information.	
	1.30	Information could be submitted vaguely or misleadingly.	
	1.31	Someone could impersonate a customer to corrupt records (identity theft).	
	1.32	Information could be taken outside the organization.	
	1.33	The integrity of information could be compromised due to the decay of information media.	
	1.34	Someone could impersonate an employee to corrupt information.	
	1.35	A terminated employee could intentionally corrupt information.	
	1.36	Organization could be targeted for system hacking by a dissatisfied customer.	
	1.37	A default username and password for a network device could be exploited to gain access to system resources.	
2	**Confidentiality**		
	2.1	Insecure email could contain confidential information.	
	2.2	Internal theft of information.	
	2.3	Employees cannot verify a client's identity—for example, by using phone masquerading.	
	2.4	Confidential information is left in plain view on a desk.	
	2.5	Social discussions outside the office could result in disclosure of sensitive information.	
	2.6	Information could be saved by unauthorized persons from dumpsters or other waste receptacles.	
	2.7	Information sent to third parties may be misused.	
	2.8	An unattended computer could give unauthorized access to files.	
	2.9	Passwords may not be required for all workstations.	
	2.10	Unauthorized people in confidential or restricted areas.	
	2.11	Confidential information may be left on the fax or copy machine, granting unauthorized viewing of documents.	
	2.12	Fraudulent representation or misrepresentation of individuals in phone (or other) conversations.	
	2.13	Documents sent out for authorization could be forged and then returned.	
	2.14	Unauthorized access to information by viewing documents over the shoulder of an employee (shoulder surfing).	
	2.15	Transactions or files associated with transactions could be excessively duplicated.	
	2.16	Employee passwords could be shared.	
	2.17	Interoffice messengers may handle confidential information.	
	2.18	Employee and messenger relationships could exchange sensitive or confidential information.	

2	Confidentiality, *continued*		Applicable (Yes/No)
	2.19	Unauthorized disclosure of information by third parties.	
	2.20	Inadequate destruction of electronic media may leave information available to unauthorized persons.	
	2.21	Inadequate firewall configuration could inadvertently allow disclosure of information.	
	2.22	Actual client information could be used on templates, causing disclosure of sensitive information.	
	2.23	Employees may be overheard discussing confidential information outside the office.	
	2.24	Documents could be inadvertently delivered to the wrong person.	
	2.25	Holding phone conversations when unable to verify identity.	
	2.26	Company (organization) could be subjected to electronic eavesdropping.	
	2.27	Terminated employees may be able to access the building or information.	
	2.28	Cleaning crews may see confidential information.	
	2.29	Rubbish could contain confidential information.	
	2.30	Employees may not always follow the dual-control procedures.	
	2.31	Temporary or new employees may be insufficiently trained.	
	2.32	Restricted areas may be accessed by visitors.	
	2.33	Use of the speaker phone may violate confidentiality.	
	2.34	Information and files may be inappropriately accessed on the company's (organization's) systems.	
	2.35	Data stored off-site could be compromised.	
	2.36	Employees may install illegal or unauthorized software.	
	2.37	Consultants or other contracted help may view confidential information.	
3	**Availability**		
	3.1	Fast payment services may be unavailable to consumers and other stakeholders	
	3.2	Hardware failures could affect the availability of critical, payment systems–related processes or other organizational resources.	
	3.3	"Acts of God": earthquake, mudslide, flood, avalanche, windstorm, and so on	
	3.4	Upgrades in the software may prohibit access.	
	3.5	The company system could be unavailable or down.	
	3.6	An undersecured work area could jeopardize the confidentiality of a customer or other sensitive information.	
	3.7	A power failure could interrupt employee access.	
	3.8	Software upgrades could affect other programs.	
	3.9	Expired user access and/or insufficient employee training could disrupt the computer system.	
	3.10	Availability of personal computers shared by multiple users may be inadequate.	
	3.11	Vendor or supplier support personnel may be unavailable due to time zone differences.	
	3.12	A communication failure could disrupt business operations.	
	3.13	Employees may have incorrect or inappropriate file access.	
	3.14	If a person is out (sick/absent), critical files cannot be accessed.	
	3.15	Outsourcing to a service provider or third-party support to fix problems would give access to confidential information.	
	3.16	An absent person or tools could prevent backup if not available.	
	3.17	The organization could be subject to bombs or other acts of terrorism.	
	3.18	Theft of equipment or other information.	
	3.19	Insufficient cross-training of critical procedures could affect the organization's business processes.	
	3.20	Availability of information resources controlled by third parties could affect business processes.	

