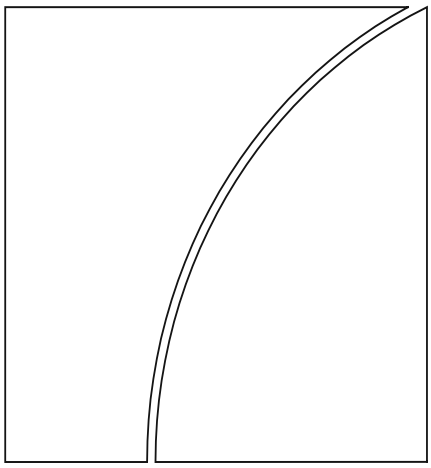
Financial Stability Institute

FSI Insights

on policy implementation

No 50



Banks' cyber security – a second generation of regulatory approaches

By Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio

June 2023

JEL classification: G21, G28, O33

Keywords: cyber risk, cyber security, cyber resilience, operational resilience

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-249X (online)
ISBN 978-92-9259-663-7 (online)

Contents

Executive summary 4

Section 1 – Introduction 6

Section 2 – International regulatory initiatives 8

Section 3 – Design of cyber resilience regulations 11

Section 4 – Key regulatory requirements for cyber resilience 14

- Cyber security strategy and governance 14
- Cyber incident response and recovery 16
- Cyber incident reporting and threat intelligence-sharing 17
- Cyber resilience testing 18
- Cyber hygiene 20
- Third-party dependencies 20
- Cyber security culture and awareness 23
- Cyber security workforce 23
- Cyber resilience metrics 24

Section 5 – Conclusion 24

References 26

Banks' cyber security – a second generation of regulatory approaches[1]

Executive summary

Cyber resilience continues to be a top priority for the financial services industry and a key area of attention for financial authorities. This is not surprising given that cyber incidents pose a significant threat to the stability of the financial system and the global economy. The financial system performs a number of key activities that support the real economy (eg deposit taking, lending, payments and settlement services). Cyber incidents can disrupt the information and communication technologies that support these activities and can lead to the misuse and abuse of data that such technologies process or store. This is complicated by the fact that the cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions. Moreover, the cost of cyber incidents has continuously and significantly increased over the years.

This paper updates Crisanto and Prenio (2017) by revisiting the cyber regulations in the jurisdictions covered in that paper, as well as examining those issued in other jurisdictions. Aside from cyber regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, Philippines, Rwanda, Saudi Arabia and South Africa. The jurisdictions were chosen to reflect cyber regulations in both advanced economies (AEs) and emerging market and developing economies (EMDEs). This highlights the fact that since 2017 several jurisdictions – including EMDEs – have put cyber regulations in place.

There remain two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations and the second involves issuing comprehensive regulations. The first approach takes as a starting point regulations on operational risk, information security etc and add cyber-specific elements to them. Here, cyber risk is viewed as any other risk and thus the general requirements for risk management, as well as the requirements on information security and operational risks, also apply. This approach is more commonly observed in jurisdictions that already have these related regulations firmly established. The second approach seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation. In both approaches, to counter the risks that might result from having too much prescriptiveness in cyber regulations, some regulations combine broad cyber resilience principles with a set of baseline requirements. Regardless of the regulatory approach taken, the proportionality principle is given due consideration in the application of cyber resilience frameworks.

Whether as part of related regulations or separate comprehensive ones, recent cyber security policies have evolved and could be described as "second-generation" cyber regulations. The "first generation" cyber regulations, which were issued mainly in AEs, focused on establishing a cyber risk management approach and controls. Over the last few years, authorities, including those in EMDEs, have issued new or additional cyber regulations. These second-generation regulations have a more embedded "assume breach" mentality and hence are more aligned with operational resilience concepts. As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

[1] Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org) and Jermy Prenio (Jermy.Prenio@bis.org), Bank for International Settlements, Jefferson Umebara Pelegrini (jefferson.pelegrini@bcb.gov.br), Central Bank of Brazil. We are grateful to Kaspar Köchli and Jatin Taneja for research assistance, and to Markus Grimpe and staff at covered authorities for helpful comments. Esther Künzi and Theodora Mapfumo provided valuable administrative support.

The "second-generation" regulations leverage existing policy approaches to provide additional specific guidance to improve cyber resilience. Cyber security strategy, cyber incident reporting, threat intelligence sharing and cyber resilience testing are still the primary focus of the newer regulations. Managing cyber risks that could arise from connections with third-party service providers has become a key element of the "second generation" cyber security framework. Moreover, there are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks. In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced in a few jurisdictions.

Authorities in EMDEs tend to be more prescriptive in their cyber regulations. Cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing are some of the areas where EMDE authorities provide prescriptive requirements. This is approach seems to be connected to the need to strengthen the cyber resilience culture across the financial sector, resource constraints and/or the lack of sufficient cyber security expertise in these jurisdictions. Hence, EMDE authorities may see the need to be clearer in their expectations to make sure banks' boards and senior management invest in cyber security and banks' staff know exactly what they need to do.

International work has resulted in a convergence in cyber resilience regulations and expectations in the financial sector, but more could be done in some areas. Work by the G7 Cyber Expert Group (CEG) and the global standard-setting bodies (SSBs) on cyber resilience has facilitated consistency in financial regulatory and supervisory expectations across jurisdictions. This is necessary given the borderless nature of cyber crime and its potential impact on global financial stability. Another area where there might be scope for convergence is the way in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics. Lastly, there might be scope to consider an international framework for critical third-party providers, in particular cloud providers, given the potential cross-border impact of a cyber incident in one of these providers.

Section 1 – Introduction

1. **Cyber risk[2] is a significant threat to the stability of the financial system and the global economy.** The financial system performs a number of key activities that support the real economy (eg deposit taking and lending, payments and settlement services). Cyber incidents[3] have been shown to disrupt these activities by affecting the information and communication technologies (ICT) that financial firms extensively rely on and the data they process. Within the financial sector, banks typically have the most public-facing products and services. Their multiple points of contact with outside parties result in significant vulnerabilities to cyber attacks and could be used as entry points for attacks that can culminate in relevant disruptions to the financial system.

2. **The cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions.** Interpol (2022) reports ransomware, phishing, online scams and computer hacking as the highest cybercrime threats globally.[4] Moreover, the complexity of the cyber threat landscape has increased due to the strong impact of geopolitics on cyber operations, especially since the Russia-Ukraine war began, with distributed denial of service (DDoS) being used as a cyber warfare tool.[5] There is also a resurgence of hacktivism with greater technical sophistication and state support as well as an increase of deepfake-enabled fraud.[6] With respect to the increasing dependency of larger parts of the financial system on cloud providers, CrowdStrike (2023) reports "a larger trend of eCrime and nation-state actors adopting knowledge and tradecraft to increasingly exploit cloud environments".

3. **The cyber threat landscape is also characterised by a significant and continuous rise in the cost of cyber incidents.** Statista (2023) estimated the global cost of cyber crime in 2022 at $8.4 trillion and expects this to go beyond $11 trillion in 2023. This reflects an annual increase of 30% in the cost of cyber crime during the 2021-23 period.[7] Moreover, the average cost of a data breach between 2020 and 2022 increased by 13%, with the financial industry scoring the second highest average cost after healthcare at $6 million.[8] According to Chainalysis (2022), 2022 was the biggest year ever for crypto hacking, with $3.8 billion stolen from cryptocurrency businesses. Cyber insurance demand continues to outweigh supply and that the cyber protection gap appears to be widening amid a market characterised by rising premiums, narrowing coverage and tighter underwriting standards.[9]

4. **In the light of the above developments, it is unsurprising that cyber resilience[10] continues to be a top priority for the financial services industry.** According to EY-IIF (2023), most chief risk officers (CROs) consider cyber risk the top threat to the banking industry and "the most likely to result in a crisis

2 FSB (2018) defines cyber risk as as the combination of the probability of cyber incidents occurring and their impact.

3 FSB (2018) defines cyber incidents as events (whether resulting from malicious activity or not) that: (i) jeopardise the confidentiality, integrity and availability of an information system or the information the system processes, stores or transmits; or (ii) violate the security policies, security procedures or acceptable use policies.

4 Interpol (2022) also reported that those types of cyber crime are expected to increase in the next three to five years. Phishing attacks related to cryptocurrency increased by over 250% year on year. See Interisle Consulting Group (2022).

5 See ENISA (2022).

6 See Moody's Investor Service (2022).

7 Admittedly, this is lower in comparison with the 50-60% increase observed during the 2019-21 period at the height of the global pandemic and lockdown.

