Basel Committee
on Banking Supervision

# Cyber-resilience:

# Range of practices

December 2018

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-228-8 (online)

## Contents

# Executive Summary

This report identifies, describes and compares the range of observed bank, regulatory, and supervisory cyber-resilience practices across jurisdictions. In preparing this range of practices document, the Basel Committee on Banking Supervision relied on input from its member jurisdictions in response to a survey conducted by the Financial Stability Board (FSB) in April 2017.

Below are some of the key findings:

1. *General landscape*: **Most supervisors leverage previously developed national or international standards – principally the NIST framework, ISO 27000 series and CPMI-IOSCO guidance for cyber-resilience of financial market infrastructures.** Published and unpublished supervisory practices converge in some areas, eg governance, testing, information-sharing between banks and regulators, and management of outsourcing arrangements. Despite convergence in high level expectations, the technical specifications and supervisory practices differ across jurisdictions. While this diversity of approaches may result in a complex and somewhat fragmented international regulatory landscape, it may also merely reflect actual differences in BCBS members' legal frameworks and degree of digitalisation.

2. *Strategy*: **While regulators generally do not require a specific cyber strategy, all expect institutions to maintain adequate capability in this area as part of their global strategies**. Cyber-risks pose growing, evolving and unique challenges to institutions and supervisors that require dedicated attention and resourcing. Regulators expect that institutions will minimise their cyber exposure through ensuring that systems are "secure-by-design" and that emphasis is placed on resilience in light of current threats rather than compliance to a standard.

3. *Cyber-risk management*: **In most jurisdictions, broader IT and operational risk management practices are quite mature and are used to address cyber-risk and supervise cyber-resilience.** In particular, jurisdictions expect banks to have a strategy and framework to comprehensively map and actively manage their IT system architecture. Banks nonetheless generally still lack a cyber-strategy that defines clear tolerance and appetite levels for cyber-risk and that has been approved and adequately challenged at board level.

4. *Governance/organisation*: Although management models such as the three lines of defence (3LD) model are widely adopted, **cyber-resilience is not always clearly articulated across the technical, business and strategic lines**. This confusion in roles and responsibilities hampers the effectiveness of the 3LD model.

5. *Workforce*: **Skills shortage leads to recruitment challenges.** Most existing IT frameworks and governance regulations generally provide broadly convergent requirements for cyber-related functions, but the skills shortage remains a challenge. A few jurisdictions have implemented or leveraged specific cyber-certifications to address this.

6. *Testing:* **Protection and detection testing is evolving and prevalent; response and recovery less so.** Incident response and recovery testing is typically done through tabletop exercises, and broader continuity testing.

7. *Incident response capabilities*: **Although an incident management framework is not required, incident response plans are.** Supervisors in all jurisdictions expect banks to prepare an incident response plan to deal with material cyber-incidents. Most supervisors expect banks to classify their information assets and services according to their operational sensitivity and business criticality.

8. *Assessment metrics***: Although some forward-looking indicators of cyber-resilience are being picked up through the most widespread supervisory practices, no standard set of metrics has emerged yet.** This makes it more difficult for supervisors and banks to articulate and engage on cyber-resilience.

9. *Information-sharing:* **Most observed information-sharing mechanisms involve bank-to-bank and bank-to-regulator communications, with the former being mostly done on a voluntary basis**. Despite common features, the content and use of information collected or shared by banks and supervisors varies widely across jurisdictions. Other types of information-sharing – especially regulator-to-regulator, domestically and cross-border – are less documented or systematic, but do take place on ad hoc and bilateral bases. Although the sharing of information among regulators can use existing channels – such as memoranda of understanding and supervisory colleges – the speed, latitude, security and fluidity of communications required to cope with a cross-border cyber-incident has led a few jurisdictions to take specific formal steps in this area.

10. *Third-party risk*: **Regulatory frameworks for outsourcing activities across jurisdictions are quite established and share substantial commonalities**. Supervisors are using these frameworks to spell out expectations with regard to their banks' management of third party dependencies. However, there is no common approach regarding third parties beyond outsourced services, which implies different scopes of regulation and supervisory actions. While third parties may provide cost-effective solutions to increase resilience levels, the onus remains on the banks to demonstrate adequate understanding and active management of the third-party dependencies and concentration across the value chain. A balanced accountability model remains to be found, especially in the case of third parties not subject to banking supervision prerogatives.

# 1. Introduction

In March 2017, the G20 Finance Ministers and Central Bank Governors noted that "the malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability".[1]

Regulated institutions' use of technology includes greater levels of automation and integration with third-party service providers and customers.[2] This results in an attack surface that is growing and is accessible from anywhere, and it incentivises cyber-adversaries to increase their capabilities. Increased use of third-party providers means that the perimeter of interest to financial sector regulators has gotten bigger, and greater use of cloud services means that the perimeter is also shared. Shared service models require regulated institutions to think differently about how they build and maintain their cyber-resilience in partnership with third parties.

Given the increase in the frequency, severity and sophistication of cyber-incidents in recent years, a number of legislative, regulatory and supervisory initiatives have been taken to increase cyber-resilience. At the international level, the G7 issued Fundamental Elements of Cyber-security for the financial sector,[3] and the Committee on Payments and Market Infrastructures (CPMI) issued, jointly with the International Organization of Securities Commissions (IOSCO), guidance on cyber-resilience for financial market infrastructures (FMIs) in June 2016.[4] In the European Union (EU), the European Commission's (EC) Fintech Action Plan invites the European Supervisory Authorities to consider issuing guidelines to achieve convergence on ICT risk. [5]

Against this backdrop, the Basel Committee on Banking Supervision (BCBS) recognised the merits of approaching operational resilience beyond the purview of operational risk management and minimum capital requirements, and established the Operational Resilience Working Group (ORG) with the intention of contributing to, inter alia, the international effort related to cyber-risk in close coordination with the other international bodies involved. The Committee therefore requested that the ORG provide this first assessment of observed cyber-resilience practices at authorities and firms.

The objective of this report is to identify, describe and compare the range of observed bank, regulatory and supervisory cyber-resilience practices across jurisdictions. In preparing this range of practices

[1] See G20, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting,* Baden-Baden, Germany, 17–18 March 2017, www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

[2] Many regulated institutions are adopting strategies that will see more data stored and/or processed outside the perimeters of the regulated institution while at the same time granting service providers (now growing to what is commonly a multitude of providers) access to their environments to perform business and technology processes.

[3] See G7, *Fundamental elements of cybersecurity for the financial sector*, October 2016.

[4] See CPMI-IOSCO: *Guidance on cyber-resilience for financial market infrastructures*, June 2016.

[5] The European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA), collective referred to as the "European Supervisory Authorities".

document, ORG members used the input provided by their organisation to an FSB survey in April 2017, which led to the publication of its stocktake of publicly released cyber-security regulations, guidance and supervisory practices at both the national and international level issued in October 2017. According to the FSB cyber-security stocktake, banking is the only sector in financial services for which all FSB jurisdictions have issued at least a regulation, guidance or supervisory practices. In addition, the FSB found that member jurisdictions drew upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cyber-security regulatory and supervisory schemes (mainly the 2016 CPIMI-IOSCO guidance, the US National Institute of Standards and Technology (NIST) cyber-security framework and the ISO 27000 series).[6]

Besides reviewing and completing their jurisdiction's responses to the FSB survey questions, ORG members shared their direct experiences and insights in order to provide a more concrete and specific understanding of the main trends, progress and gaps in the pursuit of cyber-resilience in the banking sector. Furthermore, additional insight was gained and findings were fine-tuned through outreach to a broad set of industry stakeholders including banks, utility and technology service providers, consultancies and associations involved in domestic and international cyber-security matters.

For the purpose of this report, the BCBS uses the FSB Lexicon definition of cyber-resilience,[7] which defines it as the ability of an organisation 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. Although this paper focuses on cyber-resilience, practices also relevant to the broader operational resilience context were considered. A distinction was also drawn between cyber-risk management (which deals with vulnerabilities and threats) and IT risk management, the scope of which is broader than the matter at hand in this report. Where appropriate, deeper dives on practices that reflect new approaches or address widely shared strategic concerns have been performed ORG members in the form of nine specific case studies.

The remainder of this report is divided into the following sections:

- Section 2 provides a high-level overview of current approaches taken by jurisdictions to issue cyber-resilience guidance standards.
- Section 3 assesses the range of practices regarding governance arrangements for cyber-resilience.
- Section 4 focuses on current approaches on cyber-risk management, testing, and incident response and recovery.
- Section 5 explores the various types of communications and information-sharing.
- Section 6 analyses expectations and practices related to interconnections with third-party services provides in the context of cyber-resilience.

[6] See NIST, *Framework for improving critical infrastructure cybersecurity*, 16 April 2018, www.nist.gov/cyberframework/framework, which consists of standards, guidelines and best practices to manage cyber-security-related risk.

[7] See FSB, Cyber Lexicon, 12 June 2018, www.fsb.org/wp-content/uploads/P121118-1.pdf.

## 2. Cyber-resilience standards and guidelines

Most jurisdictions address cyber through the lens of IT and general operational risk. Cyber-resilience expectations, which are sometimes embedded within high-level IT risk guidance, cover a wide range of regulatory standards.[8] The intent of IT risk guidance is to communicate jurisdictions' expectations and encourage good practice. Guidance typically addresses governance, risk management, information security, IT recovery and management of IT outsourcing arrangements. While guidance is presented as operational risk or IT risk guidance, it effectively provides coverage of cyber-risk management as a subset of these practices.

Standards on general risk topics such as business continuity planning and outsourcing contribute to the management of a wide range of risks and also have relevance to cyber-risk. Discussion at the 2017 Information Technology Supervisors' Group (ITSG) meeting highlighted that many countries are working on updates to their outsourcing standards.[9] The Australian Prudential Regulation Authority (APRA) is also considering whether the term outsourcing remains relevant or whether *service provider risk management* might be more appropriate, recognising that bank supply chains have become more complex. Section 6 of this report further discusses expectations and practices in relation to third-party interconnections.

Specific cyber-risk management guidance has emerged in the context of information security. A few jurisdictions have issued specific cyber-risk management or information security guidance, including on the importance of effective cyber-security risk management (Hong Kong SAR), on early detection of cyber intrusions (Singapore), on the establishment of a cyber-security policy (Brazil) and on the common procedures and methodologies for the assessment of ICT risk (European Banking Authority (EBA)).

In jurisdictions where no specific cyber-security regulations exist for the financial sector, supervisors encourage their regulated entities to implement international standards and apply prescriptive guidance, and supervisory practices align with the top-down initiatives of national cyber-agencies. Most jurisdictions implement key concepts from international and industry standards such as NIST, ISO/IEC and COBIT.[10] Regulators also leverage supervisory practices from the US (Federal Financial Institution Examining Council (FFIEC) IT Examination Handbook) and the UK (CBEST).

Some jurisdictions are developing enforceable standards for cyber-resilience in the financial sector. This is the theme of this report's first case study (Box 1).

[8] We note that while the majority of jurisdictions' cyber-resilience expectations are derived from common frameworks, eg NIST, each supervisory authority has designed their own assessment tools, eg questionnaires. As a result, regulated entities are required to provide slightly different information to each supervisory authority, even where the broad questions posed are the same. Banks and supervisory authorities may benefit from harmonisation and standardisation, not just of supervisory expectations, but also of the information requested by supervisors and the tools used to collect it.

[9] The Information Technology Supervisors' Group (ITSG) is an international working group of IT supervisors which meets annually to discuss approaches to IT risk (including cyber-risk).

[10] Control Objectives for Information and Related Technologies (COBIT) is a good practice framework created by international professional association ISACA for information technology (IT) management and IT governance.