2	**Availability,** *continued*		**Applicable (Yes/No)**
	3.21	Damaged or altered storage or hardware media.	
	3.22	Not all workstations have all programs loaded.	
	3.23	Users could lose or misplace files.	
	3.24	Geography and getting materials in, due to distance.	
	3.25	Vandalism and sabotage could be attempted on the payment system network.	
	3.26	The number of software licenses could be insufficient.	
	3.27	Insufficient personnel resources could affect business processes.	
	3.28	A computer virus could be introduced via email or disk.	
	3.29	DDoS attacks from malicious internet users outside the organization.	
	3.30	Employee causes a document to be inaccessible temporarily due to human error.	
	3.31	The threat of natural disasters, including floods, mudslides, earthquakes, forest fires, and so on	
	3.32	Epidemic	
	3.33	Fire: Internal, minor	
	3.34	Fire: Internal, major	
	3.35	Fire: External	
	3.36	Human error, maintenance	
	3.37	Human error, operational	
	3.38	Human error, programming	
	3.39	Human error, users	
	3.40	Toxic contamination	
	3.41	Medical emergency	
	3.42	Loss of key staff	
	3.43	Human, deliberate	
	3.44	Environmental	
	3.45	Power flux	
	3.46	Power outage, internal	
	3.47	Power outage, external	
	3.48	Water leak/plumbing failure	
	3.49	HVAC failure	
	3.50	Temperature inadequacy	
	3.51	Telecommunications failure	



APPENDIX F

INCIDENT-RESPONSE PLAN

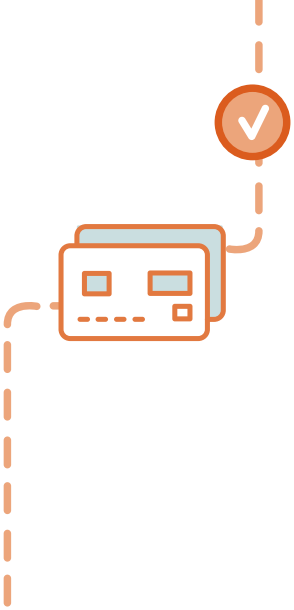
The following aspects should be considered when designing an incident-response plan:

- **Objectives:** The incident-response plan should include a set of objectives that the organization aims to achieve with its incident response.
- **Strategy:** Following the official definition of objectives, the organization needs to describe the strategy—that is, how it intends to achieve the objectives mentioned above.
- **Policy:** The incident-response plan should consist of a clearly defined policy approved by the organization. The policy should describe, at a high level, how incident response is supposed to work.
- **Definition of events:** Distinct types of events require different responses. Therefore, the responses should be customized based on the event (incident) that has occurred. The incident-response plan should not cover only the IT side of the organization. It should be comprehensive and include different types of cyber risk–related events. If needed, a subset of the incident-response plan can be created for IT specifically.
- **Preparation:** An incident-response plan needs to include clearly defined roles and responsibilities for each member of the incident-response process. In addition, communication during incident response is vital. Therefore, incident response should address whether communication can be achieved as needed, during times of need. Incident-response plans should include the following:
  - Updated contact information for all internal and external responders or stakeholders, as needed
  - Address who will be responsible for incident (event) escalation
  - Categorize communications according to priority (that is, telephone, email, in-person, fax, and so on)
  - Establish a certain location for communication and response coordination
  - Business continuity and the availability of systems during response, including for evidence-gathering activities
- **Detection and analysis:** Considerable attention needs to be paid to the process of incident detection and analysis. An incident cannot be mitigated or addressed if the organization has not realized that it has been affected by a specific event. Therefore, there should be relevant detective controls that can find specific events. At the same time, the organization's incident-response team and potentially other relevant staff members should have sufficient analytical capabilities to analyze what happened and how best to respond.
- **Containment, correction, and recovery:** The PSP's incident-response plan needs to define clearly risk-mitigation

actions for the various events that it has prepared for (or at least found). The following factors can be considered:

- Evidence gathering
- Realized or potential impact of an incident
- Resource requirements
- How long will it take to recover from an event

- **Post-incident improvement:** This section is (or should be) the lessons-learned part of incident response. If something did not work as well as intended, then the organization needs to look at the reasons why the process was ineffective. Corrective actions should also be decided at this stage if the incident response did not go as intended.