8 See IBM (2022).

9 IAIS (2023).

10 As defined by FSB (2018), cyber resilience refers to an organisation's the ability to continue to carry out its mission by anticipating and adapting to *cyber threats* and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incidents*.

or major operational disruption". Despite the significant resources invested in enhancing cyber resilience, CROs highlight two main challenges related to effectively managing cyber risk: (i) its inherent presence in every line of business, in day-to-day operations and across extensive networks of partners, suppliers and service providers on which banks increasingly depend; and (ii) the increasing sophistication of hacking tools and techniques. As a result, CROs expect to pay the most attention to cyber risk in the next 12 months and consider it the top strategic risk for the next three years. A more general aspiration highlighted by the industry is to design more consistent and coordinated regulations across jurisdictions in a way that enhances global cyber resilience and reduces regulatory fragmentation.[11]

5. **Strengthening cyber resilience is also a key focus for the official sector, including central banks and supervisory authorities.** Cyber crime is widely regarded as a national defence priority and several jurisdictions have put in place national policies or frameworks to strengthen the cybersecurity[12] of critical sectors and institutions.[13] From the perspective of central banks' own management of cyber risk, many have notably increased their cyber security-related investments since 2020, giving priority to technical security control and resiliency, and are collaborating within the framework provided by the BIS' Cyber Resilience Coordination Centre (CRCC).[14] Moreover, the central banking community is developing analytical frameworks to understand the channels through which cyber risk can grow from an operational disruption into a systemic event.[15] Finally, an increasing number of jurisdictions have issued cyber-specific guidelines for the financial sector and cyber resilience features prominently in the work-programmes of global standard-setting bodies (SSBs) and other international bodies (see Section 2).

6. **Cyber security is considered a top priority for banking supervisors worldwide**. Within the financial sector, bank authorities have been particularly active in coming up with regulatory and supervisory frameworks to enhance the banking sector's resilience to cyber attacks. This reflects the fact that cyber security features prominently in the work programme of banking supervisors in both advanced economies (AEs) and emerging markets and developing economies (EMDEs) (see Graph 1). This graph also suggests that the top priority attached to cyber security and operational resilience more broadly is correlated with supervisory work on digitalisation of the financial system and its impact on banking business models. In Europe for example, the ECB Banking Supervision published its supervisory priorities for 2023-25 in December 2022, that includes addressing deficiencies in operational resilience frameworks, namely IT outsourcing and IT security/cyber risks.[16]

[11] See IIF (2023).

[12] According to FSB (2018), cyber security mainly refers to the preservation of *confidentiality, integrity* and *availability* of information and/or *information systems* through the *cyber medium*.

[13] For instance, Singapore's Cybersecurity Strategy; Canada's Cybersecurity Standard; the US Department of Homeland Security's different initiatives to protect US critical infrastructure; South Africa's National Cybersecurity Policy Framework (NCPF); and Critical Infrastructure Protection in France.

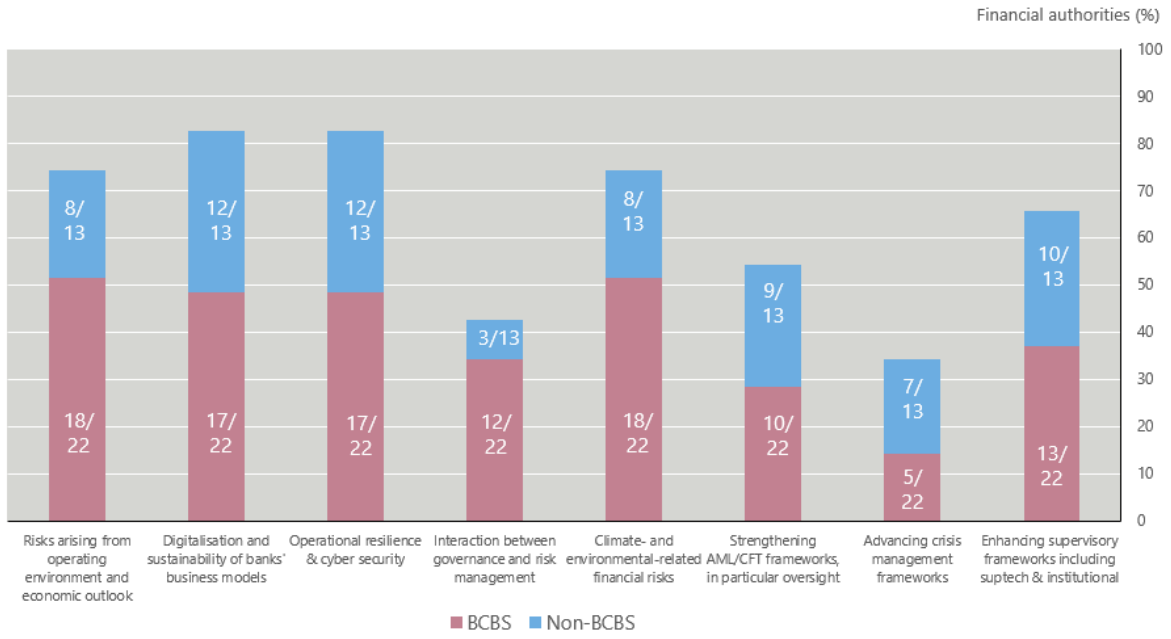
[14] See Doerr (2022) and a description of CRCC activities in the BIS's *Annual Report 2021*.

[15] For example, ECB's "Towards a framework for assessing systemic cyber risk" in its *Financial Stability Review*, November 2022; European Systemic Risk Board, *Systemic cyber risk*, February 2020; US Office of Financial Research, *Cybersecurity and financial stability: risks and resilience*, February 2017.

[16] See ECB (2022).

Main regulatory and supervisory priorities in BCBS and non-BCBS member authorities in 2023

Graph 1



Note: Analysis based on public information and includes a total of 35 banking authorities: 22 BCBS-member authorities and 13 non-BCBS member authorities.

7. **This paper updates Crisanto and Prenio (2017) by revisiting cyber security regulations in jurisdictions covered in that paper, as well as examining those issued in other jurisdictions.** Aside from cyber security regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper also covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, the Philippines, Rwanda, Saudi Arabia and South Africa. The jurisdictions were chosen to reflect cyber regulations in both AEs and EMDEs. This highlights the fact that since 2017, a number of jurisdictions – including in EMDEs – have put in place or enhanced cyber regulations. It should be noted, however, that based on an IMF survey of 51 EMDEs, 42% still lack a dedicated cybersecurity or technology risk-management regulation.[17] Section 2 provides the international context in which these regulations have evolved. Section 3 describes the different approaches in the design of cyber regulations. Section 4 presents the key cyber regulatory requirements. Section 5 concludes.

Section 2 – International regulatory initiatives

8. **Cyber resilience features prominently in the work programme of SSBs.** Given the borderless nature of cyber crime and its potential impact to global financial stability, cyber resilience requires international cooperation[18] and has therefore featured prominently in the work programme of SSBs,

[17] Adrian and Ferreira (2023).

[18] According to FSB (2017a), cyber risk is one of the top three priority areas for international cooperation.

including the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS) and the International Organization of Securities Commissions (IOSCO). This work aims to achieve greater convergence of cyber resilience approaches mainly through principles-based guidance and practical toolkits. Convergence has been facilitated by the use of common language through the FSB's cyber lexicon, which was published in 2018 and updated in 2023.

9. **The G7 Cyber Expert Group (G7 CEG) also plays an important role in enhancing cyber resilience practices in the financial sector.** The G7 CEG was set up in 2015 to identify the main cyber security risks in the financial sector and propose actions to be taken in this area across G7 jurisdictions, including on cyber security policy coordination.[19] The G7 CEG recommendations aim to reflect policy approaches, industry guidance, and best practices in place throughout its member jurisdictions. While their primary focus is on private sector financial entities, they can be of help for financial authorities' own institutional work on cyber resilience and their efforts to promote this resilience across the financial sector. That said, the G7 CEG recommendations are non-binding, non-prescriptive and designed to be tailored to individual risk profiles and threat landscapes as well as to country-specific legal and regulatory frameworks. Graph 2 provides a summary of the main SSB and G7 CEG work that is helping to facilitate international convergence of cyber regulations in the financial system.