Box 1

## Case Study 1: Recent regulatory initiatives – the Australian, German and US minimum requirements

### Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234 Information Security

This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties. The board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security. The key requirements of this Prudential Standard are that an APRA-regulated entity must:

- clearly define the information security-related roles and responsibilities of the board, senior management, governing bodies and individuals;
- maintain its information security capability commensurate with the size and extent of threats to its information assets, and so that it enables the continued sound operation of the entity;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- notify APRA of material information security incidents.

### Supervisory Requirements for IT in Financial Institutions (BaFin Circular 10/2017, BAIT)

The German Banking Act requires financial institutions to demonstrate that its risk management comprises, among other things, adequate technical and organisational resources and adequate contingency planning, especially for IT systems.

The circular on Minimum Requirements for Risk Management (MaRisk) provides a comprehensive framework for the management of all significant risks, thereby concretising the requirements of the German Banking Act. Complementing MaRisk in this regard, the Banking Supervisory Requirements for IT (BAIT) refines the German Banking Act.

The BAIT covers requirements with respect to:

- IT strategy and IT governance;
- information risk management and information security management;
- user access management;
- IT project management and application development;

- IT operations; and

- outsourcing and other external procurement of IT services.

**US agencies' notice of proposed rulemaking for new cyber-security regulations for large financial institutions**

Another example is the joint announcement from the US Federal Reserve, the Officer of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC), which provided a notice of proposed rulemaking for new cyber-security regulations for large financial institutions. The intent is to address the type of serious cyber-incident that could impact safety and soundness. As announced, requirements will relate to cyber-risk governance, risk management, internal dependency management, external dependency management, incident response, assurance management of third parties and audit.

The State of New York Department of Financial Services has also released cyber-security regulations that require regulated intuitions in New York to have a cyber-security programme designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of the financial services industry.

# 3. Cyber-governance

The majority of the regulators have issued either principles-based guidance or prescriptive regulations, with varying levels of maturity. In general, regulatory standards and supervisory practices address enterprise IT risk management but do not include specific regulations or supervisory practices that cover cyber-risk management of critical business functions, interconnectedness or third-party risk management. Against this backdrop, supervisory expectations and practices were identified and analysed in the following areas relevant to governance:

- Cyber-security strategy
- Management roles and responsibilities
- Cyber-risk awareness culture
- Architecture and standards
- Cyber-security workforce

## 3.1 Cyber-security strategy is expected but not required

Although most regulators do not require regulated entities to develop a cyber-security strategy, all expect regulated institutions to have a board-approved information security strategy, policy and procedures under the broad remit of effective oversight of technology.

Many jurisdictions (eg Australia, Brazil and jurisdictions across Europe) expect that cyber-risk should be covered by the organisation-wide risk management framework and/or information security framework which is monitored and reviewed by senior executives.

Consistent with the previous observation regarding regulatory expectations, most supervisors review regulated entities' information security strategies, but very few require or evaluate those entities' standalone cyber-security strategies. Examiners typically review an institution's information security strategy, information security plans, and cyber-security implementation, including key cyber-security initiatives and timelines. They may also review its practices for communicating with relevant stakeholders.

A variety of approaches can also be observed within regions: while the FFIEC IT Examination Handbook in the US does not specifically address the development of a cyber-security strategy, Canada's self-assessment guidance attempts to determine whether a regulated financial institution has established a cyber-security strategy aligned with the institution's business strategy and implementation plan. Mexico does not have supervisory practices focused on cyber-security strategy but has issued regulations that direct banks to develop IT security strategies.

Jurisdictions enforce cyber-security strategy requirements using three types of non-mutually exclusive regulatory approaches:

1. The regulator/authority implements cyber-security strategy requirements, either sector-specific or across multiple industries, with which financial institutions have to comply. This is a common approach in emerging market economies with relative homogeneity in their banking systems.

2. The financial institutions establish their own cyber-security strategies in compliance with principles-based risk management practices. Regulators review these strategies as part of their assessment of an institution's overall risk management practices.[11]

3. A third approach, prevalent in Europe, involves examining whether financial entities have an IT strategy and the accompanying security provisions.

## 3.2 Management roles and responsibilities

### 3.2.1 Recognition of the importance of the board of directors and senior management

Some jurisdictions have issued specific regulatory guidance and requirements addressing cyber-governance roles and responsibilities of the board of directors (BoD) and senior management. The majority of such guidance prioritises the roles and responsibilities of the BoD and senior management, while others have prioritised them even more in overseeing overall business technology risks. Other jurisdictions approach cyber-governance as a risk that regulated entities are expected to address within their existing risk management frameworks.

Almost all the jurisdictions emphasise the importance of management roles and responsibilities for cyber-governance and controls. In the US, EU and Japan, high-level guidelines

[11] The Saudi Arabian Monetary Authority (SAMA) applied the first two of these approaches by compelling financial institutions to formulate their own cyber-security strategies while it developed supervisory practices for implementing cyber-security strategy.

encourage global systemically important banks (G-SIBs) and domestic systemically important banks (D-SIBs) to implement well defined, risk-sensitive management frameworks under initiatives taken by the BoD. In addition, the EBA implements granular and prescriptive requirements, ensuring consistent cyber-security regulation and supervision across the European banking sector. Similarly, emerging market economies implement more granular and prescriptive cyber-security requirements.

### 3.2.2 Variety of supervisory approaches regarding the second and third lines of defence (3LD)

The majority of regulators have adopted the 3LD risk management model to assess cyber-security risk and controls. However, most regulators do not require the implementation of 3LD at regulated entities and do not prescribe precisely how responsibilities should be distributed across the lines, as the expectation is rather for banks themselves to clearly define responsibilities and leave no gaps between the lines. As a result, supervisory practices for assessing the degree of 3LD implementation vary widely, and there appears to be a greater supervisory focus on the first and second lines of defence than on the third line across jurisdictions, which could hamper the effectiveness of the 3LD checks and balances model. In particular, only a few jurisdictions have formulated specific expectation regarding the independent reporting line from the chief audit executive to the audit committee of the BoD.

Box 2

### Case study 2: Roles and responsibilities of chief information security officers (CISOs) in cyber-governance

A widespread practice among large and globally active banks is to establish a robust governance structure based on the 3LD model. Typically, in this model, the CISO is the executive officer responsible for a bank's cyber-security management. The CISO's role is to serve as a circuit breaker and to balance the firm's risk appetite with security protection considerations long before introducing or expanding digital services or products. However, in most cases the CISO reports to the chief risk officer (CRO) or to the chief information officer (CIO), with no independent reporting line to the CEO or board of directors (BoD). CROs typically place more emphasis on compliance over risk management. Emerging trends in cyber-governance indicate that the placement of the CISO under the CRO is not ideal because the two positions have inherently conflicting priorities. When the CISO attempts to implement risk-based cyber and IT security controls that accommodate technological innovation through the "plan-do-check-act" (PDCA) cycle, the CRO may prioritise compliance over the benefits of technological innovation. This dynamic can impede the CISO from effectively performing his/her job function. In response, some global banks are restructuring the CISO role by having the CISO report directly to the CEO or BoD.

Considering the cyber-threat landscape, the Saudi Arabian Monetary Authority (SAMA) issued a principle-based cyber-security framework and mandated financial institution to comply with various range of control considerations mentioned in different topics of this framework.

One such topic addresses responsibilities of the CISO in the cyber-security committee, security strategy, security architecture, risk-based cyber-security solutions, operational security, etc to ensure that cyber-security controls are applied throughout the financial institution. This is reinforced with the role of the cyber-security function in financial institutions where SAMA requires financial institutions to have a cyber-security function independent from the IT function. This includes separate budgets and staff evaluations along with the cyber-security function reporting directly to the CEO/managing director or senior management of the control function of the financial institution.

SAMA also requires financial institutions to perform periodic self-assessments against the cyber-security framework, which is subject to review (on- and off-site) by SAMA to determine the level of compliance and cyber-security maturity of the financial institution.

## 3.3 Cyber-risk awareness culture

An awareness of cyber-risk by staff at individual banks and a common risk culture across the banking industry are prerequisites for maintaining cyber-resilience within the sector. Regulators in most jurisdictions have published guidance emphasising the importance of risk awareness and risk culture for staff and management at all levels, including BoDs and third-party employees. Regulatory requirements include increasing cyber-security awareness and cyber-related staffing at regulated entities. In some jurisdictions, regulators require cyber-security awareness training during each phase of the employment process, from recruitment to termination.

Regulated entities may be required to include non-disclosure clauses within staff agreements. To mitigate insider threats, some jurisdictions require new employees to complete a screening and background verification process, while existing employees undergo a mandatory reverification process at regular intervals. In some jurisdictions, regulators assess whether banks have robust processes and controls in place to ensure their employees, contractors and third-party vendors understand their responsibilities, are suitable for their roles and have the requisite skills to reduce the risk of theft, fraud or misuse of facilities. The majority of the regulators encourage the development of a common risk culture sufficient to ensure effective cyber-risk management. In some jurisdictions, regulators assess each bank's cyber-risk appetite, considering such factors as the bank's business model, core business strategy and key technologies. Some jurisdictions view cyber-security as a critical business function, since a cyber-attack could lead to the insolvency of individual entities or even to widespread disruption of the entire sector.

## 3.4 Architecture and standards

For most jurisdictions, general regulatory requirements for architecture and standards are not in place, or there is a lack of coverage. Only a small number of countries specifically highlight control considerations and substantial supervisory guidance for cyber-security architecture. For instance, the US FFIEC IT Examination Handbook specifies that when discussing network architecture, supervisors should confirm that the diagrams are current, securely stored and reflective of a defence-in-depth security architecture. In Saudi Arabia, practices covering cyber-security architecture are subject to a periodic self-assessment.

## 3.5 Cyber-security workforce

The skills and competencies of cyber-workforces, their regulatory frameworks and the range of practices differ markedly across jurisdictions. Some jurisdictions have IT-specific standards that address the responsibilities of the IT workforce and information security functions, with particular attention to cyber-security workforce training and competencies. Their range of supervisory practices covers the assessment of team divisions, staff expertise (background and security checks of cyber-security specialists), the staff training processes and the adequacy of funding and resources to implement the organisation's cyber-security framework. Most of the jurisdictions are in the early stages of implementing supervisory practices to monitor a bank's cyber-workforce skills and resources. Their regulatory schemes require regulated entities to manage risks but do not set specific requirements to address cyber-security workforce skills and resources.

The majority of regulators assess the cyber-security workforce of the institutions through on-site inspections, where they have the opportunity to talk with relevant specialists. Self-assessment questionnaires are becoming common practice. Training processes are particularly scrutinised. As staff competence is integral to cyber-security, authorities have been known to raise concerns about the capability or qualifications of an institution's head of IT or information security. Jurisdictions diverge in how they regulate the roles and responsibilities of the IT and information security staff. Some jurisdictions, including Argentina, Australia, the EU, Japan and Saudi Arabia, issue regulations specifically addressing IT staff's roles and responsibilities. Sometimes regulations are embedded in a jurisdiction's global governance framework, such as those issued in Switzerland. In regulations issued by Mexico, the US, and Saudi Arabia, regulatory requirements addressing the roles and responsibilities of the IT and information security functions are encompassed by requirements for the BoD and senior management. In South Africa, such regulations are included in the national cyber-security strategy.

The range of practices and regulatory expectations for workforce competence is wide, and many jurisdictions have not formulated any. The FISC in Japan and FSI in South Korea are both examples where public authorities have set guidelines on appropriate cyber-security workforce management. In other jurisdictions, regulatory requirements for cyber-workforce management are limited to supervisory expectations, and there may be no assessment by supervisors of cyber-security skills and staff training at regulated entities. Only the Hong Kong, Singapore and the UK have issued dedicated frameworks to certify cyber-workforce skills and competencies.