APPENDIX G

INFORMATION-SHARING ARRANGEMENTS

An information-sharing and analysis center (ISAC) may share a fairly wide variety of information with its participants. While general operational risk–related data and information can be sent, the information that is shared should be actionable and, in most cases, related to cybersecurity. Information about credit risk, market risk, and other forms of financial risk unrelated to operational risk should not be shared in an ISAC context.

The following information is usually issued within ISACs:

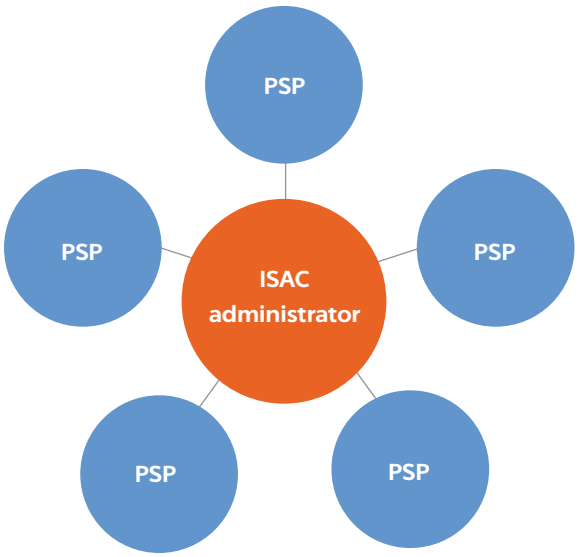
- Incident-specific information on cyber risk–related and operational risk events (although, in some cases, operational risk–related events may not be shared since this might be too broad)
- Advice and support on how to take protective measures or mitigate risk
- Information about systemic risk, which may have an impact on the financial system
- Alerts on imminent threats to the financial system
- Analysis of incidents and threats that can aid financial institutions in the risk-mitigation process
- Technical vulnerabilities that might affect the financial system
- Good practices on incident handling
- Any other relevant information that can help financial system participants mitigate risk promptly

Specific rules or protocols such as the Traffic Light Protocol should be considered to control what information could be shared and with whom.

Furthermore, members can use or develop a format for the sharing of incident-related information. The financial regulatory authority (or a central bank) can also require members to submit information on incidents using a specific format that might be shared in a sanitized manner once it is validated by the operator of the information-sharing platform (if the ISAC is centralized and participants do not share information horizontally). Figure 19 presents a diagram for a centralized information-sharing and analysis center.

In figure 19, each financial institution in the form of PSPs and the administrator of the ISAC platform (which can be an

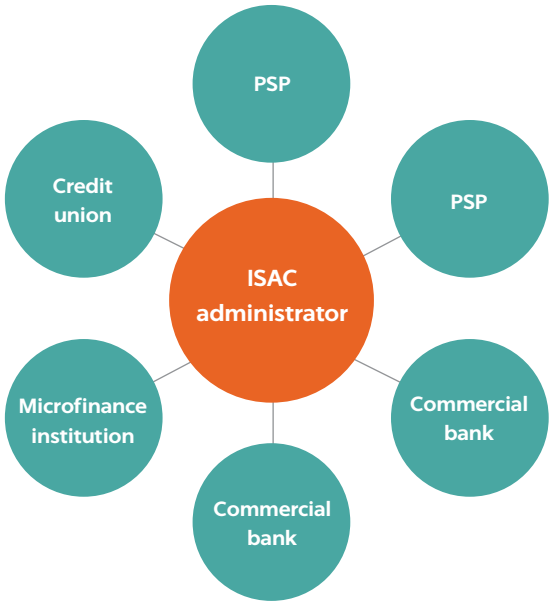
FIGURE 19 **Example Illustration of a Centralized ISAC for the Payment Ecosystem**



organization such as a central bank) share incident-related information. The ISAC administrator is responsible for aggregating, validating (checking), and analyzing the information that is received before it is sent to any of the other participants in the ISAC. It is important to note that incident-related information should be anonymized before it is shared with any of the other participants of the ISAC. This means that only event- or process-related and technical details should be shared with the participants, and not the names of specific financial institutions (or individuals) that share the information within the context of the ISAC, as stipulated by relevant legal requirements.