10. **SSBs generally emphasise the importance of cyber resilience as part of their efforts to enhance the operational resilience of the financial sector.** The dramatic growth of technology-related threats and the Covid-19 pandemic brought to the forefront the need to enhance the ability of financial institutions to deal with operational risk-related events that could cause significant disruptions in the financial markets, including cyber incidents. With this aim, the BCBS issued Principles for Operational Resilience in 2021[20] to facilitate banks' ability to withstand, adapt to and recover from those severe adverse events. A key element of the Principles is ensuring a resilient ICT framework, including cyber security, to fully support and facilitate the delivery of the bank's critical operations.[21] The 2021 BCBS *Newsletter on cybersecurity* not only highlights the interaction between operational resilience and cyber security but also the need to align cyber risk management with widely accepted industry standards.[22]

11. **The CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (FMIs) has become a key point of reference for the financial sector when designing a sound framework to address cyber risk.** This cyber guidance was published in 2016 with the purpose of supplementing the 2012 Principles for FMIs. As such, it sets out additional details related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities.[23] The cyber guidance focuses on five cyber risk management categories: governance; identification; protection; detection; and response and recovery. It also envisages three overarching components to be addressed across the cyber resilience framework: testing; situational awareness; and learning and evolving. More recently, CPMI and IOSCO have focused their attention on assessing the level of adoption of their guidance by financial market infrastructures and the results have highlighted the challenges related to the development of adequate response and recovery plans to deal with severe cyber incidents.

[19] Additional G7 actions include information sharing, testing and incident response.

[20] These Principles build on the Committee's *Revisions to the principles for the sound management of operational risk*, and draw on previously issued principles on corporate governance for banks, as well as outsourcing, business continuity and relevant risk management-related guidance (BCBS, 2021).

[21] See Principle 7 – ICT Including cyber security.

[22] In addition, building upon previous work, the IAIS released a draft "Issues paper on insurance sector operational resilience" in 2022 where the issue of insurer cyber resilience featured prominently.

[23] The 2016 Cyber guidance provides supplemental information, primarily with respect to the following 2012 PFMI Principles: governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).

12. **The G7 CEG's *Fundamental elements of cyber security* is another common point of reference for developing and implementing a strong cyber resilience framework.** This 2016 guidance has played a pivotal role in providing financial institutions and authorities with building blocks to design and implement sound cyber security policies and practices. These include eight fundamental elements that rely on an appropriate cyber security strategy and framework; effective governance structure; thorough evaluation of cyber risks and respective controls across the business; systematic monitoring of processes to rapidly detect cyber incidents (eg testing and audit); timely incident response and recovery; timely sharing of relevant information; and periodic update of fundamental elements in line with the evolving threat landscape. To assess how effectively these elements are being implemented, the G7 CEG issued tools in 2017 that describe desirable outcomes and components to evaluate progress in enhancing cyber security.

13. **With regards to specific components of cyber resilience, the FSB work has focused on cyber incident response and recovery as well as on cyber incident reporting.** In 2020, the FSB issued a final report that provides a toolkit to guide financial institutions response to and recovery from a cyber incident in a way that limit any related financial stability risks. Since this requires timely and accurate information on cyber incidents, the FSB issued recommendations in 2023 to address impediments to achieving greater convergence in cyber incident reporting, including proposing a concept for a common format for incident reporting exchange (FIRE) to address operational challenges arising from reporting to multiple authorities and to foster better communication.

14. **The G7 CEG has provided additional guidance to assess the effectiveness of cyber resilience measures and to address ransomware threats.** In 2018, the G7 CEG further elaborated on its fundamental elements of cyber security by providing financial sector firms with a guide for assessing their resilience to malicious cyber incidents through simulation and a guide for financial sector authorities considering the use of threat-led penetration testing (TLPT) within their jurisdictions. Moreover, recognising the need for clearly defined and regularly rehearsed response and recovery procedures in case of disruptive cyber events, the G-7 CEG developed tools in 2020 to guide the establishment of cyber exercise programmes with internal and external stakeholders. These tools could also serve as guide for establishing cyber exercise programmes across jurisdictions and sectors. Additionally, to deal with the recent growth of ransomware threat in the financial sector, the G7 CEG issued key considerations in 2022 that are essential to address this threat.

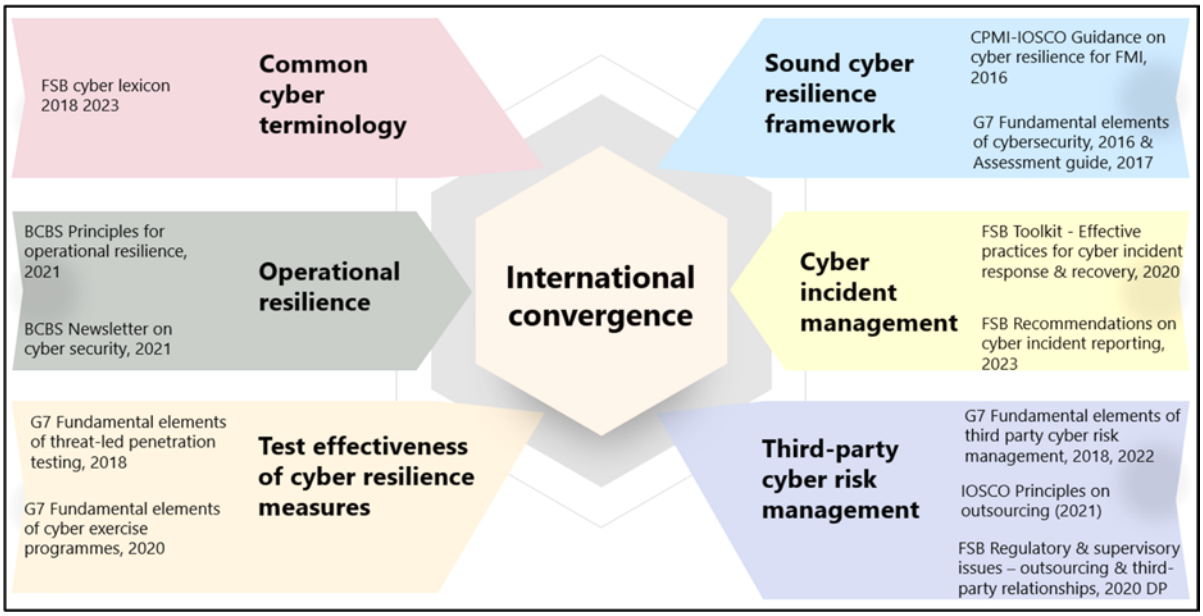
15. **Enhancing third-party cyber risk management has also been part of the work programme of the G7 CEG and FSB.** The use of third parties generally introduces additional cyber risks that need to be well managed. In 2018, the G7 CEG issued the fundamental elements that needed to be considered throughout the third-party cyber risk management life cycle not only within an individual entity but also as part of the system-wide monitoring of cyber risk, including for the purposes of cross-sectoral coordination. In 2022, the G7 CEG revised these fundamental elements to reflect the latest financial industry developments, most notably the expanded reliance on ICT providers and the need to effectively manage ICT supply chain-related cyber exposures. Complementing this work, the FSB's work programme for 2023 includes releasing a consultative document aimed at strengthening financial institutions' ability to manage third-party and outsourcing risk.

16. **The IAIS (2023) reports that cyber insurance only covers a small proportion of the potential economic cost resulting from cyber events.** Insurers are not only exposed to cyber risks in their operations but are also active takers of cyber risk through their cyber underwriting activities. Regarding the latter, the 2020 IAIS Cyber Risk Underwriting Report concluded that cyber underwriting practices, while serviceable, were not yet optimal, particularly due to challenges surrounding the measurement of risk exposures and clarity of cyber insurance policies. In view of this, the report recommended proactive supervisory attention to facilitate the monitoring, understanding and assessment of cyber risk underwriting exposure and impact; as well as enhancing the corresponding supervisory expertise.

17. **More generally, SSBs have devoted resources to increase the mutual understanding of their members of their individual efforts to strengthen cyber resilience.** This has mainly taken the form of stock-taking of cyber security regulations, guidance and supervisory practices. Examples of this work are the 2017 FSB report *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*[24], which was conducted with FSB member jurisdictions, and the 2018 BCBS report entitled *Cyber-resilience: range of practices,* which describes and compares the range of regulatory and supervisory cyber resilience practices across BCBS member jurisdictions. Another relevant example is the 2019 report from the IOSCO Cyber Task Force. This report examines how IOSCO member jurisdictions are using internationally recognised cyber frameworks and how these frameworks could help address any gaps identified in IOSCO members' current regimes rather than proposing any new guidance.

Main SSB and G7 CEG work that is facilitating the international convergence of cyber regulations in the financial system

Graph 2



Section 3 – Design of cyber resilience regulations

18. **There are two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations, and the second involves issuing comprehensive cyber regulations.** In the first approach, existing related regulations (eg regulations on operational risk management, IT risk management, outsourcing) are enhanced to include cyber-specific elements. This approach views cyber risk as any other risk and thus the general requirements for risk management (eg governance, setting of risk appetite), and the requirements on IT, information security and operational risks, also apply. As a result, this approach facilitates strong alignment with regulatory expectations on enterprise risk management and operational risk including operational resilience. This approach is more commonly observed in jurisdictions (eg the United States and Europe) that already have established regulations on operational risk management, business continuity, information security and/or information

[24] FSB (2017b).

technology risk management. The second approach, on the other hand, seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation. This is the case for example in México and in South Africa's public consultation on Joint Standard on Cybersecurity and Cyber Resilience Requirements.

