TC Notes

Practical leadership & technical guidance from **Toronto Centre**

Supervision of Cyber Risk

DECEMBER 2018

Global Affairs Canada
Affaires mondiales Canada
Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY
TORONTOCENTRE
Global Leadership in Financial Supervision

Contents

Introduction[1]

"Cyber Risk" in context of the financial services sector refers to the operational risks that may result in loss of confidentiality, integrity and availability of data or information; and risk that can negatively impact the information technology (IT) infrastructure or business operations. Operational risk is commonly understood as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Cyber risk is generally integral to operational risk and emerges from intentional or malicious "cyber" events where something goes wrong in the business environment of interconnected computers – be it physical or virtual.

Cyber risk is considered as the risk of doing business in the "cyber" or virtual environment comprising Internet, wireless communications or cloud computing[2]. There have been attempts at defining this risk more precisely. For example, the CRO Forum[3] defines it as "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the Internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments." Cyber risk events also present a significant reputation risk, notably to financial institutions, potentially leading to the loss of customer confidence and trust in the system.

As financial services grow exponentially in the cyber environment the nature and the scale of the underlying cyber risks are evolving rapidly. The major contributing factors include the changing nature of technologies, increase in deployment of financial technology (commonly referred to as FinTech[4]), aggressive lead times for launching electronic financial services, as well as the expanding roles of FinTech and IT service providers often operating outside the local regulatory ambit. The global, pervasive nature of financial services and large-value transaction flows make financial services particularly vulnerable to cyber attacks. Increasingly, organized criminal groups that are transnational or allegedly supported by national governments have found ingenious and pernicious ways to carry out cyber attacks for illicit gain, terrorism or disruption of financial systems.

Notably, these cyber attacks have been made on companies like Equifax, Target, JP Morgan Chase, and Sony among others. Increasingly, there have been targeted attacks on a large number of commercial or central banks in countries like Bangladesh, Ecuador, India, Ukraine, Taiwan, etc. The typical modus operandi involved exploiting the vulnerabilities in the banks' payment systems and their interfaces with SWIFT to make fraudulent wire transfers.

The high-profile cyber attacks on financial institutions have focused attention on the need to strengthen cybersecurity and manage cyber risks:

- At the international level, the G7 finance ministers and central bank governors issued a set of "Fundamental elements of cybersecurity for the financial sector",[5] with the aim of helping banks tailor their cybersecurity approaches to their operational and regulatory environment.

---

[1] This note was prepared by Abhilash Bhachech on behalf of Toronto Centre.
[2] Cloud computing refers to the provision of computing services such as software, computer servers, storage, databases, networking, etc., on the Internet (referred to as "the cloud").
[3] The CRO Forum, *CRO Forum Concept Paper on a Proposed Categorisation Methodology for Cyber Risk*, June 2016, https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf.
[4] FinTech, a term abbreviated from "financial technology", is broadly described as any technological innovation in financial services where companies develop new technologies to transform or disrupt the traditional financial markets.
[5] *G-7 Fundamental Elements For Effective Assessment Of Cybersecurity in the Financial Sector*, October 2016, https://www.treasury.gov/press-center/press-releases/Documents/(PRA)_(BCV)_4728453_v_1_G7%20Fundamental%20Elements%20for%20Effective%20Assessment.pdf.

- The Financial Stability Board (FSB) included in its 2017 work plan the need to monitor cyber risk arising from FinTech and to identify the supervisory and regulatory issues from a financial stability perspective. The FSB's report for the July 2017 G20 Hamburg summit places the need to mitigate the adverse impact of cyber-risk on financial stability among the top three priority areas for future international cooperation.[6]

- In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) issued Guidance on cyber resilience for financial market infrastructures.[7]

- In April 2016, the International Association of Insurance Supervisors (IAIS) published an issues paper to raise awareness among insurers and supervisors of the challenges presented by cyber-risk.

- The Financial Stability Institute (FSI), established under the auspices of the Bank for International Settlements (BIS), issued its own policy insights titled "Regulatory approaches to enhance banks' cyber-security frameworks".[8]

There is a strong consensus on the ubiquitous nature of cyber risk, its increasing global reach to large and small financial institutions and the need for its effective supervision. However, there is a debate on whether cyber risk is amenable to conventional supervisory practices or not given the changing nature of this risk.

This note provides a primer on the nature of cyber risk and outlines the fundamental elements of a framework for implementing an effective supervision program for cyber risk assessment in regulated financial institutions. It is a broad-based guidance on how supervisors can assess institutions' governance policies and practices for cyber risk management. Examples of cyber risk guidance and leading-edge international supervisory practices are included in the Appendix to this note.