Box 3

## Case study 3: Frameworks for professional training in cyber-security and certification programmes

**The Center for Financial Industry Information Systems (FISC)**, a public-private partnership, was founded in Japan in 1984 to promote the cyber-security initiatives of financial institutions. FISC facilitates the exchange of staff between financial sector supervisors, banks, and IT security vendors by partnering with the private sector and supervisors. FISC's efforts have resulted in the development of FISC Guidelines for cyber-security preparedness in Japan, as well as cyber-security education and training programs for its bankers. Bank examiners at the FSA and BoJ reference FISC Guidelines to ensure a consistent and integrated supervisory approach. The same structure can be found in the Financial Security Institute (FSI) founded in Korea in 2015. This illustrates the effectiveness of cross-border public-private partnerships when the supervisors leverage the industry for cyber-security enhancement. At a minimum, FISC's efforts serve as a model for other jurisdictions transitioning from prescriptive to more risk-based and incentive-compatible regulatory models.

**Bank of England (BoE)**: The BoE has established the CBEST accreditation for suppliers who offer threat intelligence and penetration testing services who wish to be involved in the CBEST scheme. This is in addition to the accreditation for individuals offered by the Council for Registered Ethical Security Testers (CREST), ie the CREST Certified Threat Intelligence Manager (CCTIM) for providers of threat intelligence services, and the CREST Certified Simulated Attack Manager (CCSAM) and CREST Certified Simulated Attack Specialist (CCSAS) for providers of penetration testing services.

**Monetary Authority of Singapore (MAS)**: MAS requires financial institutions to have in place a comprehensive technology risk and cyber-security training programme for the BoD. Such a programme may include periodic briefings conducted by in-house cyber-security professionals or external specialists. The goal is to help equip the BoD with the requisite knowledge to competently exercise its oversight function and appraise the adequacy and effectiveness of the financial institution's overall cyber-resilience programme.

**Hong Kong Monetary Authority (HKMA)**: The HKMA's Professional Development Program (PDP) is one of the three elements of HKMA's Cybersecurity Fortification Initiative (CFI). It seeks to increase the supply of qualified cyber-security professionals in Hong Kong SAR. The HKMA has worked with the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute (ASTRI) to develop a localised certification scheme and training programme for cyber-security professionals.

# 4. Approaches to risk management, testing and incident response and recovery

This section sets out a range of observed practices on cyber-risk management, and incident response and recovery. It aims to identify practices in the supervision of banks' cyber-resilience which could inform future work. This section is divided into four sub-sections:

- Methods for supervising cyber-resilience
- Information security controls testing and independent assurance
- Response and recovery testing and exercising
- Cyber-security and resilience metrics.

## 4.1 Methods for supervising cyber-resilience

### 4.1.1 Risk specialists assess information security management and controls

Jurisdictions apply different approaches to supervise regulated institutions' cyber-resilience. Most focus on key risks such as cyber in the context of the scale, complexity, business model and previous findings, often assigning institutions to categories to aid decisions about which institutions will be in scope for various supervisory initiatives. Guided by existing international and national legislation, a programme of supervision is then agreed spanning financial and operational resilience matters.

Half of the jurisdictions in the EU have internal guidance addressing the circumstances when the competent authority should conduct a cyber-security review. These include institutions' own risk assessments, findings from on-site inspections or questionnaires, and incidents (eg cyber incident trend analysis).

Risk specialists typically draw on documentary evidence including survey responses, physical inspections, incident reports, and in-person meetings to assess the adequacy of controls in place. Many supervisory expectations are aligned with industry standards (eg COBIT, NIST) but approach, depth and breadth of supervisory assessments vary between jurisdictions.

Most jurisdictions undertake off- and on-site reviews and inspections of regulated institutions' information security controls to assess compliance with regulatory standards and alignment with good practice.[12] Reviews are completed either as part of general technology assessments or risk management assessments more broadly. They tend to focus on governance and strategy, management and frameworks, controls, third-party arrangements, training, monitoring and detection, response and recovery, and information-sharing and communication.

The number, type, and nature of regulated institutions vary by jurisdiction, as do the size of the specialist risk teams of the regulator. Some jurisdictions (eg Australia, Brazil and Singapore) have developed approaches to equip front-line supervisors with knowledge and tools to assess (triage) IT risk issues. Techniques used include guidelines on how to identify and evaluate IT risk, questionnaires, risk assessments and tools to quantify risk assessments. Additionally, a number of jurisdictions (eg Australia and the UK) have powers to appoint an auditor or other third party to provide a report to the regulator on a particular aspect of the regulated institutions' risk management, including cyber.

### 4.1.2 Jurisdictions increasingly engage with industry to address cyber-resilience

Industry engagement is used to either influence industry behaviour, or to seek feedback and views to inform regulatory work. For instance, the French Autorité de Contrôle Prudentiel et de Résolution (ACPR) and the UK Prudential Regulation Authority (PRA) both released discussion papers, on IT risk and operational resilience respectively, in 2018.[13] Common methods of engagement also include speaking at conferences and other communications to reach a range of regulated entities and industry participants.[14]

Some jurisdictions include third-party service providers in this engagement. In the EU, both the European Commission EU FinTech Lab and the EBA FinTech Knowledge Hub have organised events with regulators, supervisors, industry and third-party service providers. Communicating key messages through these channels can be faster and more responsive.

## 4.2 Information security controls testing and independent assurance

### 4.2.1 Mapping and classifying business services should inform testing and assurance

Most jurisdictions (eg Australia, the EU, Hong Kong, Singapore and the US) recognise the importance of mapping and classifying business services and supporting assets and services as a basis for building resilience. A clear understanding of business services and supporting assets (and their criticality and sensitivity) can be used to design testing and assurance of end-to-end business services. This is typically completed as part of business impact analysis, recovery and resolution planning, reviewing dependency of critical services on external third parties, and scoping for assessments.

[12] On-site reviews usually consist of one or more meetings with regulated institutions at their premises. Off-site reviews usually consist of desk-based assessment of documentation or a meeting at the office of the regulator.

[13] See ACPR, "IT Risk", *Discussion Paper*, March 2018, www.acpr.banque-france.fr/sites/default/files/medias/documents/it_risk.pdf; and Bank of England and Financial Conduct Authority, "Building the UK financial sector's operational resilience", *Discussion Paper*, July 2018, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

[14] Publications used include white papers, information papers, annual reports and in some cases letters to industry.

A number of jurisdictions assess institutions' monitoring and surveillance of emerging threats, including real-time detection capability, ability to detect adversaries before they move between systems and relevant continuity and control policies. Some jurisdictions perform thematic reviews (eg Sweden completed a review of institutions' access controls and management of user access rights), while some members use existing international standards, applying them to other types of institution (eg South Africa applies the CPMI-IOSCO guidance on cyber-resilience for FMIs to banks).

Independent assurance also provides management and regulators with an evaluation of whether appropriate controls have been implemented effectively. Jurisdictions commonly also leverage the management information outputs of these activities, providing the regulator with another source of information for their own assessments.

### 4.2.2 Penetration testing

Cyber-security controls are implemented through risk-based decisions against a regulated institution's risk appetite. Regulated institutions typically test information security controls applied to hardware, software and data to prevent, detect, respond and recover from cyber-incidents.

Supervisors review and challenge regulated institutions' approach to testing controls and the remediation of issues identified. This can include reviewing survey responses, threat and vulnerability assessments, risk assessments, audit reports and control testing reports (eg penetration testing, health checks).

Five EU jurisdictions have developed programmes of regulator-led penetration tests and three (the ECB, the Netherlands and the UK) have provided guidance for regulated institutions on how to test. Tests are typically voluntary, funded by the regulated institution and targeted at larger, more systemic institutions. In particular, threat-led red team penetration tests delivered by third-party threat intelligence and penetration testers are becoming more widespread. The majority of directed penetration tests focus on regulated institutions' protective and detective cyber-resilience capabilities, while a few also test response and recovery capabilities.

In May 2018, the ECB published the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU),[15] which is the first Europe-wide framework for controlled and bespoke tests against cyber-attacks in the financial market. The framework facilitates testing for cross-border entities under the oversight of several authorities. It is up to the relevant authorities and the entities themselves to determine if and when TIBER-EU based tests are performed. Tests will be tailor-made and will not result in a pass or fail – rather they will provide the tested entity with insight into its strengths and weaknesses, and enable it to learn and evolve to improve cyber-maturity.

### 4.2.3 Taxonomy of cyber-risk controls

While putting cyber-risk controls in place is only one aspect of building cyber-resilience, many jurisdictions find review of controls a ready way to engage with regulated institutions. Some jurisdictions use taxonomies of controls to understand whether there are any gaps in the coverage of their

[15] ECB, "ECB publishes European framework for testing financial sector resilience to cyber-attacks", press release, 2 May 2018, www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html.

supervisory approach. Currently the taxonomies are jurisdiction-specific and do not rely on harmonised concepts and definitions. If an authority is unable to assess a particular type of control, for example because it has no supervisory approach, assessment method or the required skillset to assess the control, then that is identified as a gap. An example taxonomy of cyber or information security controls is included in Annex A.

## 4.3 Response and recovery testing and exercising

### 4.3.1 Evaluation of service continuity, response and recovery plans and continuous learning

Evaluation of service continuity plans focuses on reviewing alignment with institutions' risk management frameworks, the business continuity management strategies chosen, IT disaster recovery arrangements and data centre strategies.

The majority of regulators require entities to establish a framework or policy for prevention, detection, response and recovery activities, including incident reporting. Specific requirements vary across supervisory authorities, and most are not specific to cyber-risk. Indeed, few regulators have issued cyber-specific business continuity or disaster recovery regulatory requirements for the sector. A few jurisdictions, like China and India, have prescribed cyber-incident response framework to be a key component of cyber-governance. The US also has supervisory guidance regarding incident management, covering identification of indicator of compromise, analysis and classification of events and escalation and reporting of incidents. Some authorities, such as the Japanese Financial Services Agency (JFSA) and Bank of Japan, also focus on potential threats and information-sharing to minimise delays in reporting cyber-incidents.

Evaluation of regulated institutions' incident response and recovery plans focuses on how plans are triggered, institutions' ability to implement plans, preservation of data and specific actions for "critical" technology. In Canada, the assessment of a bank's internal and external communication plans and protocols seeks to determine if all relevant stakeholders are included, to avoid contagion.

Several jurisdictions (eg Australia, Belgium, Hong Kong, Japan and the US) complete a supervisory review of post-incident learning. This is conducted through the discussion of regulated institutions' response and the root cause analysis, but no further standard practice could be observed.

### 4.3.2 Joint public-private exercising

Distinct from testing, most supervisors and banks use exercises to train and practice how they would respond to an incident. Cross-border international exercises have made this more visible. Examples include the UK/US exercise Resilient Shield (Box 4) and the TITUS exercise in 2015,[16] as well as the G7 exercise under planning in 2018.

[16] TITUS was a crisis communication exercise for euro area financial market infrastructures held in November 2015.

In the UK, the Sector Exercising Group (SEG), which is a subgroup of the Cross Market Operational Resilience Group (CMORG), manages the sector's annual exercise regime, which incorporates cyber-specific scenarios.[17] In Japan, the JFSA has conducted tabletop exercises to improve cyber-security, and in particular communication and coordination of response mechanisms. Over 100 regulated institutions including banks, credit unions, insurance companies and securities companies participated in the 2017 exercise, which covered two cyber-scenarios. A summary of results was then published to enable others to draw lessons from the exercise.

Box 4

## Case Study 4: "Exercise Resilient Shield"

One example of an international public-private exercise was UK/US "Exercise "Resilient Shield in 2015 – a joint exercise with leading global financial firms to enhance cooperation and ability to respond effectively to a cyber-incident in the finance sector. The exercise was not a test of individual financial firms or financial systems, but was designed to improve understanding across governments and industry of information-sharing, incident response handling and public communications.