19. **In either approach, there is a risk that regulations could become too prescriptive or result in inefficiencies.** The risk exists that regulation becomes too prescriptive, so that it falls behind both the constantly evolving threat from cyber risk and advances in cyber risk management. There is also a risk of creating inefficiencies and silos. Comprehensive cyber regulations, in particular, might result in financial institutions establishing governance and risk management frameworks for cyber risk and resilience that are separate from their enterprise-wide frameworks.

20. **To counter the risk of too much prescriptiveness, there is an emerging regulatory approach that seeks to combine broad cyber resilience principles with a set of baseline requirements.** This approach focuses more on "what expectations to achieve" and less on "how to achieve them".[25] It supports a regulatory framework that is flexible enough to be adapted to the dynamic and evolving nature of cyber risk while having clear supervisory expectations with respect to the core aspects of governance and risk management that aim to enhance cyber resilience. For example, the Australian Prudential Regulation Authority (APRA) published the Prudential Practice Guide CPG 234 Information Security, providing detailed expectations regarding the requirements established in Prudential Standard CPS 234 – Information Security.

21. **Finding the right level of prescription when developing cyber resilience regulations is challenging.** While prescriptive rules may be necessary in some areas, for example, by requiring banks' boards to establish a cyber risk management framework and risk appetite, other areas are clearly less suitable for specific rules and it is important to prevent regulations from falling behind both the constantly evolving threat from cyber risk and advances in cyber risk management. For example, given the rate of technological change, any regulation that prescribes the use of a specific technology is likely to become rapidly outdated and ineffective.[26] Mandating a specific recovery time is another example where regulators need to be careful how banks go about implementing it. The aim is to prevent the lengthy disruption of critical financial operations, but an excessively stringent and rigid recovery time may prove counterproductive if this comes at the expense of banks' ability to thoroughly check that all their systems are no longer compromised. Regulations that are very prescriptive may also result in a compliance-based approach to dealing with cyber risk.

22. **Whether as part of related regulations or separate comprehensive ones, a distinction can also be made between "older" (first generation) and "newer" (second generation) cyber regulations.** Authorities recognise that cyber risk management is constantly evolving. Hence, the focus of the first generation and second generation of cyber regulations are somewhat different. The first generation focused on establishing a cyber risk management approach and defining requirements on typical security controls (eg, access controls and vulnerability analysis). The second generation goes one step further, emphasising the need to develop capabilities (e.g., cyber incident management, cyber incident reporting and third-party risk management) essential to ensure a financial institution's cyber resilience in an increasingly digital financial system. Authorities are also continuously thinking of ways to improve their cyber regulations. They could, for example, focus on the establishment of business continuity arrangements involving coordination between relevant financial institutions to respond to systemic crises caused by cyber incidents.

[25] See Wilson et al (2019).

[26] See Gracie (2014).

23. **Regardless of the regulatory approach taken, the application of the proportionality principle is given due consideration in the application of cyber resilience frameworks**. Proportionality is defined as the application of simplified prudential rules to smaller and less complex banks to avoid excessive compliance costs without undermining key prudential safeguards.[27] Translating this concept to the cyber security world is challenging, given that exposure to cyber risk depends not only on a bank' size and complexity but also on how it uses technology and how it provides its products and services using digital channels, as well as the level of financial sector interconnectedness. Authorities are aiming to identify key aspects of cyber resilience governance and risk management that should apply to all supervised firms regardless of traditional indicators used to group peer banks. At the same time, other authorities such as the Peruvian Superintendency of Banks and Private Pension Funds apply a proportionality framework in which systemically important banks are subject to heightened cyber resilience requirements reflecting their potential financial stability risks. Table 1 provides a comparative description of the first and second generation of cyber regulations.

24. **Supervisory assessments of cyber security capabilities tend to use existing technical standards for cyber and information security as a valuable point of reference.** Jurisdictions take industry standards into account when developing their regulatory and supervisory frameworks. Credible technical standards provide essential knowledge of practices and controls for managing cyber and technological risks. Examples of influential technical standards in the cyber/information security community include:

- the US National Institute of Standards and Technology (NIST) *Cyber security framework*;
- the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standards – in particular the ISO/IEC 27000 series on information security management, ISO 22301 on security and resilience and ISO 31000 on risk management;
- ISACA's Control objectives for information technologies (COBIT) framework for IT governance and management; and
- the Center for Internet Security (CIS) Controls.

[27] See Castro Carvalho et al (2017).

Comparative description of the first and second generation of cyber regulations. Table 1

	1st generation (2017 paper)	2nd generation (2023 paper)
Conceptual underpinning	Focus on building "strong perimeter"	More embedded "assume breach" mentality
Scope	Aligned with IT/ICT and information security framework	In addition, aligned with operational resilience framework
Requirements	Emphasis on enhancing security capabilities	Emphasis on improving resilience capabilities
	Guidance/expectations regarding cyber risk management and (typical) security controls	In addition, guidance/expectations regarding key aspects of cyber resilience framework
	Third-party dependencies largely managed through outsourcing lens	Third-party dependencies increasingly becoming a key part of cyber resilience framework
Types of rules	(i) Leverage existing regulations and (ii) "all-in-one" cybersecurity frameworks	In addition, (iii) principles plus baseline requirements
Tailoring	Apply proportionality approach	
References	In addition to SSB & G7 guidance, well-established technical standards on cyber & information security	

Section 4 – Key regulatory requirements for cyber resilience

25. **As mentioned in Section 3, regulators in different jurisdictions have two broad ways of communicating their cyber security requirements or expectations.** Some regulators issue "all-in-one" regulations that encompass all aspects of cyber security. Other regulators insert cyber security requirements in various relevant regulations (eg, relating to IT, third party service providers). In both cases, regulations share a high degree of commonality, which is expected given that these are based on international regulatory and industry standards. This section discusses key regulatory requirements and expectations – whether they are found in "all-in-one" regulations or inserted in relevant regulations – in the areas of cyber security strategy and governance; cyber incident response and recovery; cyber incident reporting and threat intelligence sharing; cyber resilience testing; cyber hygiene; third-party dependencies; cyber security culture and awareness; cyber security workforce; and cyber resilience metrics.

Cybersecurity strategy and governance

26. **An increasing number of regulators, particularly in EMDEs, require banks to develop specific cyber security "strategies".**[28] However, regulations may not explicitly call them strategies but may refer to them as "policies", "programmes" or "frameworks". Such regulatory requirements typically follow the cyber security framework advocated in CPMI-IOSCO (2016) involving identification, protection, detection, and response and recovery (see Graph 2). More concretely, such strategies, policies, programmes and frameworks include the following core elements:

[28] This is in contrast to the findings of the BCBS, which is made up mostly of regulators in AEs, that only a few regulators require banks to develop such strategies (BCBS, 2018).

- mapping of exposure to cyber risk;
- defining action plans to address mapped cyber risks;
- allocating resources to implement action plans;
- defining and allocating roles and responsibilities;
- continuous review of the adequacy of controls;
- monitoring of the threat landscape;
- reporting to the board and senior management; and
- promoting cybersecurity awareness and culture.

Cybersecurity framework — Graph 3

Identification
- Baseline situation – threat profile, risk exposure & expected losses

Protection
- Internal & third-party patches to ensure security & functionality of the application environment
- Increased third-party security capabilities

Detection
- Assessment of applications' security capabilities
- Periodic scans for known security issues & vulnerabilities (vulnerability scans)
- Identification of vulnerabilities in network & physical security (penetration tests)
- Stealth assessment of organisation's digital infrastructure & defenses (red team exercises)

Response
- Incident response capabilities across pre-determined threat scenarios (table top exercises)
- Dynamic simulation of a threat to assess incident response readiness & effectiveness (war gaming)

Recovery
- Stakeholders' preparedness & effectiveness of business continuity plans
- Initiation of action plans & mobilisation of resources to tackle the consequences of a cyber incident

Sources: Adapted from CPMI-IOSCO (2016) and Oliver Wyman's approach as described in Mee and Morgan (2017)

27. **The same regulators that require specific cyber security strategies also specify cyber security governance arrangements.** Such governance arrangements require the board to set and approve the bank's cyber security strategy, framework and policy, and oversee their implementation by senior management. Senior management, on the other hand, are required to develop the bank's cyber security framework and policy in line with the overall strategy, implement the framework and policy and monitor their effectiveness. Other regulations, particularly those in AEs, typically do not specify cyber security governance arrangements. Presumably, these regulations consider that existing general risk management frameworks, particularly those for information security or operational risk/resilience, already cover the roles and responsibilities of the board and senior management when it comes to addressing cyber risks.