Figure 20 offers an alternative, expanded, sector-specific setup for a centralized financial-sector ISAC. The participants include PSPs, commercial banks, microfinance institutions, and credit unions. As in the earlier example, the ISAC administrator may be the fast payment service operator in the form of a central bank or another entity that aggregates, validates, and analyzes cyber risk–related information and then disseminates relevant information to participants. The main difference is that, instead of having only organizations that are associated solely with the payment ecosystem, the ISAC also includes financial intermediaries in the form of commercial banks, microfinance institutions, and credit unions. By adding different financial institutions to the information-sharing process, a larger variety of organizations may be able to provide a greater amount of relevant data and information for cyber risk mitigation.

FIGURE 20 **Example Illustration of a Centralized Financial-Sector ISAC with Participating PSPs, Banks, Microfinance Institutions, and Credit Unions.**



Initial Development

Key entities and individuals need to be named once the decision to set up an ISAC is made. The entity or entities that decide to set up the ISAC should name who will be the process owner for the ISAC (that is, an administrator/facilitator) and which members will have the right to share information within the ISAC. During the early stages of the ISAC, it makes considerable sense to involve only a few financial institutions, including PSPs or other entities, such as commercial banks, in order to make sure that the process is set up effectively and builds trust.

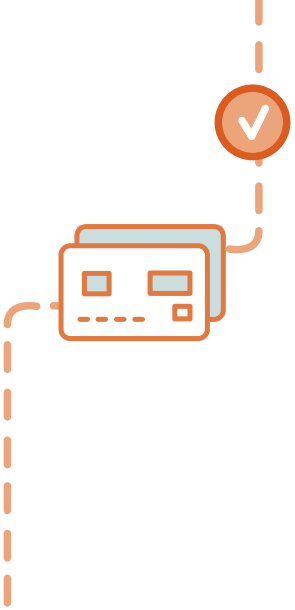
It is unlikely that useful information will be shared among participants without a trust relationship. Whoever takes on the responsibility for setting up the ISAC should therefore make sure that trust is built into the set-up process from the very initial (developmental) stages of the ISAC.

It is also important to identify and delineate the kind of information that will be shared. A taxonomy or a set of rules should be developed to foster the information-exchange process. In most cases, it is not recommended that information be shared in a free format, where it is difficult to classify information based on relevant categories and rules. As a result, a specific lexicon of terms for classification is recommended.

Before an ISAC is set up, all members should be bound by certain rules that govern the operation of the ISAC. This will ensure that each participant understands the responsibility that has been assumed (taken on) by taking part in the information-exchange mechanism.

External Database for Operational Risk Loss

In certain cases, FPS operators and service providers may consider joining a data exchange for operational risk loss that consists of an external loss database for operational risk–related events. This may be especially beneficial if joining or developing a sector-specific ISAC is impossible. While becoming a member of data exchange for operational risk loss may seem too broad and extensive, an operational loss database offers a wide array of operational risk data that may include detailed information on cyber threats and cyber risk events. A data exchange for operational risk loss can also function as a complementary source of information if the operator or service provider is already a member of an ISAC.



APPENDIX H

FAST PAYMENT SYSTEMS AND PCI DSS

The contemporary, globalized environment of the 21st century has facilitated tremendous growth in both economic activity and electronic commerce. A financial institution such as an FPS operator or a PSP is a complex organization that stores a wide range of confidential information in a diverse set of electronic information systems. The Payment Card Industry Data Security Standard (PCI DSS) offers a comprehensive framework for securing information systems. While the main objective of the standard revolves around the protection of cardholder-related data, information, and processes, the standard can be leveraged by fast payment operators and service providers to secure payment systems. PCI DSS is based on six control objectives and 12 related requirements (principles) that an organization should fulfill. Table H1 lists the control objectives in addition to the associated requirements that need to be considered within the scope of the standard.

A payment system operator or service provider typically needs to perform considerable planning and assessment before deciding on the network security controls to deploy organizationwide. PCI DSS contains relevant requirements upon which the internal controls may be based. Putting the size and complexity of the organization aside, there are several important, universal principles to consider when designing a secure network. `

One key aspect for providing an adequate level of security is defense in depth. Security controls of different types should be used to complement each other. The main assumption behind the deployment of diverse (and layered) information security controls is that what may be missed by one control can potentially be caught by a different, complementary control. For example, a perimeter network firewall may not detect a particular form of malware, whereas an IPS may be able to stop the same malware if deployed in conjunction with the firewall. Additionally, the principle of "defense in multiple places" may be used. This implies that security controls should be placed in different locations on the network and within IT systems.