Participants included UK and US supervisory authorities, government departments and cyber-agencies. The exercise examined how the UK and US could enhance cyber-security cooperation by:

- enhancing processes and mechanisms for maintaining shared awareness of cyber-security threats between US and UK governments and the private sector;
- furthering mutual understanding of each country's cyber-security information-sharing processes and incident response coordination structures, including scenarios that may call for a coordinated response and public communications; and
- exchanging best practices domestically and between the US and UK on a government-to-government and government-to-financial sector basis.

The exercise did not:

- amount to a "cyber war game" or include live play;
- test the actions of law enforcement or the security and intelligence agencies;
- seek to involve the entire range of the UK and US finance sectors; or
- seek to test individual firms or financial systems, but instead rehearse communication and coordination links.

[17] CMORG is a UK industry forum which is co-chaired by the Bank of England and UK Finance and attended by senior representatives from regulated institutions.

## 4.4 Cyber-security and resilience metrics

### 4.4.1 Cyber-security and resilience metrics are not yet mature

Some jurisdictions have methodologies to assess or benchmark regulated institutions' cyber-security and resilience. Those jurisdictions that have developed ways to assess cyber-security and resilience have focused on reported incidents, surveys, penetration tests and on-site inspections. None of these methodologies produce quantitative *metrics* or risk indicators comparable to those available for financial risks and resilience, eg standardised quantitative metrics where established data are available. Instead, *indicators* provide information on regulated institutions' approach to building and ensuring cyber-security and resilience more broadly. Supervisory authorities also rely on entities' own management information, although this differs across entities and is not yet mature.

### 4.4.2 Emerging forward-looking indicators of resilience

It is common for jurisdictions (and often regulated institutions themselves) to focus on backward-looking indicators of the performance of the technology function. These indicators are presented to Board members and executives as part of management information that regulators may review (examples can be found in Annex B).

Backward-looking indicators comment on past performance as an indicator of future performance, which is reasonable when institutions' operations and risk environment are relatively stable over time and more or less independent from outside influences. However, cyber-risk frustrates this because adversaries are dynamic, themselves adapting to institutions' responses and protective measures, sometimes changing their tactics and strategies even in the space of a single cyber-incident. Distributed denial of service (DDOS) incidents are a good example, where the volume and scale of disrupted internet traffic generated has increased significantly in the last two years and adversaries adapt their techniques in response to an institution's defences. While backward-looking metrics continue to be important, jurisdictions are increasingly recognising the need for forward-looking indicators as direct and indirect metrics of resilience, indicating whether a regulated institution is likely to be more or less resilient in the event of a risk crystallising.

Regulated institutions are also seeking to improve metrics for resilience more broadly. Annex C contains cyber-centric metrics collated by a sample set of regulated institutions for decision-making bodies (boards and board sub-committees). It is notable that the data provided typically allow for trend information so that the reviewer can assess if the situation is getting better or worse. Some metrics track compliance with internal policies while others measure inherent risk. Patch ageing in particular is a widespread and comparable metric.

This list of cyber-metrics collated by regulated entities can be reviewed by regulators to gain insight into what may be collected across the regulated population to gain an enhanced set of cyber-metrics for measuring the state of cyber-resilience more broadly. Collectively, these indicators can inform on the broad adequacy of an institution's cyber- and operational resilience levels for its business needs and risk appetite. However, no single item taken in isolation is seen as a sufficient metric, and no standard set of indicators has been identified so far to provide a meaningful benchmark.

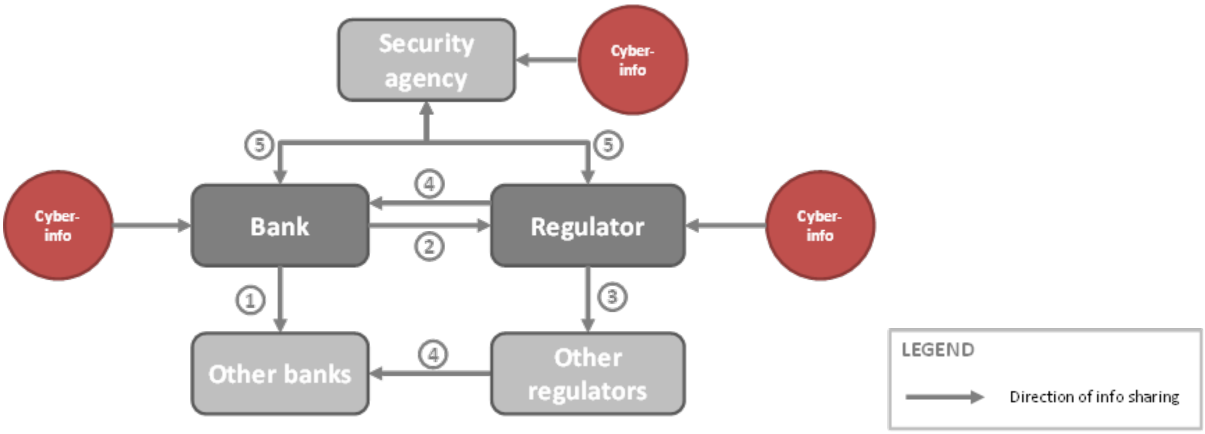
A number of jurisdictions (eg Australia, Canada, the ECB-SSM, Hong Kong, Singapore, the UK and the US) analyse survey responses to assess regulated institutions' capabilities and inform prioritisation of follow-up work. The outcomes of this work tend to be institution-specific findings and remediation or action plans which can be monitored over time, and/or thematic reports. As such, they provide indicators and trends if performed on a regular basis. Results from the Australian surveys are subsequently published to influence industry behaviour. In the UK, thematic findings are often shared with participating firms for the same purpose.

# 5. Communication and sharing of information

Most Basel Committee jurisdictions have put in place cyber-security information-sharing mechanisms, be they mandatory or voluntary, to facilitate sharing of cyber-security information among banks, regulators and security agencies. These communications are established for multiple purposes, including helping relevant parties defend themselves against emerging cyber-threats.

This section sets out a range of observed cyber-security information-sharing practices among banks and regulators. For the purpose of this report, they are divided into five categories according to the parties involved in the sharing. Figure 1 illustrates the interlinkages of the five types of practices.

Figure 1: Interlinkage of different types of cyber-security information-sharing practices (1)

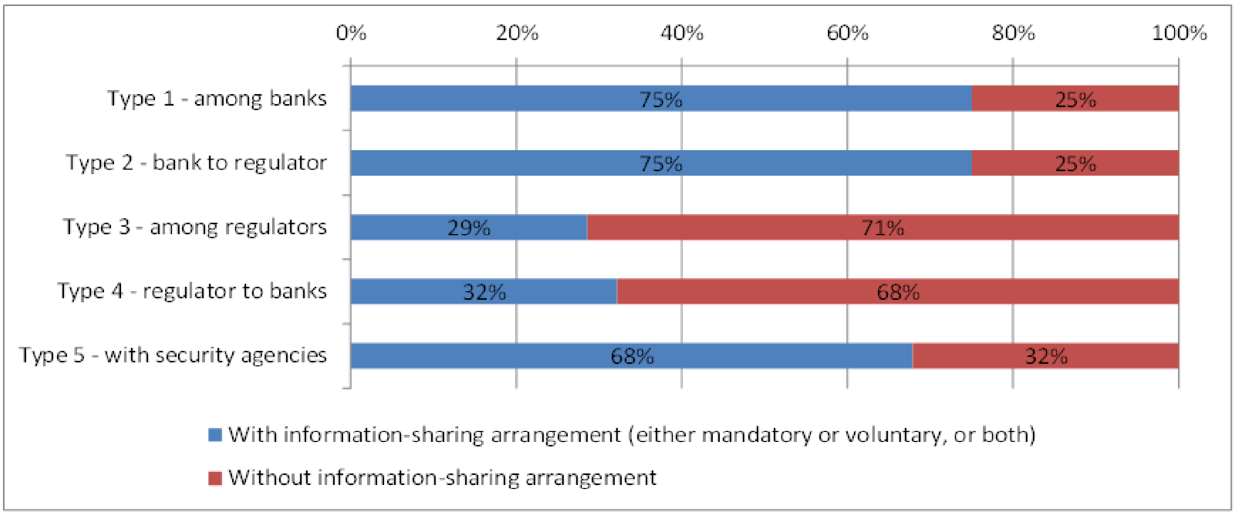


(1) the numbered circles next to the arrows indicate the “types” of info sharing as described in section 5.1 and Figure 2
Source: Basel Committe on Banking Supervision.

## 5.1 Overview of information-sharing frameworks across jurisdictions

Among the five types of cyber-security information-sharing practices, sharing among banks; sharing from banks to regulators and sharing with security agencies are the most commonly observed. Sharing among regulators is the least observed type. This is partly due to the less systematic nature of information-sharing arrangements between regulators, where it can happen on an ad hoc basis at a bilateral level or within supervisory colleges, under specific circumstance. Figure 2 illustrates the adoption rate of different types of cyber-security information-sharing, both mandatory and voluntary, by the jurisdictions covered by this report.

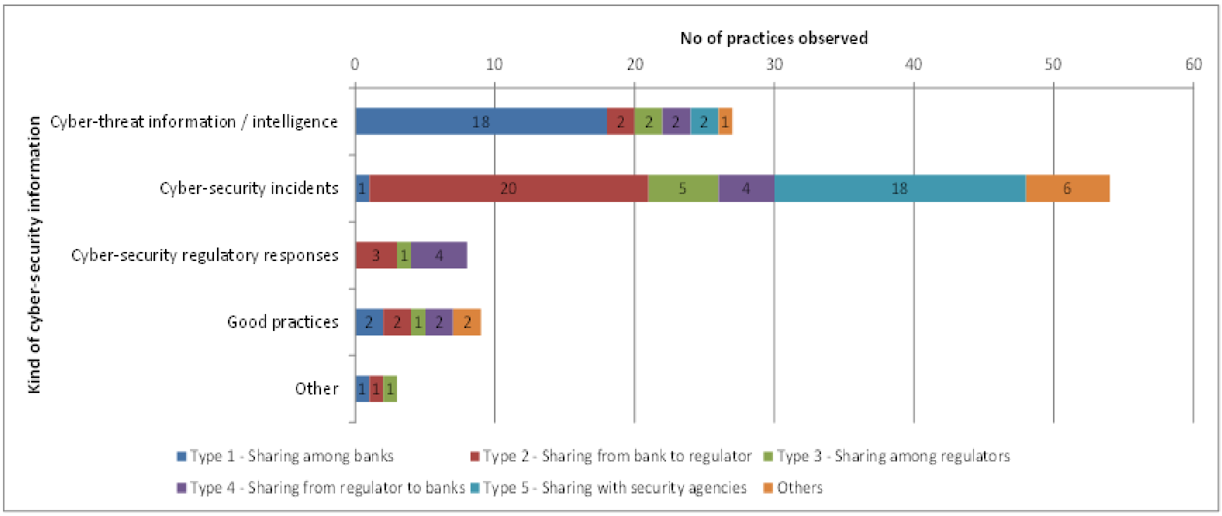
Figure 2: Percentage of jurisdictions with/without information-sharing arrangement



Source: Basel Committee on Banking Supervision.

Different kinds of cyber-security information are shared by banks and regulators, including cyber-threat information, information related to cyber-security incidents, regulatory and supervisory responses in case of cyber-security incidents and/or identifications of cyber-threat, and best practices related to cyber-security risk management. Depending on the type of arrangement, the kind of information shared varies. For instance, information related to cyber-security incidents is more widely observed in sharing from banks to regulators and with security agencies, whereas cyber-threat information/intelligence is the most common kind of information shared among banks.

Figure 3: Kinds of information shared



Source: Basel Committee on Banking Supervision.