28. **Regulatory guidance and requirements relating to cyber security roles and responsibilities are common.** While most regulators do not require banks to implement the "three lines of defence" risk management model, regulations often require documented policies on the clear assignment of cyber-related management responsibilities relating to identification, protection, detection, and response and

recovery. Board and senior management roles are emphasised. In some cases, regulatory guidance or requirements include the designation of a unit, function or position that is responsible for the implementation of cyber security within the bank.

29. **Designation of a person responsible for cyber security at the top level is increasingly becoming mandatory.** The exact position may not be specified in regulations, but it is common that this position is required to be a C-level position (ie part of top management). In providing prominence to this position, there also seems to be a thrust towards highlighting that cybersecurity is no longer just an area of IT risk and business continuity management, but an explicit part of enterprise risk management of a bank. The requirement to designate a chief information security officer (CISO) or equivalent seems to be more common in EMDEs (eg Brazil, Kenya, Mexico, Philippines and Saudi Arabia), but it is also possible to find examples in AEs such as the UK[29]. However, the lack of information security professionals in these jurisdictions could pose challenges to the implementation of this requirement. This problem is not exclusive to EMDEs. In fact, the New York State's Department of Financial Services (DFSNY) cyber security requirements for financial services companies, for example, allows the CISO to be employed by a third-party service provider of the bank (ie not an employee), subject to certain conditions. Presumably, this is to anticipate the challenge that smaller institutions might face in hiring CISOs.

30. **Regulators generally expect banks to be able to identify their critical operations[30], including supporting information assets.** At the national level, governments identify critical infrastructure and firms to which their national cyber security frameworks apply. Banks are expected to do the same at their own level. Banks should be able to map their operations to their supporting assets and be able to classify their operations according to their criticality and sensitivity to cyber risk. This makes it possible to focus cyber security efforts on operationally sensitive and critical operations and information assets. Ideally, the entire bank should be protected but, given limited resources, banks should be able to deploy their resources in a targeted manner to maximise the benefits and ensure operational resilience.

Cyber incident response and recovery

31. **Cyber incident management is certainly one of the pillars of a sound cyber resilience framework.** Incident management is a typical and well-established IT process. But the complexity and high impact of cyber incidents have led almost all jurisdictions considered in the analysis to reinforce the provisions in their regulations specifying that banks should establish processes and capabilities to properly manage cyber incidents. A bank should be able to manage cyber incidents throughout their lifecycle. This should include establishing classification criteria and escalation and reporting procedures. Some jurisdictions stipulate that banks should also consider incidents that occurred at third party providers in their cyber incident management framework.

32. **Many regulators now require banks to develop cyber incident response and recovery (CIRR) plans, in addition to the general incident management requirement.** Considering that it is a question of when, not if, banks will experience a cyber attack, supervised institutions are now generally required to have response and recovery plans that allow them to promptly respond to a cyber incident, mitigating its impact and facilitating the rapid recovery of bank's operations.[31] This "assume breach"

[29] PRA (2021).

[30] According to BCBS (2021a), the term critical operations is based on the Joint Forum's 2006 high-level principles for business continuity, encompasses critical functions as defined by the FSB "Recovery and resolution planning for systemically important financial institutions" and is expanded to include activities, processes, services and their relevant supporting assets (people, technology, information and facilities necessary for the delivery of critical operations) the disruption of which would be material to the continued operation of the bank or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the bank and its role in the financial system.

[31] This is different from the BCBS (2018) findings that most of such requirements were not specific to cyber incidents but related to incidents in general.

mentality has totally replaced the traditional concept of building a strong perimeter to ward off a cyber attack. The new threat environment, characterised by multiple points of potential entry for attacks, has reduced the effectiveness of the traditional security approach, which relies solely on marshalling all of an institution's security devices/detective capability to guard the perimeter. The assumption of breach approach complements the traditional measures with intrusion detection techniques as well as response measures (eg to prevent the extraction of critical data). Jurisdictions aiming at strengthening their cyber resilience framework by introducing CIRR requirements are increasingly taking note of the FSB CIRR toolkit.

33. **Regulators typically stress that CIRR plans should be tested and constantly reviewed to ensure adequate response and recovery capabilities.** Given the dynamics and increasing complexity of cyber attacks, regulators expect banks to periodically assess the adequacy of their CIRR plans for managing cyber incidents. Lessons learned from previous incidents are essential to improve CIRR plans, thus allowing banks to properly respond to cyber attacks. The testing of CIRR plans is typically required in cyber resilience regulations, as can be seen in APRA's *Prudential standard on information security* and in the proposed *Joint standard on cybersecurity and cyber resilience requirements* under public consultation in South Africa. In the case of the proposed standard in South Africa, a financial institution must test all elements of its cyber resilience capacity and security controls to determine the overall effectiveness, whether it is implemented correctly, operating as intended and producing desired outcomes. Moreover, there are several examples that show authorities and/or trade associations running sector-wide exercises to test financial institutions' ability to respond and recover from disruptive event in a coordinated fashion (see Box 1)

34. **Experience with cyber attacks shows the importance of coordinating cyber incident management, crisis management and business continuity**. Successful ransomware attacks are examples of cyber incidents that can rapidly evolve into a crisis, given the potential to completely disrupt a bank's operations. Sound banking practices show the usefulness of defining and periodically reviewing the criteria to be used to characterise crisis situations, thus allowing crisis management and business continuity procedures to be adequately triggered in the case of incident escalation.

Cyber incident reporting and threat intelligence sharing

35. **Cyber incident reporting and threat intelligence-sharing are valuable tools to increase situational awareness of the cyber threat landscape**. On one hand, reporting of cyber incidents is important to assess the impact of successful incidents as well as to anticipate the likelihood of systemic risk materialising (eg systemic implications of a ransomware infection in a critical financial market infrastructure). On the other hand, threat intelligence-sharing constitutes an important source of information about threats and vulnerabilities, allowing banks to assess the adequacy of their cyber security controls.

36. **The timely communication of material cyber incidents is common across regulations.** Although timeframes and materiality thresholds vary, many regulators establish requirements for cyber incident reporting, including reporting of material cyber incidents as soon as possible, followed by a full report at a later date. The timely notification of a material incident allows authorities to start monitoring the impact of the incident on individual banks and on the financial system, while the full report is useful for collecting threat intelligence information and a root cause analysis that could be shared with banks or support supervisory activities. In some cases, intermediate reports may be required to provide updated information on the occurrence. For example, the Monetary Authority of Singapore (MAS) requires the incident to be reported within an hour of it occurring, and then a root cause and impact analysis to be

submitted to the authority within 14 days of the discovery of the incident.[32] However, when examining a broader sample of 51 EMDEs, the IMF found that 54% lack a dedicated cyber incident reporting regime.[33]

37. **Although requirements vary across jurisdictions, a few authorities have begun to develop their own threat intelligence-sharing initiatives.** Regulators recognize the relevance of information sharing on security issues for the development of a sound cyber resilience framework. Although there is no common approach to threat intelligence-sharing, this is one of the key elements of the cyber resilience framework of some jurisdictions, such as Brazil[34], the EU and Saudi Arabia. Threat intelligence-sharing is a practice that is still maturing. Some regulators are developing their own initiatives, such as the ECB's Cyber information and intelligence-sharing initiative (CIISI-EU). In Saudi Arabia, the Cyber threat intelligence (CTI) principles describe best practices focused on producing, processing, and disseminating threat intelligence to enhance the identification and mitigation of cyber threats relevant to the financial sector through actionable threat intelligence. There are also industry-led initiatives, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Cyber resilience testing

38. **Regulators expect banks to undertake cyber resilience testing and to address identified issues.** The CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, which has provided a coherent approach to improving cyber resilience in financial institutions more broadly, called for the establishment of a comprehensive cyber resilience framework that includes a testing programme to validate the framework's effectiveness. Such a testing programme could employ various testing methodologies and practices, such as vulnerability assessment, penetration testing, tabletop simulations and TLPT.

39. **In general, banking regulators do not specify the nature and frequency of testing.** These typically depend on a number of factors, including the size and complexity of a bank, the criticality and sensitivity of its business services and information assets, and changes in the threat landscape. Interestingly, some regulators in EMDEs tend to be more prescriptive. Common requirements in these jurisdictions include annual penetration testing and bi-annual vulnerability assessments or systematic scans of banks' information systems. However, many EMDEs still do not mandate testing and cyber exercises or provide further guidance.[35]

40. **There is recognition of the importance of TLPT.** A number of regulators in developed economies have TLPT frameworks in place, although the objectives and implementation details may differ.[36] The frameworks apply typically to large or critical financial institutions, but authorities may have the discretion to include other financial institutions such as banks deemed risky from a supervisory perspective. The frameworks also differ in terms of whether threat intelligence and red team test providers must be external to the financial institution, accredited and formally assessed.