Various other domains of the PCI DSS can be transposed to fit the cybersecurity requirements of FPS. While protecting cardholder data may not be directly relevant for FPS, securing both consumer- and employee-related data and information is critical. Additionally, maintaining a vulnerability-management program that includes vulnerability assessments is important. A vulnerability assessment consists of a methodical review of security to verify that no predictable and unaddressed attack vectors (such as unnecessarily open ports or services) could be used to compromise a payment system environment, intentionally or unintentionally. The scope of an assessment may range from a single payment system or application to an entire facility or end-to-end business process. The purpose of a vulnerability assessment is to deliver information to management that can be used both to understand the effectiveness of the risk-management program and to make decisions regarding the treatment of identified vulnerabilities, such as the implementation of new controls. Conducting regular vulnerability assessments should be an inseparable part of the risk-management process of both FPS operators and FPS service providers.

TABLE H1 **PCI DSS Control Objectives and Requirements**

CONTROL OBJECTIVES	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability-management program	5. Use and regularly update antivirus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement strong access-control measures	7. Restrict access to cardholder data by business need to know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Monitor and test networks regularly	10. Track and monitor all access to network resources and cardholder data
	11. Test security systems and processes regularly

Likewise, conducting penetration tests is increasingly becoming a necessity for digitally enabled organizations. A penetration test is a targeted attempt to break into an environment. As with a vulnerability assessment, the target of a penetration test may be a system, application, facility, or end-to-end business process. Domains four, five, and six of PCI DSS can also be directly relevant for FPS. This includes the implementation of strong access controls and maintaining the principle of least privilege, monitoring and testing networks regularly via the use of operational key risk indicators and key performance indicators, and maintaining a credible information security policy, which is updated regularly and as needed. At the same time, the use of encryption is an additional dimension where PCI DSS may be relevant for fast payment operators and service providers. This includes the use of digital signatures to ensure the integrity of payments and protect transactional (and other) data that is either traveling over networks or being stored within the payment ecosystem.

Last but not least, another concept to consider is the compartmentalization of information. Payment system resources of varying sensitivity levels typically need to be placed in separate security zones. Devices and information systems that provide services to the outside world (such as internet-based payment apps) are usually placed in a security zone separate from the internal network. Furthermore, strategic, and mission-critical information systems should logically be located in dedicated security zones. It is also worth mentioning that servers with low trust levels, such as remote access servers, must be segregated in a similar manner as the strategic and mission-critical information systems.

ENDNOTES

1. https://fastpayments.worldbank.org/sites/default/files/2021-10/Oversight_Final_0.pdf
2. https://fastpayments.worldbank.org/
3. https://www.worldbank.org/en/topic/financialinclusion/brief/gpss
4. https://www.worldbank.org/en/topic/digital/brief/cybersecurity
5. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability
6. https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf
7. https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/
8. https://www.centralbank.org.ls/images/Public_Awareness/Press_Release/Cyber_Security_Incident_CBL.pdf
9. https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf
10. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622
11. https://fastpayments.worldbank.org/sites/default/files/2021-10/Cross_Border_Fast_Payments_Final.pdf
12. https://www.bis.org/cpmi/publ/d146.pdf
13. Laudon, K.C., and J.P. Laudon. 2012. *Management Information Systems: Managing the Digital Firm.* Prentice Hall.
14. https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
15. https://www.swift.com/myswift/customer-security-programme-csp
16. https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075
17. https://www.weforum.org/agenda/2024/07/global-outage-it-cyber-resilience-alarm-world/
18. Gaur, R., and A. Diamond. 2024. "Digital Public Infrastructure Can Bring Enormous Benefits—or Pose Significant Risks. Safeguards Make the Difference." Digital Impact Alliance, July 24, 2024, https://dial.global/dpi-can-bring-benefits-or-risks-safeguards-make-the-difference/.
19. https://fastpayments.worldbank.org/sites/default/files/2021-10/QR_Codes_in_Payments_Final.pdf
20. IMF. 2024. *Global Financial Stability Report.* Washington, DC: International Monetary Fund, April 2024.
21. IMF. 2024. *Global Financial Stability Report.* Washington, DC: International Monetary Fund, April 2024.
22. Kaspersky. 2023. "200,000 New Mobile Banking Trojan Installers Discovered, Double from 2021." Press release, February 27, 2023, https://www.kaspersky.co.uk/about/press-releases/200000-new-mobile-banking-trojan-installers-discovered-double-from-2021.
23. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
24. ://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident.pdf {~?~URL OK?}
25. Stallings, W., and L. Brown. 2014. *Computer Security: Principles and Practice,* 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
26. https://www.zimperium.com/resources/zimperiums-2023-mobile-banking-heists-report-finds-29-malware-families-targeted-1800-banking-apps-across-61-countries-in-the-last-year/
27. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
28. https://thedocs.worldbank.org/en/doc/189821576699037673-0130022019/original/FIGIECBOperationalCyberFinalWeb1213.pdf
29. Westerman, G., and R. Hunter. 2007. *IT Risks: Turning Business Threats into Competitive Advantage.* Boston, MA: Harvard Business School Press.
30. https://www.worldbank.org/en/topic/financialinclusion/brief/gpss
31. ISACA. 2013. *COBIT 5 for Risk.* Rolling Meadows, IL: ISACA.
32. https://csrc.nist.gov/files/pubs/sp/800/34/r1/upd1/final/docs/sp800-34-rev1_bia_template.docx
33. ENISA. 2017. *Information Sharing and Analysis Centres (ISACs): Cooperative Models.* Heraklion, Greece: European Union Agency for Network and Information Security.
34. https://www.worldbank.org/en/topic/financialinclusion/brief/gpss
35. Richardson, R. 2010. *2010/2011 Computer Crime and Security Survey.* New York, NY: Computer Security Institute.
36. Information systems comprise five areas: applications (programs), hardware, databases, networks, and people.
37. https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf
38. Maurer, T., and A. Nelson. 2020. *International Strategy to Better Protect the Financial System against Cyber Threats.* Washington, DC: Carnegie Endowment for International Peace.
39. https://www.nist.gov/cyberframework
40. https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf
41. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
42. Williams, B.R., and A. Chuvakin. 2012. *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance,* 3rd ed. Waltham, MA: Syngress.
43. https://fastpayments.worldbank.org/sites/default/files/2023-09/Customer%20Authentication%202.0_August%2031_Final.pdf