Various jurisdictions have put in place certain cyber-security information-sharing arrangements to facilitate more effective sharing of cyber-security information by banks and regulators. Full adoption of all types of information-sharing arrangements within a jurisdiction is still exceptional.

That said, it was also noted that for jurisdictions with observed practices of information-sharing among banks, there are less observed practices of information-sharing from regulators to banks. This is probably attributable to the lesser need for sharing by regulators to banks if an effective peer sharing mechanism among banks already exists. Similarly, jurisdictions with observed practices of information-sharing from banks to regulators display lower rates of sharing with security agencies, potentially due to the allocation of responsibilities for cyber-security information processing among regulators and security agencies within a jurisdiction.

For some of the jurisdictions, both mandatory and voluntary information-sharing arrangements are noted for the same type of information-sharing arrangement. This is because voluntary/mandatory sharing is sometimes applicable when different types of information are being shared, or when information is shared with different parties. For example, there is a mandatory requirement in Singapore for financial institutions to report relevant cyber-security incidents to MAS, while cyber-threat information exchange between MAS and the Cyber Security Agency (CSA) is voluntary.

Other types of information-sharing arrangements are observed, which include public announcement/disclosure of information about cyber-security incidents and cross-sector information-sharing with public and private institutions. In particular, the range of stakeholders involved in cyber-attacks typically includes non-bank critical infrastructure operators, third-party service providers and customers who could contribute to sharing information with security agencies for further distribution to other sectors, or be part of other setups such as a joint-industry groups. [18]

The remainder of this section summarises common practices adopted by various jurisdictions, describes more specific practices adopted by individual jurisdictions and summarises key gaps observed.

## 5.2 Sharing among banks

Banks share information (eg knowledge of a cyber-security threat) with peer banks through established channels, mainly to allow peer banks to take more timely action in response to similar threats. Although there is no common standard for automated information-sharing, regulators in most jurisdictions are not directly involved in bank-to-bank information-sharing but do play a role in facilitating the establishment of voluntary sharing mechanisms for cyber-vulnerability, threat and incident information, and in some cases indicators of compromise.

Some jurisdictions have established public sector platforms to accomplish information-sharing initiatives while others have encouraged private sector development of information-sharing organisations. Three jurisdictions (Brazil, Japan and Saudi Arabia) have mandated cyber-security information-sharing among banks through regulations or statutes.

[18] This “other” type of information is shown in Figure 3. One example is the EBA guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05) and recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), which assumed good information-sharing of IT risks between banks and supervisors, although there was no specific requirement for banks to report security incidents to their supervisors.

Box 5

## Case Study 5: FS-ISAC – key features and benefits

The Financial Services Information-sharing and Analysis Center (FS-ISAC) is a non-profit entity established in 1999 to collect and provide financial services sector member organisations with information on potential vulnerabilities as well as timely, accurate and actionable warnings of physical, operational and cyber-threats or attacks on the national financial services infrastructure. Its members include banks, credit unions, insurance companies, investment companies, financial services regulators and law enforcement entities.

In addition to the core information-sharing platform, the FS-ISAC hosts conferences and educational seminars, conducts sector and cross-sector contingency planning exercises, and is an internationally recognised source for threat intelligence information. Core elements of the FS-ISAC include:

- Rapid response: the FS-ISAC analyses and disperses information and threat intelligence information among its members through their proprietary real-time Critical Infrastructure Notification System (CINS).

- Information analysis and sharing: the FS-ISAC receives information from many sources that is verified and classified by type and severity. The information is then sent out by CINS and reaches members instantly. FS-ISAC also conducts crisis calls if necessary, and has a team working 24/7 to analyse any incoming data and disseminate information.

- Anonymised data: Information received and disseminated through the FS-ISAC is considered confidential and stored in a standalone, secure portfolio so that no threat or information can be traced back to its source by any members and all information is anonymously shared. This makes the FS-ISAC a safe place for its members and encourages sharing.

- Member-driven: The members of the FS-ISAC run the organisation, tailoring it specifically for the needs of the financial industry.

- Recognised by US Financial Services Regulators: the Federal Financial Institutions Examination Council, a group consisting of federal and state US financial services regulators, has recognised the FS-ISAC as a key threat intelligence source and recommends financial institutions participate in its process to identify, respond to and mitigate cyber-security threats and vulnerabilities.

Outside the information-sharing and analysis centre construct, some jurisdictions have established public/private forums or government-led centres for information-sharing. In some jurisdictions, local regulations on data protection are perceived to be an obstacle to cyber-security information-sharing among banks and may warrant a specific dialogue between banks and their local or regional regulators.

Sharing of information and collaboration among banks depend on the financial industry's culture and level of trust among participants. Experience shows that a two-level information-sharing structure through which information would be first shared on the interpersonal level with a closer group and then be exchanged at the company level with a broader group of banks helps build trust into the system.

## 5.3 Sharing from banks to regulators

The sharing of cyber-security information from a bank to its regulator(s)/supervisor(s) is generally limited to cyber-incidents based on regulatory reporting requirements. Such requirements are mainly established to (i) enable systemic risk monitoring of the financial industry by regulator(s); (ii) enhance regulatory requirements or issue recommendations by regulator(s) to adjust policies and strategies based on information collected; (iii) allow appropriate oversight of incident resolution by regulator(s); and (iv) facilitate further sharing of information with industry and regulators to develop a cyber-risk response framework.

Reporting requirements are established by different authorities for specific purposes depending on their mandate (eg supervisory and regulatory functions, consumer protection and further distribution of information to national cyber-security agencies for systemic operators). Incident reporting by banks to regulator(s) is a mandatory requirement in many jurisdictions, with different scopes of requirements and ranges of application. For jurisdictions already enforcing the requirement in the past, the reporting obligation has a broader operational incident scope, including cyber-incidents. The perimeter can include all supervised institutions but is more often limited to systemically important institutions. Nearly all institutions regulated in the EU are required to report cyber-security incidents to the competent authorities. The requirements stem from supervisory frameworks (such as the Single Supervisory Mechanism (SSM) cyber-incident reporting framework), EU directives (PSD2, NIS) and local law. Some requirements also include the obligation to submit a root cause analysis for the incident, or a full post-mortem or lessons learnt after the incident.

Different scopes and perimeters may depend on the type of authority (eg supervisors, regulators, national security) and their mandate (ie national cyber-security agencies, consumer protection, banking supervision, etc), sector(s) involved (eg multisector or specific: banks, significant banks, systemic operators, payment) and geographical range (eg national, multiregional). While many of the supervisors focus only on reporting and tracking incidents that have already taken place, some require proactive monitoring and tracking of potential cyber-threats because concerns about reputational risk may lead to a delay in incident reporting by the regulated entity.

Based on these considerations, different reporting frameworks are also observed. These range from formal communications to informal communications (eg free-text updates via email or verbal updates over the phone).

Differences are noted in: (i) taxonomy for reporting; (ii) reporting time frame (immediately, after two hours, after four hours and after 72 hours are examples of practices observed); (iii) templates; and (iv) threshold to trigger an incident reporting. These differences highlight the fragmentation issue facing the banks operating in multiple jurisdictions or supervised by different authorities, as these banks are likely to be obliged to fill in various templates with different taxonomy, reporting time frame and threshold. This may increase their regulatory burden, consuming significant resources to ensure compliance. It may be possible for an authority with multiple functions to receive from a bank multiple reports with distinct formats for multiple times.

All incident reporting processes have a single direction flow, by a bank to an authority, although an informal flow back can be used for alerting firms in case of an incoming threat. By normalising the prompt exchange of information between banks and supervisors, reciprocal flow mechanisms can help remove the possible stigma associated with incident reporting by banks, thereby fostering effective and timely incident reporting.

## 5.4 Sharing among regulators

Regulators share information with fellow regulators, be they domestic or cross-border, as appropriate according to established mandatory or voluntary information-sharing arrangements. Cyber-security information shared among regulators may include regulatory actions, responses and measures. Considering different types of cyber-security information-sharing, information-sharing among regulators is the least observed practice across jurisdictions, although it is expected that many informal and ad hoc communication channels exist, such as through supervisory colleges and memoranda of understanding. Cyber-fraud is becoming more sophisticated and cross-jurisdiction, and sharing of cyber-security information among regulators could assist in maintaining awareness of the cyber-threat situation for timely guidance to be provided to banks to protect financial systems against cyber-frauds.

Box 6

### Case study 6 – Bilateral cyber-security information-sharing between the Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS)

Given the importance of facilitating more cross-border cyber-security information-sharing, the HKMA and MAS established a bilateral cyber-security information-sharing framework in the first quarter of 2018.

As part of the framework, the HKMA and MAS have agreed upon four important guiding principles and key design features of the governance arrangement, the scope of information-sharing, a traffic light protocol, standard taxonomy and dedicated communication channels.

- *Voluntary:* Given that some cyber-security information may be highly sensitive, the sharing of information under the framework should be voluntary, without creating any legal obligations for the participating authorities.

- *Timely:* The HKMA and MAS recognise that timely sharing of cyber-security information is of paramount importance to building an effective framework. The authorities have therefore agreed that information about cyber-security incidents should be shared as soon as possible to the extent permitted by law. If a cyber-security incident is assessed to have the potential to spread to other jurisdictions, the related information should be shared within 24 hours. Incomplete information about cyber-security incidents can be shared so long as a reasonable degree of validity has been ascertained.

- *Effective:* To ensure the efficacy of the framework, sharing of cyber-security information should not be limited to information related to those financial institutions with an operation in both jurisdictions (ie unlike typical supervisory college or memoranda of understanding, "supervisory locus" is not required to be established). A taxonomy was also established with reference to the Structured Threat Information eXpression (STIX) framework.

- *Confidential:* The confidentiality of any information shared between the authorities should be properly protected. The framework will focus on the sharing of general information such as the modus operandi of the attacks. The authorities also adopted a Traffic Light Protocol (TLP) for subsequent sharing of information.

The HKMA and MAS have been exchanging information regarding real-life cyber-threats and cyber-security-related regulatory responses and measures since April 2018.

## 5.5 Sharing from regulators to banks

Information-sharing from regulators to banks occurs through established channels, based on the information the regulator receives both from banks and other sources. Various jurisdictions (eg Australia, China, Korea, Saudi Arabia, Singapore, Turkey and the US) have established clear guidance in the form of standards and practices to enable cyber-security information-sharing by regulators to banks. In these jurisdictions, information flows from the bank to the regulator, and the regulator assesses the risk to the financial industry and shares the information with the industry, as appropriate, based on the risk assessment. In cases where the information is sensitive (eg contains customer-specific or bank-specific information), the regulator anonymises or summarises it to allow sharing.

Regulators with a regulator to bank sharing mechanism more readily share publicly available information such as cyber-security risk management best practices. They use informal channels such as industry sharing platforms (eg participation in industry forums), meetings and informal communications to disseminate information to the banks.

In cases where non-public information is obtained by regulators, the information is shared with selected parties via informal meetings or other informal communication vehicles, so as to preserve anonymity and confidentiality of the institution(s)/bank(s) impacted by a cyber-attack, and maintain banks' confidence and trust in the regulators generally.

Mandatory requirements for regulators to share information with banks have only been established for a few jurisdictions (eg China). A few other jurisdictions have put in place practices for voluntary sharing (eg Singapore, the UK). However, many jurisdictions have not put in place any standard practices for regulators in the sharing of information with banks, nor established any process or time frame to enable timely, risk-based information-sharing. Classification of information could ensure that the appropriate audience could receive the appropriate information and help to build trust between regulators and banks.

## 5.6 Sharing with security agencies

This section examines sharing of information by banks or regulators with the security agencies operating in their respective jurisdictions.