41. **Some regulators coordinate or participate in cyber exercises aimed at testing crisis events that could disrupt the financial system or other critical national infrastructures.** Given the greater complexity of financial services and the increasing interconnection between financial institutions, some jurisdictions are leveraging the testing capabilities of banks and other relevant players by introducing scenarios and developing plans to respond to major disruptions of the financial system (eg unavailability of critical payment systems). Although not commonly covered by regulatory or supervisory activities, these

[32] MAS (2013).

[33] Adrian and Ferreira (2023).

[34] BCB (2021), Cyber security policy, February 2021.

[35] Adrian and Ferreira (2023).

[36] See Kleijmeer et al (2019).

initiatives contribute to the development of controls and practices to mitigate potential systemic crises (see Box 1). In the same way, it is worth mentioning that some national cyber exercises involve different sectors that could be impacted by disruptive cyber incidents, such as energy, telecommunications and financial services.

Box 1

Cyber testing and exercises

Testing is certainly one of the key elements when designing a sound cyber resilience framework. Cyber threats are constantly evolving, new software vulnerabilities are discovered every day, and cyber attacks are getting increasingly complex. It is well understood that financial institutions' cyber resilience needs to be periodically tested to ensure implemented security controls and capabilities are still adequate to properly manage cyber risk and mitigate the impact of cyber incidents.

Penetration testing and vulnerability analysis are useful tools to discover the security weaknesses of IT solutions and services. The use of code analysis tools and the implementation of development, security and operations (DevSecOps) are examples of practices and procedures that can be considered for the provision of secure IT solutions and services. But there are circumstances in which the implemented controls are not sufficient to ensure a secure environment (for instance, in the occurrence of zero-day vulnerabilities). Thus, security teams need to have the capabilities to respond to and recover from cyber incidents. Kleijmeer et al (2019) provided an overview of red teaming requirements in a number of jurisdictions, discussing their characteristics and the conditions necessary for their implementation. Some jurisdictions already require the implementation of red teaming, at least for relevant financial institutions, for example, CBEST from the Bank of England and Prudential Regulation Authority (PRA), Australia's Cyber operational resilience intelligence-led exercises framework (CORIE)®, the European framework for threat intelligence-based ethical red-teaming (TIBER-EU), and Saudi Arabia's Financial entities ethical red-teaming framework (FEER).

Despite the development of initiatives to improve the cyber security framework of financial institutions, additional actions may be necessary to ensure financial stability. The financial sector's business processes are becoming more and more distributed, resulting in the increased interconnection of different stakeholders. Moreover, new innovative projects, such as new solutions for cross-border payments, reinforce the importance of discussing the implications and risks arising from these new distributed arrangements as a cyber incident at one financial institution can affect other institutions and have implications for financial stability.

Typically, system-wide cyber exercises include tabletop simulations used to test crisis management and communication protocols in the event of systemic cyber incidents. These exercises are very useful for testing established contingency and communication plans, and for identifying situations that require coordination between different institutions or even between different critical sectors (for example, coordination between the financial sector and the telecommunications sector). The Hamilton Series is an example of a tabletop exercise coordinated by the FS-ISAC and the US Treasury. It resulted in Sheltered Harbor, an initiative that includes a standard for critical customer account data backups designed to "protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyber attack causes an institution's critical systems to fail". SIMEX, a high-profile biannual sector-wide simulation exercise coordinated by PRA and Bank of England, is another initiative designed to validate the effectiveness of the sector framework for responding to severe but plausible sector-wide operational incidents.

With the proliferation of increasingly distributed business processes, system-wide cyber exercises can become an essential tool for financial stability. These exercises can make it possible to test crisis scenarios with implications for financial stability and thus to identify mitigating actions that require coordination between the different relevant players. In addition, these exercises can support the establishment of contingency arrangements that can be implemented to strengthen the financial system's operational resilience.

Cyber hygiene

42. **Since a number of successful cyber attacks are the result of routine weaknesses in the basic maintenance and security of hardware and software, it is unsurprising that cyber hygiene is a key element of cyber regulations of banks as well as in national cyber security strategies.** Regulators have added cyber hygiene requirements to their regimes. For instance, in the US, supervisory expectations for an effective cyber security posture include basic cyber hygiene, such as IT asset management, vulnerability management, and patch management.[37] In Singapore, banks (and other financial institutions) need to comply with cyber hygiene requirements related to securing accounts with full privileges and unrestricted access; applying periodic security patching; establishing baseline security standards; deploying network security devices; implementing anti-malware measures; and strengthening user authentication.[38]

Third party dependencies

43. **Third parties are widely used by banks to provide services, systems and IT solutions that support banks' operations.** Traditionally, third parties refer to the providers of outsourced activities. In the cyber security context, third parties can be defined in a much broader sense to include products and services that are typically not considered as outsourced (eg power supply, telecommunication lines, hardware, software) as well as interconnected counterparties (eg payment and settlement systems, trading platforms, central securities depositories and central counterparties). These third parties may hold or may be able to access non-public information of banks and their customers. In addition, cyber security vulnerabilities in these third parties could become channels of attack on banks. The security capabilities of third-party service providers are therefore critical elements of any cyber security framework.

44. **In most cases, regulators use outsourcing regulations to address third party dependencies.** Outsourcing regulations typically require either prior notification or authorisation of material outsourcing activities, the maintenance of an inventory of outsourced functions and submission of reports on measurements of service level agreements (SLAs) and the appropriate performance of controls. Some outsourcing regulations also require sub-outsourcing activities to be visible to regulated entities so that they can manage the associated risks. In addition, outsourcing regulations generally require that banks develop management- and/or board-approved outsourcing and contractual frameworks that defines banks' outsourcing policies and governance and set out the respective obligations of the institution and the service provider in an outsourcing agreement.

45. **Regulations stress the importance of aligning business continuity as well as information confidentiality and integrity when dealing with third parties.** Business continuity plans of critical third party providers (and their subcontractors) should be aligned with the needs and policies of the bank in terms of business continuity and security. Data confidentiality and integrity are especially emphasised when it comes to third parties providing data processing services. This issue is addressed in general data protection requirements, contractual terms that are required to include a confidentiality agreement, and security requirements for safeguarding the data of a bank and its customers**.**

46. **Many jurisdictions have specific regulatory requirements for the use of the cloud by banks.** These range from requiring information transferred to the cloud to be subject to a contractual clause on data confidentiality and security to more specific requirements. Examples of specific requirements include those relating to data location (eg restricting the transfer of data abroad, the requirement that the location of at least one data center for cloud computing services be in the country or region), data segregation,

[37] Board of Governors of the Federal Reserve System, Supervision and Regulation Report , November 2021.

[38] MAS Notice # 655, Notice on Cyber Hygiene to Banks in Singapore, Banking Act (Cap.19), 6 August 2019.

data use limitations (eg requiring explicit client consent for data handling by third parties), treatment of data in case of an exit from the third party agreement, and the right to audit.

47. **More recently, at least a couple of jurisdictions have been moving towards having oversight frameworks for critical third parties.** Financial institutions' increased reliance on technology and the additional complexity and interconnections that technology has brought to the financial ecosystem pose operational risks not only for individual institutions but also for the financial system. This is especially true for the increasing use of cloud services, in which disruption could lead to severe consequences for the national and international financial system. This is largely because cloud services are provided by only a handful of technology companies, which operate globally. This highlights that the current approach of relying on financial institutions to manage the risks arising from third party services may not be sufficient (see Box 2), and that this may need to be complemented with an oversight framework for critical third parties.[39] The EU has already approved its Digital Operational Resilience Act (DORA), which provides for this oversight framework. In the UK, the Bank of England and the Financial Conduct Authority (the UK regulators) jointly issued a discussion paper on the same issue, following the issuance of a policy statement by the UK HM Treasury. Feedback on the discussion paper will feed into a consultation paper that is expected to be published after the relevant primary legislation giving the UK regulators oversight of critical third parties (currently before the UK Parliament) is adopted. These are in addition to jurisdictions that already have inspection powers over third parties, either through formal requirements (eg Singapore and the US) or voluntary engagements (eg Australia).[40]

[39] Prenio and Restoy (2022).

[40] BCBS (2018).

Box 2

Cloud computing and cyber resilience

Adoption of public cloud services in the financial sector has rapidly increased over the last decade (US Treasury 2023). Financial institutions (FIs) have various motivations for using cloud services, including enhanced cyber security capabilities. FIs expect to benefit from increased resilience to cyber incidents through the use of multiple data centres from the same cloud service provider (CSP) and access to state-of-the-art security technology in cloud services (eg broader use of encryption and superior built-in logging capabilities).