44. https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq
45. https://fastpayments.worldbank.org/sites/default/files/2021-10/QR_Codes_in_Payments_Final.pdf
46. https://www.emvco.com/specifications/
47. https://www.iso.org/standard/80988.html
48. Stallings, W., and L. Brown. 2014. *Computer Security: Principles and Practice,* 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
49. https://fastpayments.worldbank.org/sites/default/files/2023-09/Customer%20Authentication%202.0_August%2031_Final.pdf
50. Banco de México. n.d. "Interbanking Electronic Payment System (SPEI®) Characteristics," https://www.banxico.org.mx/services/spei_-transfers-banco-mexico.html.
51. Rebill. n.d. "What Is SPEI?," https://www.rebill.com/en/glossary/what-is-spei.
52. Carnegie Endowment for International Peace. n.d. "Timeline of Cyber Incidents Involving Financial Institutions," https://carnegieendowment.org/features/fincyber-timeline.
53. Carnegie Endowment for International Peace. n.d. "Timeline of Cyber Incidents Involving Financial Institutions," https://carnegieendowment.org/features/fincyber-timeline.
54. Banco de México. 2018. *Reporte de análisis forenses.* Banco de México, August 29, 2018, https://www.banxico.org.mx/spei/d/%7B4A977A24-0889-3F24-A717-DF9DBBA118C1%7D.pdf.
55. Banco de México. 2018. *Reporte de análisis forenses.* Banco de México, August 29, 2018, https://www.banxico.org.mx/spei/d/%7B4A977A24-0889-3F24-A717-DF9DBBA118C1%7D.pdf.
56. https://www.nist.gov/cyberframework
57. https://www.iso.org/standard/75652.html
58. https://www.iso.org/standard/75106.html
59. https://www.iso.org/standard/71670.html
60. https://www.iso.org/standard/80988.html
61. https://www.isaca.org/resources/cobit
62. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
63. https://www.ncsc.gov.uk/collection/10-steps?s=09
64. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
65. https://www.bis.org/cpmi/publ/d146.pdf. FSB Effective Practices for Cyber Incident Response and Recovery (2019) https://www.fsb.org/uploads/P191020-1.pdf
66. Stallings, W., and L. Brown. 2014. *Computer Security: Principles and Practice,* 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
67. The full English version of the threat checklist has been published in T.R. Peltier, Information Security Risk Analysis, 3rd ed. (Boca Raton, FL: Auerbach Publishers, 2010)


WORLD BANK GROUP