Given that cyber-security incidents encountered by banks or regulators could potentially be experienced by entities in other sectors, effective communication of relevant cyber-security incidents with security agencies could facilitate broader awareness of cyber-threats in a timely manner, and enhance defensive measures against adversaries.

For jurisdictions with operations of Computer Emergency Readiness Team (CERT) or similar security agencies, these agencies may act as focal points for cyber-security incident notification. Banks or regulators share cyber-security information with these agencies for broader circulation of information and collaboration with other sectors within the country (eg public sector, civilian sector, computer community).

Jurisdictions have generally set out standards and practices for critical infrastructure entities and regulators to share cyber-security information with national security agencies. While most jurisdictions adopt a voluntary approach, a few jurisdictions mandate formal sharing requirements. Some jurisdictions (eg Luxembourg, the US) have established sharing platforms to facilitate multilateral sharing of cyber-security incident or cyber-threat information. In the US, an online portal is available for cyber-security information to be submitted to the National Cyber-security and Communications Integration Center and the US CERT. In Luxembourg, the Computer Incident Response Center (CIRCL) has established a Malware Information-sharing Platform (MISP) to gather, review, report and respond to computer security threats and incidents. The MISP allows organisations to share information about malware and their indicators. The aim of this trusted platform is to help improve the counter-measures used against targeted attacks and set up preventive actions and detection.

For jurisdictions with mandatory requirements for cyber-security incident information-sharing with national security agencies (Canada, France, Singapore and Spain), the sharing arrangements are bilateral in general. Instead of requiring banks or regulators to share all cyber-security incidents, these jurisdictions require cyber-security incidents affecting key operators of critical infrastructure to be reported.

Some jurisdictions have established procedures for relevant information to be exchanged voluntarily and bring together relevant parties for coordination of responses to incidents. In the UK, the Authorities Response Framework can be invoked by financial authorities to bring together the Financial Conduct Authority (FCA), the Bank of England, the Treasury, the National Crime Agency and the National Cyber-security Centre to coordinate their response to a cyber-security incident. Meetings and formal communications can be triggered as appropriate.

Box 7

## Case study 7– Computer Security Incident Response Teams (CSIRTs) in the EU

The Network and Information Security (NIS) Directive is a component of EU legislation with the specific objective to improve cyber-security throughout the EU. The requirements came into full effect on 10 May 2018. The NIS Directive defines different obligations across the EU, one of which concerns the establishment of one or more Computer Security Incident Response Teams (CSIRTs) at national level for comprehensive incident management nationwide. Incident reporting notification to national CSIRTs (directly or through a competent authority) is mandatory for entities identified as Operators of Essential Services (OES) and Digital Service Providers (DSP) (some banks have been included in the first category). In some countries, competent authorities for banks that have been identified as OES[19] are the supervisory authorities, while in others it can be the Ministry of Finance or a specific government authority. The NIS Directive also established the requirements to have a CSIRTs European network (ie a dedicated network for all national CSIRTs, run by the member states, with its secretariat provided by the European Network and Information Security Agency) with the following competencies:

- Exchange information on services, operations and cooperation capabilities

[19] As required by the NIS Directive, identification of OES should have been completed by October 2018.

- Exchange and discussing information related to incidents and associated risks (on request, on a voluntary basis)
- Identify a coordinated response to an incident (on request)
- Providing member states support in addressing cross-border incidents (on a voluntary basis)
- Issue guidelines concerning operational cooperation
- Discuss, explore and identify further forms of operational cooperation (risks and incidents, early warnings, mutual assistance, coordination)
- Discuss the capabilities and preparedness of certain CSIRTs (on request from that CSIRT)

## 6. Interconnections with third parties

All jurisdictions recognise the challenge of gaining assurance of an entity's cyber-resilience, a challenge both for regulators with regard to financial institutions, and for financial institutions with regard to their third-party service providers. Extensive use of third-party services increases the challenge for jurisdictions and regulated institutions themselves to have full sight of the controls in place, and the level of risk. For the purpose of identifying the range of practices in relation to cyber-resilience, "third parties" is understood in a broad sense, including: (i) all forms of outsourcing (including cloud computing services); (ii) standardised and non-standardised services and products that are typically not considered outsourcing (power supply, telecommunication lines, commercial hardware and software, etc); and (iii) interconnected counterparties such as other institutions (financial or not) and FMIs (eg payment and settlement systems, trading platforms, central securities depositories and central counterparties).

Cyber-resilience practices in relation to third parties are analysed across the following areas:

- Governance of third-party interconnections
- Business continuity and availability
- Information confidentiality and integrity
- Specific expectations and practices regarding visibility of third-party interconnections
- Auditing and testing
- Resources and skills

## 6.1 Governance of third-party connections

### 6.1.1 Widespread expectations and practices

Regulations across different jurisdictions require that institutions develop a management- and/or board-approved outsourcing (or organisational) framework that defines the applicable roles and responsibilities, the outsourceable activities and concrete conditions for outsourcing, the specific risks that need to be analysed (either prior to selection of a provider or when substantially amending/renewing an agreement) and recurrent obligations (such as monitoring procedures or regular risk assessments).

Regulators typically also require that institutions implement a contractual framework, defining generic rights, obligations, roles and responsibilities of the institution and the service provider, specifying the responsibility for reviewing, approving and signing contracts (eg involvement of a cyber-security function), with specifications on the result (ie an official, written and detailed contract) and the applicability of the framework (typically also for intragroup outsourcing).

The regulatory expectations on risk assessments and contracts tend to specify in a rather comprehensive way which risks (and mitigating measures) to cover, albeit mostly in general terms. Next to a description of the nature of the service, the expected results of the outsourcing, and the roles and responsibilities of the service provider and the financial institution, risk assessments and contracts are expected to include analysis and clauses on strategic risk, compliance risk, security risk (typical areas of attention are security monitoring, patch management, authentication solutions, authorisation management and data loss/breach procedures), business continuity risk, vendor lock-in risk (the general ability of an institution to withdraw from the service provider and to absorb the outsourced activity or transfer it to another service provider), counterparty risk (the visibility into the service provider's organisation), country risk, contractual risk, access risk (meaning that financial institutions and/or supervisors cannot audit the third-party connection due to inadequate contractual agreements) and concentration risk.[20]

Along with the outsourcing and contractual frameworks, regulators typically expect that information, cyber-security and/or continuity frameworks address some crucial aspects of third-party arrangements to ensure the availability of critical systems and the security of sensitive data that are accessible to, or held by, third-party service providers. These aspects include the identification and prioritisation of interconnections, as well as the classification and response to incidents with third parties according to service agreements and the communication of these policies to relevant external parties.

As regards supervisory practices, the following activities appear to be widespread:

[20] "Concentration risk" in this context does not refer to the potential systemic risk to the industry as a whole, but rather to the potential lack of control of an individual firm over one single provider as multiple activities are outsourced to the same service provider. These different aspects of concentration risk are explained in Joint Forum, Outsourcing in financial services, February 2005; and Committee of European Banking Supervisors, *Guidelines on outsourcing*, December 2006.

- Intrusive on-site inspections with respect to cyber-risk in relation to outsourcing. During such inspections, the outsourcing framework, the applicable processes and the completeness and adequacy of specific risk assessments and contracts will typically be reviewed.

- As part of their off-site supervision practices, most jurisdictions receive periodic statements or reports that assess the outsourcing policies and risks at the financial institution. These reports will typically contain statements on the existence and adequacy of outsourcing policies, processes, risk assessments and contracts.

### 6.1.2 Expectations on the scope of the ecosystem and management of third parties

Some international standards explicitly recognise that institutions may critically depend on third-party interconnections, other than those that are typically considered outsourcing. The CPMI-IOSCO guidance on cyber-resilience for FMIs discusses the identification of cyber-risks and the coordination of resilience efforts from the perspective of the ecosystem of an FMI. The ISO 27031 standard specifies requirements for hardware, software, telecoms, applications, third-party hosting services, utilities and environmental issues, such as air conditioning, environmental monitoring and fire suppression.

Some jurisdictions require that financial institutions enter into a prior agreement with their clients when they offer financial services via the internet that involve the consultation and management of personalised data or carrying out transactions (eg precise description and demarcation of the responsibilities of each party in using the technologies provided or recommended by the institution for the purpose of identifying and authenticating the client and validating the transactions).

In Luxembourg, authorities have put in place a specific regulation for companies that supply specialised services to financial institutions. For these "financial sector professionals", the same regulation for authorisation and ongoing supervision applies as for the financial institutions themselves (Box 8).

Consistent with the expanding scope of supervisory scrutiny or regulated entities, in Europe legal mandates that regulate interaction between institutions, supervisors and third-party providers are provided by the Mifid II Directive, and 12 competent authorities can directly review third parties involved in IT services. In addition, specific expectations for control and location of data are starting to emerge in the form of requirements that the location of at least one data centre for cloud computing services provided in the country or region (eg in the EU) be identified, or data ownership, control (Australia) and location (Brazil and France) be identified and monitored as part of the outsourcing agreement. Some jurisdictions (Germany, Singapore and Switzerland) further require a contractual clause that reserves the right for institutions to intervene at, or give directives to, the service provider.

Beyond the assurances required prior to engaging with third parties, most jurisdictions also require either prior notification or prior authorisation of material (cloud) outsourcing activities. To this end, jurisdictions have created questionnaires/templates (sometimes specifically for IT outsourcing or cloud computing). Although these are not harmonised in their coverage and metrics across jurisdictions, they facilitate the creation and documentation of risk assessments locally.

By focusing on the products and services themselves, new expectations for secure development and procurement also contribute to making regulations and practices future-proof. In particular, specific requirements (eg regarding "internet of things" systems in Japan) are in place for systems to be designed, developed and operated under the principle of security by design, considering that many individual devices, applications and systems will be interconnected in the future, providing new opportunities and possibly introducing new vulnerabilities.

Box 8

## Case study 8: Regulated/certified third parties in Luxembourg

The Luxembourg government has put in place a specific regulation for companies that supply specialised services to financial institutions. For these "financial sector professionals" (PSFs), the same regulation for authorisation and ongoing supervision by the Commission de Surveillance du Secteur Financier (CSSF) applies as for the financial institutions themselves. PSFs that exclusively offer operational services are called support PSFs. By regulating and supervising technical, administrative and communications-related activities, the Luxembourg government seeks to facilitate the outsourcing of core activities by ensuring a high quality of service and professional confidentiality. If a financial institution is outsourcing to a PSF, the ultimate responsibility remains with the institution, in accordance with the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing. However, in some cases it is observed that an institution is more enticed to neglect its monitoring and audit obligations, as it might consider them to be performed by the supervisor.

Cloud service providers (CSPs) are not subject to this regulation. The Luxembourg regulator (CSSF) defined specific criteria for outsourcing that will be considered IT outsourcing based on a cloud computing infrastructure. If these criteria are met, the specific obligations of CSSF circular 17/654 on cloud computing apply. An institution can outsource directly to a CSP or indirectly through a support PSF or a non-regulated entity (which will outsource to CSP in a chain). The signatory of the contract with the CSP can be either the financial institution or the operator of the resources provisioned by the CSP, who can be the support PSF or the non-regulated entity outside of Luxembourg. Several provisions on the governance of cloud services apply, including the appointment of a cloud officer for the cloud resources operating entity (which can be the institution itself or a third party).

Depending on the materiality of the activity supported by the cloud infrastructure, the institution needs prior approval from the CSSF. If the outsourced activities are not material or if the cloud service contract is signed with a support PSF, notification to the CSSF is sufficient. The CSSF circular 17/654 will be amended by abolishing the notification of non-material outsourcing and asking all financial institutions to set up a register containing all outsourcing in the cloud regardless of materiality.