Cloud services are generally deployed using a "shared responsibility" model. This involves a division of responsibilities between CSPs and FIs concerning "security-of-the-cloud" (CSP) and "security-in-the-cloud" (FIs). Although this division of responsibilities varies depending on the chosen service, CSPs generally commit to maintain a security baseline and resilience controls for the purchased cloud service while FIs are typically responsible for the design and configuration of and access to the cloud services, including the respective security controls. The cloud service contract reflecting the "shared responsibility" model generally includes cyber security as a critical component of the evaluation, development and testing application of the cloud services and outlines the division of cyber resilience tasks between FIs and CSPs (eg threat detection, incident response, patching).

FIs face various challenges with the implementation of the "shared responsibility" model. Some of them are connected with the misconfiguration of cloud services, which has resulted in a variety of cyber incidents. In most cases, these are due to a lack of skilled staff able to develop sound architecture for cloud applications, as well as to the complexity involved in deploying and securing certain cloud service offerings. Another group of challenges relates to a lack of understanding of CSPs' cyber security capabilities based on available information (eg lack of information regarding cyber security incidents and testing results). A third type of challenges relates to the weak bargaining power of smaller financial institutions in negotiating contracts with CSPs.

In spite of the "shared responsibility" model, financial authorities deem FIs as ultimately responsible for managing their cloud services risks, including those related to operational resilience and cyber risks. Recent practices in the financial sector show that FIs are seeking to fulfil this expectation while overcoming challenges mentioned above by: (1) implementing risk-based assessments of CSPs and their service in light of FIs' risk appetite, risk management framework and regulatory expectations; (2) establishing security, resilience and monitoring controls[41], generally following well established industry standards such as those outlined by NIST[42] and the Cyber Risk Institute (CRI)[43]; and (3) auditing or testing operational or security capabilities offered by CSPs. It is becoming increasingly common practice for cloud service contracts to allow FIs' own internal auditors, regulators and/or third parties to conduct these audits and/or test security controls. Some FIs rely on third-party assurance reviews, such as service organisation controls (SOC) reviews[44], penetration tests, and vulnerability assessments, to understand CSP's control environment. Other FIs are combining their resources to conduct or hire auditors to conduct "pooled" audits and certifications or are considering doing so.

[41] Monitoring controls include dashboards and logging capabilities offered by CSPs and financial institutions' own customised, compatible solutions to monitor operational performance and security threats.

[42] For example, NIST SP 500-291 Cloud computing standards roadmap or SP 500-332 Cloud federation reference architecture.

[43] See CRI (2022).

[44] One of the most common kinds of third-party service provider audits is the SOC2 reports, conducted in accordance with the American Institute of Certified Public Accountants standards for assessing service organisations. SOC2 reports involve an evaluation of the security, availability, processing integrity, confidentiality, or privacy of information and systems across an entire entity, a particular subsidiary or operating unit, or a particular function. The SOC2 report can be a type I report, a point in time assessment largely based on documented controls, or type II report, a sustained observation of a period in time. Typically, CSPs will offer options within the contract that will allow the financial institutions to receive SOC reports or additional reports or evidence for an additional fee.

Cyber security culture and awareness

48. **Banking regulators emphasise the importance of disseminating a cyber security culture to banks' staff, third-party providers, clients and users.** Regulators highlight the responsibility of the board and senior management to promote a cyber security culture, which is typically supported by training programmes suitable for different target audiences (staff, providers, clients etc). In the US, a supervised institution with a strong security culture generally integrates its information security programme into its line of business, support functions, third-party management and new initiatives. The Brazilian regulation[45] requires banks to establish mechanisms for dissemination of a cyber security culture within the institution, including the provision of information to clients and users regarding precautions when using financial products and services**.**

49. **Most regulators establish cyber security awareness and training requirements.** According to Ponemon Institute (2022), negligent employees or contractors are a major source of cyber security incidents.[46] In light of this, most regulations require cyber security awareness programmes for staff, contractors and service providers of the supervised institution. These programmes aim to reinforce the cyber security culture of the institution. They generally take the form of periodic training and are envisaged to cover at least the existing cyber threat landscape, the institution's information security policies and procedures, and the individual's cyber security responsibilities. Some regulators, such as the Saudi Arabian Monetary Authority (SAMA), require institutions to measure the effectiveness of their awareness programmes and to foster their customers' awareness as part of these programmes. Other regulators, such as the Bank of Israel, require institutions to foster their service providers awareness too and to review their programmes periodically according to the cyber threat landscape and corresponding risk assessment.

Cyber security workforce

50. **Regulators expect banks to allocate adequate resources to implement their cyber security framework.** Although drawing up expectations regarding cyber security expertise is quite challenging, given that different banks are likely to have different needs related to cyber security staff, many regulators stess that the implementation of a sound cyber security framework depends on the allocation of adequate resources, including human resources with the necessary skills to implement the cyber security strategy. Hong Kong is unique in that it has established the Enhanced competency framework on cybersecurity (ECF-C), which sets out the common core competences required of cyber security practitioners in the Hong Kong banking industry. While the ECF-C is not mandatory, banks are encouraged to adopt it in order for the banking industry to; (i) develop a sustainable talent pool of cyber security practitioners; and (ii) raise and maintain the professional competence of cyber security practitioners.[47] It is also worth noting Carnegie's efforts to develop capacity with the launch in 2019 of a "Cyber resilience capacity-building toolbox for financial organizations" together with several partner organisations.[48]

51. **On the regulatory and supervisory side, there is also a need to ensure that they have the requisite resources to implement cyber security regulations.** Coming up with cyber regulations is the easy part because these are mainly based on international standards, but enforcing these regulations is the real challenge. Supervisory staff should be able to properly assess whether banks are following the

45 BCB (2021).

46 This Ponemon Institute report includes survey responses from over 1,000 IT professionals worldwide, all of which have experienced a recent cybersecurity incident due to an insider threat. This report concludes that, over the past two years, insider threats have increased "dramatically", with 56% of insider-related incidents caused by a negligent employee.

47 HKMA (2016).

48 See FinCyber Project (2019). Carnegie's partners in this initiative include the IMF, SWIFT, FS-ISAC, Standard Chartered, the Cyber Readiness Institute, and the Global Cyber Alliance. A new version of the tool was launched in 2021.

spirit of the regulations and not merely doing a box-ticking exercise This entails attracting and retaining staff with relevant cyber expertise which is another challenge for the regulatory community. To mitigate these challenges, regulators are using various approaches such as developing internal talent through professional development requirements (eg MAS and Bank of Italy) and centralising their risk specialists, including cyber risk experts, in single units (eg Bank of England).[49] However, based on an IMF survey, 68% of authorities in 51 EMDEs lack a specialised risk unit in their supervision department.[50]

Cyber resilience metrics

52. **Regulators do not typically require banks to submit or monitor specific cyber resilience metrics.** The few regulators that do so have very high-level requirements. Typically, such requirements ask banks to define metrics that indicate the effectiveness of their cyber security practices or to highlight the information assets that have the highest risk exposure.

53. **Where it exists, the requirement to define metrics and indicators forms part of reporting, monitoring, controlling and incident management activities.** APRA, for example, provides practical guidance to its banks on what types of quantitative and qualitative information would give boards and senior management a clearer picture of their cyber security.[51] For example, the guidance states that results of control testing activities and security events detected could be some of the information that could be provided to the board and senior management. The BSP, on the other, hand, requires banks to define metrics or indicators of possible compromise to enhance fraud detection and monitoring capabilities and facilitate regulatory cyber incident reporting. This could include access to a highly sensitive system beyond office hours and failed log-in attempts of privilege user accounts.[52]

54. **Examples of metrics mentioned in existing regulations only provide broad information on banks' approaches to building and ensuring cyber security and resilience.** This shows that the development of cyber resilience metrics for supervisory purposes is still at an early stage. The nature of cyber risk, however, makes a backward-looking approach to cyber resilience metrics ineffective. Cyber threat players are dynamic and continuously adapt to responses and protective measures. There is thus an increasing recognition of the need for forward-looking indicators as direct and indirect metrics of cyber security and resilience.

Section 5 – Conclusion

55. **Banking regulations relating to cyber security and cyber resilience have matured and are now well established in several jurisdictions.** The regulations relating to cyber security and cyber resilience covered in Crisanto and Prenio (2017) were quite new. These regulations existed only in a few jurisdictions – mainly in Aes – and focused on establishing a cyber risk management approach and controls. Six years hence, many jurisdictions, including EMDEs, already have cyber-related regulations in place. Many of these newer regulations (or second-generation cyber regulations) focus on improving cyber resilience capabilities and providing financial institutions and authorities with tools to manage cyber risks adequately. Nonetheless, a material number of EMDEs still do not have relevant regulations.