### 6.1.3 Observed supervisory practices

Overall, although jurisdictions' mandates to supervise third-party service providers vary, supervisors have been using traditional supervisory tools in order to ensure that the common expectations described above are met. Thematic exercises based on self-assessment questionnaires to assess the cyber-security and IT outsourcing risk of banks are a typical example. Third-party providers can also be reviewed during on-site reviews and inspections, either on the basis of formal requirements or authority (as is done in Hong Kong, Singapore and the US) or based on cooperation from service providers. For example, Australia engages with systemically important third-party service providers which host critical systems for regulated institutions. Periodic engagements are voluntary and focus on service providers' systemic role as opposed to their relationship with individual institutions. This allows for a more open discussion of relevant strategy, governance, customer engagement, controls and capabilities (including those pertaining to cyber). It also can provide useful insight into the maturity (or lack thereof) of regulated institutions oversight practices, informing further supervisory activities. They can also be used as a mechanism to influence the provider regarding regulatory expectations and best practice.

In the same vein, supervisors can work directly with cloud suppliers both on formal or informal grounds, to include the right to audit in contracts for the financial industry (as in the Netherlands) or to take part in regulatory summits organised by major cloud providers (including for discussions of assurance frameworks; see Box 9).

Against the above findings, a "supervisory college" model to supervise and share information about large, internationally active service providers (particularly cloud providers) could also be a way to address the blind spots resulting from mandate limitations and regulatory fragmentation.

Box 9

### Case study 9: Cloud service providers' regulatory cloud summits

Some cloud service providers organise regulatory cloud summits that provide examples of how a supervisory college model could work in practice when applied to a global technology provider.

These summits are organised with regulators and supervisors with the objective of:

(i) holding cloud-focused discussions on the threats related to cloud, the international regulatory landscape and the cloud service provider's stance in this regard; and

(ii) providing the regulators with an opportunity to learn about products, processes and practices and to discuss approaches to supervise and gain assurance that financial institutions using these cloud services operate in a safe and sound manner.[21]

The main part of the summits is usually organised into sessions provided by the staff of the service provider. Typically, one session consists of a panel discussion of regulators (chosen by the cloud service provider) that starts a dialog with the cloud service provider's staff, after which the discussion is opened to all regulators. Discussions are typically not recorded, but the cloud service provider's staff takes notes.

Regulatory summits could also be organised by regulators or an independent body to allow examiners to understand the products and compliance controls so as to usefully complete their expertise and become more effective doing on-site examinations.

## 6.2 Business continuity and availability

To safeguard the availability and continuity of critical business activities in case of exceptional events or crises (eg cyber-attacks), regulators typically request that financial institutions analyse these activities,[22] to design and implement appropriate plans, procedures and technical solutions, and to adequately test

[21] In addition to these summits with regulators and supervisors, these cloud service providers typically also organise comparable summits with their most important financial customers.

[22] The analysis step typically involves a business impact assessment (BIA) identifying the most critical activities, resources and services, their internal and external dependencies, their acceptable recovery time frames in case of disruption, the events/scenarios (either natural or manmade) that can affect these critical business activities and the potential impacts of a (major) disruption.

mitigating measures. The same holds true where critical business activities depend on interconnections with third parties, with regulations stressing the importance of aligning the business continuity plans of critical suppliers (and their subcontractors) with the needs and policies of the financial institution in terms of continuity and security.

It is common practice to request that recovery and resumption objectives be defined for critical business activities from an end-to-end perspective[23] For instance, Italy specifies that among the risk scenarios for the continuity of systemically important processes that are documented and constantly updated, institutions should include catastrophic events that affect essential operators and third-party infrastructures (eg large-scale cyber-attacks). Typical activities and services that are considered by regulators are cloud outsourcing, settlement processes or internet services offered to customers.

Expectations with regard to plans and procedures typically address tasks and responsibilities in processes for incident management and for response and recovery in case of material disruptions, the information and communication needs from and towards key internal and external stakeholders and the required resources, including planned redundancy, so as to ensure the prompt transfer of outsourced activities to a different provider in case continuity or quality of the service provision are likely to be affected.

Most regulators and international standards expect financial institutions to test protective measures periodically in order to verify their effectiveness and efficiency and make adjustments where necessary. Advanced regulators require that tests for critical activities are based on realistic and probable disruptive scenarios, conducted at least on a yearly basis and that service providers and significant counterparties are involved through collaborative and coordinated resilience testing. These tests are typically complemented by audits and monitoring activities (on availability, security incidents, etc) of the outsourcing vendors.

In terms of business continuity and availability, commonalities in supervisory expectations and practices are observed, which are mainly focused on the "standalone business continuity" of the institutions. Such commonalities could provide an opportunity to extend continuity and resilience testing to a more collaborative and coordinated form that involves larger parts of the ecosystem of a financial institution.

## 6.3 Information confidentiality and integrity

Confidentiality and integrity of information for third-party interactions are commonly addressed in general data protection requirements, through explicitly requiring contractual terms to include confidentiality agreement and security requirements for safeguarding the bank's and its customers' information. In addition, banks are generally required to manage or take appropriate steps to ensure

[23] The CPMI-IOSCO guidance on cyber-resilience for financial market infrastructures, for instance, specifies that a Financial Market Infrastructure should, design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Some banking supervisors have similar expectations for systemically important functions.

that their service providers protect their confidential information and that of their clients. Steps include verifying, assessing and monitoring security practices and control processes of the service provider.

A growing number of jurisdictions have cloud-specific requirements, which range from requirements that information transferred to the cloud be subject to a contractual clause and that different cloud-specific issues be considered to ensure data security, to more specific requirements on data location, data segregation, data use limitations, security and exit. One example of data access limitation is the prohibition imposed on staff of cloud service providers in Luxembourg to access a bank's data without the explicit agreement of the bank and without a mechanism available to the bank to detect and control access.

In a number of jurisdictions, regulations explicitly include expectations that outsourcing arrangements comply with legal and regulatory provisions on protection of personal data, confidentiality and intellectual property. Evidence of more technical and operational requirements is more scattered and less harmonised, with jurisdictions emphasising different aspects of information confidentiality and integrity, ranging from explicitly requiring encryption solutions for confidential data to be under the banks' control, to regulating the transfers of data abroad and requiring explicit client consent for data handling by third parties.

## 6.4 Specific expectations and practices with regard to the visibility of third-party connections

As mentioned in Section 6.1, in many jurisdictions the supervisory authority requests to be informed about the material outsourcing agreements made by supervised institutions and imposes some conditions on them, including about preserving a minimum level of visibility on the outsourced functions by the supervised entity.

Beyond the prior notifications and authorisation processes mentioned in Section 6.1, supervised institutions are commonly expected to maintain an inventory of outsourced functions and to receive regular reports from service providers, mainly about measurements of service level agreements and the appropriate performance of controls. Some jurisdictions also require sub-outsourcing activities to be visible for the supervised entities so that the associated risks can also be managed.

Inventorying expectations can be set in relation to IT assets in some jurisdictions, such as the identification of both hardware and software elements together with the function they are related to (even for outsourced functions) in Luxembourg.[24] Other frameworks, such as the US FFIEC IT Examination Handbook and the CPMI-IOSCO guidance, focus on the connections and information flows of financial institutions with external parties.

[24] See CSSF, *CSSF Circular 01/27*, 23 March 2001.

The current practices inspired by the various expectations set at national supervisory level and by international guidance play a complementary role. While supervisory authorities' expectations define activities that can fit into classical cyber-security frameworks (identify, protect, detect, respond and recover), standard setting bodies have an organisational process-oriented approach: for instance, ISO IEC 27036-2 addresses configuration management, information management processes and the outsourcing relation termination processes, and ISACA COBIT 5 elaborates on the implementation of an information security management system. On the other hand, both ISO and the US NIST framework[25] recommend the identification, documentation and categorisation of suppliers to address information security issues, while ISACA COBIT 4.1 and 5 recommend to identify suppliers and associated contracts and categorise them into type, significance and criticality in order to establish a process for their evaluation.

Analysis of supervisory expectations for the visibility of third-party connections shows that the scope, format and content of supervisory authorities' information requests about material outsourcing vary greatly across jurisdictions.

## 6.5 Auditing and testing

Supervisory expectations regarding the audit of third parties (internal and/or external) are aligned in two areas. First, the majority of the requirements state the necessity for the supervised organisations to guarantee the "rights to inspect and audit" their service providers. Some jurisdictions require that this right be cascaded to the significant subcontractors while other jurisdictions (France, Switzerland and Singapore) have granted this right directly to supervisory authorities.

Second, for several jurisdictions the audit opinion on the outsourcing arrangements may be formed based on the report of the service provider's external auditor. Others accept pooled audits, organised by multiple financial institutions,[26] or audits performed by the internal audit department of a service provider, under the condition that the audit department comply with certain regulatory conditions. Some jurisdictions specify that these independent reports should be based on widely recognised standards or be performed by auditors with adequate skills and knowledge.

Current regulations focus on traditional outsourcing and, in some cases, cloud computing providers. The scope of the requirements for "rights to inspect and audit" critical third parties is nonetheless still focused on the strict banking sector. Shared and independent audit reporting on the critical interconnections with third parties could therefore facilitate the audit approach effectiveness and efficiency.

As regards testing of the security requirements for outsourcing and cloud computing providers, although institutions are generally required to monitor their providers' compliance, most regulations are not aligned in terms of how compliance should be verified or tested. One possible method is the application of supervisor-led or bank-led (intelligence-based) red teaming exercises

[25] See NIST, *Framework for improving critical infrastructure cybersecurity*, version 1.1, draft 2, 16 April 2018.

[26] As an example, a group of eight European financial institutions performed a joint audit in June 2018 of a common cloud service provider.

focused on interconnections. In the EU, the scope of the TIBER-EU test appears to include the institution's critical functions that are outsourced to third-party service providers.

## 6.6 Resources and skills

The Basel Committee's *Sound Practices: Implications of fintech developments for banks and bank supervisors*, published in February 2018, indicate that banks may require specialist competencies to assess whether their risk functions are capable of maintaining effective oversight of the emerging risks posed by new technologies.

This topic is usually covered by the broader outsourcing and management processes, with the expectation that the relevant personnel have the necessary expertise, competencies and qualifications to effectively monitor outsourced services or functions and are able to manage the risks associated with the outsourcing beyond the mere compliance dimension.

Regulators expect that institutions contract sufficient and qualified personnel to ensure continuity in managing and monitoring outsourced services or functions, even if key personnel leave the institution or become otherwise unavailable. When institutions do not have internal resources sufficient in know-how or number, the general expectation is that external experts or technical resources, such as consultants or specialists, would be proactively identified to complement or supplement in-house personnel. In Belgium, institutions are required to provide a monitoring and replacement plan for employees who are crucial for ensuring the proper functioning of the critical activities, services and resources and who are difficult to replace due to their specific expertise and limited number. Even beyond the supervised institution personnel, institutions should also provide documentation to clients of financial internet services on security awareness and responsibilities with regard to their secure use to strengthen those connections.

As with the regulatory expectations, supervisory practices mostly reflect commonalities, as the assessment of human resources and qualifications for managing third-party connections and relationships is usually done during on-site inspections. In those jurisdictions where financial supervisors have the authority to examine third parties directly, they assess the sufficiency and qualifications of staff at the third parties, and expect the third parties to perform appropriate background checks.

Personnel who are Certified Information Systems Security Professionals or an organisation that conforms to the ISO 9001 Quality Management System could provide additional assurance that personnel have the necessary competencies to manage third-party connections.