[49] Mauer and Nelson (2020).

[50] Adrian and Ferreira (2023).

[51] Attachment H of APRA (2019).

[52] Appendix 75 of the BSP's Manual of Regulations for Banks.

56. **Regulators are adding specific requirements or expectations on some areas or add new elements in their cyber regulations.** There are now more specific regulatory requirements on cyber incident response and recovery, as well as on third-party management and oversight, incident reporting and testing frameworks. A few jurisdictions have also introduced requirements or expectations for cyber security workforce and cyber resilience metrics. However, cyber security strategy, cyber incident reporting, threat intelligence-sharing, third party dependencies and cyber resilience testing are still the primary focus of these regulations.

57. **Cyber regulations in EMDEs tend to be more prescriptive.** This is especially the case when it comes to cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing. Banking regulators in EMDEs perhaps see the need to strengthen cyber resilience culture across the financial sector and/or to be clearer and more specific in their expectations given the resource constraints and limited supply of skills and expertise in their jurisdictions. This way, banks' boards, senior management and staff have concrete guidance to follow in enhancing cyber security of their institutions.

58. **There is a need to guard against a compliance-based approach to dealing with cyber security.** Too much prescriptiveness may result in a tick-box approach to cyber security. Putting cyber regulations in place should not be viewed as a tick-box exercise either. It should be complemented by appropriate supervisory resources to ensure effective implementation and enforcement. There is scope therefore for international organisations and financial authorities in Aes to support supervisory capacity building efforts in EMDEs, particularly in the area of cyber security. After all, cyber threats know no boundaries.

59. **International work (eg by the SSBs and the G7) has facilitated a helpful level of cyber resilience convergence in the financial sector, but more work is needed.** No single firm or regulator can successfully tackle cyber risk alone. Moreover, the cross-border nature of cyber risk requires a reasonable degree of alignment in national regulatory expectations. The work by the G7 CEG and the SSBs on cyber resilience has made financial regulatory and supervisory expectations more consistent across different jurisdictions and is therefore a step in the right direction. In particular, the FSB's proposal for greater convergence in cyber incident reporting is an important development since it tries to reconcile differing jurisdictional requirements that only burdens supervised institutions rather than help address these incidents. Going forward, there might be scope to align the ways in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics. Moreover, given the potential cross-border implications for the financial system of a cyber incident at one critical third-party provider, particularly a cloud provider, there might be scope to consider an international oversight framework for such providers.

References

Adrian, T and C Ferreira (2023): "Mounting cyber threats mean financial firms urgently need better safeguards: regulators and supervisors must act now to strengthen the prudential framework", 2 March.

Australian Prudential Regulation Authority (APRA) (2019): "Prudential practice guide: CPG 234 information security", June.

Banco Central do Brasil (BCB) (2021): "Cyber security policy", February.

Bangko Sentral ng Pilipinas (BSP): "Manual of Regulations for Banks".

Bank of England and Financial Conduct Authority (BoE/FCA) (2022): "Operational resilience: Critical third parties to the UK financial sector", 21 July.

Basel Committee on Banking Supervision (BCBS) (2018): "Cyber-resilience: Range of practices", December.

——— (2021a): "Principles for operational resilience", March.

——— (2021b): "Newsletter on cyber security", 20 September.

Carvalho, A P, S Hohl, R Raskopf and S Ruhnau (2017): "Proportionality in banking regulation: A cross-country comparison", FSI Insights no 1, August.

Center for Internet Security (CIS) (2021): "18 CIS critical security controls".

Chainalysis (2023): "2022 Biggest year ever for crypto hacking with $3.8 billion stolen, primarily from DeFi protocols and by North Korea-linked Attackers", 1 February.

Cloud Risk Institute (CRI) (2022): "Cloud profile", Cloud Security Alliance, Bank Policy Institute, "CRI announces completion of cloud profile extension", April.

Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions (CPMI/IOSCO) (2012): "Principles for financial market infrastructures", April.

——— (2016): "Guidance on cyber resilience for financial market infrastructures", June.

——— (2022): "Implementation monitoring of the PFMI Level 3 assessment on financial market infrastructures' cyber resilience", November.

Crisanto, J C and Prenio, J (2017): "Regulatory approaches to enhance banks' cyber-security frameworks", FSI Insights on policy implementation no 2, 2 August.

Crowdstrike (2022): "2023 Global threat report".

Doerr, S., L Gambacorta, T Leach, B Legros and D Whyte (2022): "Cyber risk in central banking", September.

Department of Financial Services of New York State (DFSNY) (2017): "Cybersecurity requirements for financial services companies".

European Parliament (2022): "Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector", 17 November.

European Union Agency for Cybersecurity (ENISA) (2022): "ENISA threat landscape 2022", 3 November.

EY and Institute of International Finance (EY-IIF) (2023): "Seeking stability within volatility: How interdependent risks put CROs at the heart of the banking business", 12th annual EY-IIF global bank risk management survey, January.

Financial Stability Board (FSB) (2017a): "Financial stability implications from fintech: supervisory and regulatory issues that merit authorities' attention", June.

_____ (2017b): "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices", 13 October.

——— (2018): "Cyber lexicon", 12 November.

——— (2020): "Effective practices for cyber incident response and recovery: Final report", 19 October.

——— (2022): "Achieving greater convergence in cyber incident reporting – consultative document", 17 October.

——— (2023): "FSB Chair's letter to the G20 finance ministers and central bank governors", 16 February.

G7 (2016): "G7 Fundamental elements of cybersecurity for the financial sector", October.

——— (2017): "G7 Fundamental elements for effective assessment of cybersecurity in the financial sector", October.

——— (2018): "G7 Fundamental elements for threat-led penetration testing", October.

——— (2018): "G7 Fundamental elements for third party cyber risk management in the financial sector", October.

——— (2020): "G7 Fundamental elements for cyber exercise programmes", October.

——— (2022): "G7 Fundamental elements of ransomware resilience for the financial sector", October.

——— (2022): "G7 Fundamental elements for third party cyber risk management in the financial sector", October.

FinCyber Project (2019): "Cyber resilience and financial organizations: A capacity-building toolbox", Carnegie Endowment for International Peace.

Gracie, A (2014): "Managing cyber risk – the global banking perspective", 10 June.

Hong Kong Monetary Authority (HKMA) (2016): "Enhanced competency framework on cybersecurity", 19 December.

IBM (2022): "Cost of a data breach 2022 report".

Institute of International Finance (IIF) (2023): "How fragmentation is continuing to challenge the provision of cross-border financial services: Issues and recommendations", March.

International Association of Insurance Supervisors (IAIS) (2020): "Cyber risk underwriting: Identified challenges and supervisory considerations for sustainable market development", December.

——— (2022): "Issues paper on insurance sector operational resilience: draft for public consultation", October.

——— (2023): "Special topic edition: cyber", Global Insurance Market Report (GIMAR), April.

International Organization for Standardization (ISO) (2018): "ISO 31000: Risk Management".

——— (2019) "ISO 22301: Security and Resilience — Business Continuity Management systems".

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) (2018): "ISO/IEC 27000: Information Technology — Security Techniques — Information Security Management Systems".

Interisle Consulting Group (2022): "Phishing landscape 2022 - An annual study of the scope and distribution of phishing", 19 July.

ISACA (2019): "COBIT 2019 framework".

Kleijmeer, R, J Prenio and J Yong (2019): "Varying shades of red: how red team testing frameworks can enhanced the cyber resilience of financial institutions", FSI Insights no 21, November.

Maurer, T and A Nelson (2020): "International Strategy to Better Protect the Financial System Against Cyber Threats", Carnegie Endowment for International Peace, November.

Monetary Authority of Singapore (MAS) (2013): "MAS Notice 644", 21 June.

Moody's Investor Service (2022): "2023 Outlook – Governments and industries toughen cyber stance; credit effects mixed", 7 November.

National Institute of Standards and Technology (NIST) (2018): "Framework for improving critical infrastructure cybersecurity: Version 1.1", 16 April.

Ponemom Institute (2022): "2022 Ponemon cost of insider threats global report".

Prenio, J and F Restoy (2022): "Safeguarding operational resilience: a macroprudential perspective", FSI Briefs no 17, 25 August.

Prudential Regulation Authority (PRA) (2021): "Strengthening individual accountability in banking", December.

Statista: "Estimated cost of cybercrime worldwide from 2016 to 2027".

The International Criminal Police Organization (INTERPOL) (2022): "Global crime trend report".

UK HM Treasury (2022): "Critical third parties to the finance sector: policy statement", 8 June.

Wilson, C, T Gaidosch, F Adelmann and A Morozova (2019): "Cybersecurity risk supervision", IMF Monetary and Capital Markets Department Paper No19/15, September.