# Annex A: Taxonomy of cyber-risk controls

| Control objective | Control description | Example controls and practices | Example testing approaches |
|---|---|---|---|
| Restrict access and usage to only those who have been authorised | Access is limited to what has been authorised based on job role and principle of least privilege | Identity and access management (IAM), user identification and authentication, physical security, employee awareness and training | Social engineering test |
| | User is authenticated whereby strength of authentication is commensurate with the sensitivity of the asset being accessed | Password policy, system authentication controls | Audits of user access |
| | Networks are protected from unauthorised traffic | Firewalls, routers, network segmentation | Penetration tests |
| | Systems are protected from malicious attacks | Anti-malware, web and email filtering | Non-functional testing |
| | System-to-system communication (including exchange of data) is protected from unauthorised access and use | Encryption, key management | Key management review |
| Detect unauthorised access and usage (including change) | Detect unauthorised access and use of systems in a timely manner | Logs, security information and event management (SIEM), security cameras, intrusion detection solutions (IDS), integrity change detection solutions, event analysis and escalation procedures | Penetration tests, red team tests |

| Control objective | Control description | Example controls and practices | Example testing approaches |
|---|---|---|---|
| Respond to unauthorised access and usage | Orderly response to cyber-incidents | Cyber-incident response playbooks, crisis management, business continuity planning (BCP) | Tabletop exercises, public-private exercises |
| Systems are designed in a manner to maximise uptime | Systems are able to handle the failure of individual components | Active-active, active-passive solutions deployed, sandboxed solutions, zero trust architecture | Chaos Monkey testing, architecture review, failover testing |
| Recover wherever possible | Recover from backups stored in a manner which cannot be compromised by the same cyber-incident | Recovery plans, arrangements and tests | Technical recovery tests |
| Reduce vulnerabilities by minimising introduction of new vulnerabilities and taking steps to mitigate risks associated with them | Implementation controls in place to minimise introduction of new vulnerabilities from system change; systems are secure by design | Secure software development, non-functional testing, change control, system hardening | Change control review, code scanning, architecture review |
| | New vulnerabilities are identified and remediated in a timely manner | Patching | Vulnerability scans, penetration testing, fuzzing |
| | New threats are identified and remediated in a timely manner | Cyber-intelligence, information security strategy | Independent capability review |
| Oversee and direct (govern) cyber-security | Decision-makers are informed with respect to the sufficiency of cyber-controls and direct activity as appropriate | Reports, governance forums, internal audit, independent assurance, consulting reviews | Governance reviews |

# Annex B: Board IT metrics which are applicable to cyber-resilience

| | Forward-looking indicators/metrics | Use | Collected by regulators | Collected by banks |
|---|---|---|---|---|
| **Governance, organisation and resources** | | | | |
| **Strategy** | Budget allocation | The regulated institution and supervisors can discuss and challenge whether the allocation of budget to operating and capital expenditure, and budget allocated to IT outsourcing, is appropriate in the context of resilience. Proportion of budget allocated to risk mitigation/remediation could also be discussed. | ✓ | ✓ |
| | IT priorities | A forward-looking, balanced IT strategy is defined, documented, periodically updated, approved by the management body and aligned with the business and risk strategies. Senior management of the business line(s) is adequately involved in defining the institution's strategic IT priorities and aware of the development, design and initiation of major business strategies and initiatives.<br>Consideration of the number of cross-border business locations and locations of IT functions.<br>The institution has an integrated and institution-wide risk culture, based on a full and common understanding of the IT risks it faces and how they are managed, taking into account its risk tolerance/appetite set by the board and senior management ("tone from the top") and defined in a risk appetite framework. | ✓ | ✓ |
| **IT risk managemen t** | Roles and responsibilities | There is an independent IT risk control function (second line of defence) with a direct reporting line to the management body. Exceptions from IT regulations and policies are escalated to the management body.<br>Clear roles and responsibilities of IT personnel, including the management body and its committees are defined, documented and implemented in order to support the IT strategic objectives. | ✓ | ✓ |
| | IT asset | Data quality management procedures are defined, documented and tested. The institution has defined and documented its data architecture, data models, data flows, golden (authoritative) sources and a data dictionary and validated them with relevant business and IT stakeholders.<br>The institution has adequate physical security controls to protect its premises, data centres and sensitive areas (eg technical areas hosting cabling, UPS, backup media). | ✓ | ✓ |
| | Interconnections with third parties | The regulated institution and supervisors can discuss the outsourcing plan. For each outsourcing, there is a contract between the institution and the service provider, defining service levels and IT security requirements.<br>Recognition of number of third parties and channels for end user to internal systems, dependency of business-critical processes on no longer supported end-of-life (EOL) systems. | ✓ | ✓ |

| | **Forward-looking indicators/metrics** | **Use** | Collected by regulators | Collected by banks |
|---|---|---|---|---|
| | Communications and sharing of information | Establishment of cyber-security information-sharing scheme (internal and external). | ✓ | ✓ |
| **Cyber-controls** | | | | |
| **Restrict access** and usage to only those who have been authorised | Identity and access management (IAM), user identification and authentication, physical security, penetration testing | Access is limited to what has been authorised based on job role and principle of least privilege. | ✓ | ✓ |
| | Password policy, system authentication controls | User is authenticated whereby strength of authentication is commensurate with the sensitivity of the asset being accessed. | ✓ | ✓ |
| | Firewalls, routers, network segmentation | Networks are protected from unauthorised traffic. | ✓ | ✓ |
| | Anti-malware, web and email filtering | Systems are protected from malicious attacks. | ✓ | ✓ |
| | Encryption, key management | System-to-system communication (including exchange of data) is protected from unauthorised access and use. | ✓ | ✓ |
| **Detect** unauthorised access and usage (including change) | Logs, security information and event management (SIEM), security cameras, intrusion detection solutions (IDS), event analysis and escalation procedures, red team tests | Detect unauthorised access and use of systems in a timely manner. | ✓ | ✓ |
| **Respond** to unauthorised access and usage | Cyber-incident response playbooks, crisis management, business continuity planning (BCP) | Orderly response to cyber-incidents. | ✓ | ✓ |
| **Recover** wherever possible | Recovery plans, arrangements and tests | Recover from backups stored in a manner which cannot be compromised by the same cyber-incident. | ✓ | ✓ |
| **Reduce vulnerabiliti** | Vulnerability scans, patching, penetration testing | New vulnerabilities are identified and remediated in a timely manner. | ✓ | ✓ |

| | Forward-looking indicators/metrics | Use | Collected by regulators | Collected by banks |
|---|---|---|---|---|
| **es** by taking steps to mitigate risks | Cyber-intelligence, information security strategy | New threats are identified and remediated in a timely manner. | ✓ | ✓ |
| **Oversee and direct (govern)** cyber-security | Reports, governance forums, internal audit, independent assurance, consulting reviews | Decision-makers are informed with respect to the sufficiency of cyber-controls and direct activity as appropriate. | ✓ | ✓ |
| **Maintenance and operation** | | | | |
| **Staff and culture** | Staff allocation | The regulated institution and supervisors can discuss and challenge whether the allocation of staff to plan, build and run activities is appropriate in the context of resilience. This could also include allocation to security. | | ✓ |
| | Staff attrition rate | Staff attrition rates could suggest problems with communication, governance, culture etc. Some institutions monitor this specifically within teams contributing to critical business services or infrastructure, and loss of subject matter experts. | | ✓ |
| | Staff satisfaction rate | Usually monitored through surveys, this is used for the same purpose and in the same way as staff attrition rates. | | ✓ |
| | Training statistics | Monitored to identify developing gaps in capability or where there may be a lack of oversight of staff supporting critical business services or a lack of subject matter experts to call on.<br>Also monitored in relation to cyber to provide context to other indicators such as mock phishing campaign results.<br>Plan to provide ongoing technical training to new and existing employees. | | ✓ |
| **Operations and change** | Processing rates | This applies across a number of business services and focuses on checking that expected and intended processing rates are being delivered. | | ✓ |
| | Forecasting spikes in operations | Used as an indicator of absorptive capacity. | | ✓ |
| | Critical application trends | Business units' expectation of future spikes in volume/value or activity which could stress/stretch capability can be an indicator that the institution may need to absorb/respond. | | ✓ |
| | Change trends | Tracking the number of planned, unplanned and emergency changes over time, as well as the changes that are rolled back and defects identified, can help to identify potential causes of operational failures, and system and process weaknesses and vulnerabilities. | | ✓ |

|  | **Forward-looking indicators/metrics** | **Use** | Collected by regulators | Collected by banks |
|---|---|---|---|---|
|  | Instance of fraud | Tracking instances and methods of fraud (including cyber-fraud) enables an institution to respond quickly. Tracking this over time can identify weaknesses and vulnerabilities. |  | ✓ |
| **Testing and exercising** | Business continuity and crisis response plan tests | Used to confirm the validity of business continuity and crisis response plans (including communication to customers and other key stakeholders).<br>Possible impacts of disruptions in services with regard to the business processes are assessed (eg by conducting a business impact analysis). As a result, appropriate recovery time objectives, recovery point objectives and maximum tolerable downtimes are defined. |  | ✓ |
|  | Disaster recovery tests | Used to confirm the validity of disaster recovery plans and arrangements. | ✓ | ✓ |
|  | Lessons | All tests and exercises should identify lessons. Identification and themes of these lessons can suggest capability gaps which need to be addressed in relation to the scenario, but also possibly more strategically. |  | ✓ |
|  | Completion and closure of remedial actions | Used to confirm whether remedial action plans established from eg penetration testing have been completed and closed as expected. | ✓ | ✓ |
| **Incidents** | Incident trends | Tracking the number of incidents and their root cause over time can suggest weaknesses and vulnerabilities. | ✓ | ✓ |
|  | Critical system incidents | Tracking numbers of critical system outages, mean time to recover over time and total losses can identify weak critical systems and impactful system interdependencies. | ✓ | ✓ |
| **Events and situations** | Near-miss events | Identification and analysis of near misses including evaluation of whether they were avoided or minimised by luck or by design. |  | ✓ |
|  | Indicator trends | Monitoring all indicators and metrics to detect a step-change (or in some cases unexplained stability) which may provide early warning of an unexpected outcome. This would include consistent green or red reporting which could suggest that indicators are set at too low or high a level of granularity. |  | ✓ |
|  | Persistent thematics | Tracking of thematic findings from assessments, reviews, audits or testing which could suggest a common or shared weakness. | ✓ | ✓ |

# Annex C: Cyber-resilience metrics

| | **Event** | **Practices** |
|---|---|---|
| **Before compromise** | • External scanning blocked connections (count)<br>• New vulnerabilities (by OWASP type: count)<br>• Malware stopped (count)<br>• Phishing sites known (count)<br>• Phishing site takedown (count, hours open)<br>• Unique malware targeting bank (count)<br>• Vulnerabilities per line of code (count)<br>• Applications going into production with code vulnerabilities (count)<br>• Security events detected (count) | • Penetration testing (by type: count and finding rating)<br>• Systems protected by IAM (count)<br>• Internally developed systems which cannot be updated (by type: count)<br>• Systems with out-of-vendor support components (by type: count)<br>• Systems without anti-malware solutions (count)<br>• Non-authorised (compliant) devices (by type: count)<br>• Information security configuration compliance (coverage %)<br>• Awareness exercises (coverage %, count)<br>• Staff responding to phishing tests (% of total staff)<br>• User access review (coverage %)<br>• Security assessments of providers over 12 months (% coverage of relevant third parties)<br>• Patch ageing (by criticality: days)<br>• Assurance report on information security (findings by rating, ageing to remediation) |
| **Compromise** | • Detected malicious software endpoints (count)<br>• Detected malicious software on servers (count)<br>• Online directories containing staff/customer info (count)<br>• Incident type over period (count per: denial of service, malicious code, misuse, reconnaissance, social engineering, unauthorised access, other) | • Resolution and recovery plans developed (by type: count)<br>• Incident rehearsals (by type: count) |
| **After compromise** | • Detected APT (count)<br>• Blocked connections to malicious websites (count)<br>• Data breaches detected (count)<br>• Bank losses (value)<br>• Customer loss (value) | • Post-incident reports (count) |