Characteristics of Cyber Risk Supervision

Risk Characteristics

Cyber risk could originate internally from within the organization or from an external source. A cyber risk event is often intentional, deliberate or malicious but it could be unintentional, linked to a software glitch, hardware malfunction or misconfiguration of an IT component. Understanding causality of cyber risk is relevant from the perspective of a financial institution establishing its internal system controls and IT security components.

The impact of a cyber risk event converges with several other risk domains. Cyber risk is generally discussed on a standalone basis, as it has become a material risk in the past few years. In reality the impact of a cyber risk event is not isolated or confined, but often triggers a consequential train of events that impacts and overlaps with other risks. Impact assessment of possible cyber risk, within the broader risk management framework, is therefore challenging.

---

[6] Financial Stability Board, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, October 2017, http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.
[7] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Guidance on Cyber Resilience for Financial Market Infrastructures*, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.
[8] "Juan Carlos Crisanto and Jermy Premio, *Regulatory Approaches to Enhance Banks' Cyber-Security Frameworks*, Financial Stability Institute, FSI Insights on Policy Implementation no. 2, August 2017, https://www.bis.org/fsi/publ/insights2.htm.

For example, cyber risk impact converges with:

- Operational risk, where the cyber risk event may lead to an external fraud, willful re-routing of a wire transfer, financial loss from denial of electronic banking services or a broad-based disruption of business operations linked to a computer virus or ransom threat,

- Legal and Regulatory risk, also by definition operational risk, where client or institutional privacy breach or loss of confidentiality may result in legal or regulatory penalties,

- Systemic risk, where given the scale of cyber risk impact, there is large scale loss of data integrity in a bank that may impact interbank clearing operations or worse, systemic loss of client access to banking services, or

- Reputational risk, that may lead to loss of public confidence in a specific financial institution or the jurisdiction as a whole, if there is a material financial loss, regulatory penalty or prolonged disruption of financial services.

Cyber risk has increased exponentially also because there are multiple points of information exchange or "data leakage" from the financial institutions. Access to financial data or information is truly global and no longer confined to any corporate, institutional or national perimeter. Internal or external threats to intentional or inadvertent loss of information have increased as these points for information exchange have grown. For example:

- The workplace processes that necessitate email access for almost all staff (or clients), both incoming or outgoing, pose a vulnerability to the spread of cyber risk through transmission of a virus or malware to financial systems or its users.

- The use of removable storage devices (USBs) has vastly increased. Given the increasing data storage capacity and portability of these devices, the possibility of data theft is always a risk. USBs also poses the additional risk of targeted distribution of computer malware, disruption of online financial services or corruption of financial data.

- Smartphones and Personal Digital Assistants (PDAs) are pervasive across institutions and these can be used for unauthorized access to and transfer of data stored on institution's financial systems as well as spread of computer malware.

- Increasing use of outsourcing to third-party FinTech service providers (including cloud-computing services), which involves data transmissions, transfer of financial information or client interfaces for banking services, increases cyber risk due to possible weakness in security controls, human error or targeted intrusion of technology platforms.

The lead players or actors behind any cyber risk incident are numerous and diverse. Based on the experience to-date, there is a wide range of players that conceive, plan, initiate, fund or conduct these cyber attacks; or inadvertently cause the cyber incident. Notably, these may include untrained staff, disgruntled or dishonest employees, competitors, international criminals or organized crime, activists, (often dubbed "Hacktivists") or reportedly, government-sponsored entities.

Supervisory Challenges

Broadly speaking, supervision of technology risks presents multiple challenges. These challenges typically include:

- Limited availability of supervisory resources - in terms of number of staff, skills-set and time allocation - relative to number of institutions and/or complexity of risks.
- Increasing technology and operational risks, information security and privacy threats.
- Increased proliferation of 'FinTech' platforms, vendors, applications and associated risks.
- Decreasing time-to-market product development for banking products and services.

Supervisory challenges over *cyber risk* are further compounded due to the nature, scale and impact of cyber risk incidents and where, supervisory reach and coverage may not be commensurate with the dynamic nature of cyber risk.

Supervisory expectations, regulations, guidance and processes need to be continuously assessed for their relevance and effective alignment with the risk factors underling cyber risk. It is, therefore, important to strike a balance between an effective principle-based supervisory expectations and assessment approach versus establishing highly prescriptive standards that may become irrelevant or obsolete.

Availability of appropriately qualified technical or experienced professionals, in cyber risk space, is limited in almost all jurisdictions. Also, there is an ever-increasing demand for these skills in professional firms and in industry. As a result, supervisory authorities have a major challenge to build or retain such qualified personnel for supervisory functions.

Effective supervision of cyber risk needs a material level of information exchange and coordination within national stakeholders as well as internationally. Timely information sharing on likelihood, impact and mitigation of cyber risk is critical to enhance the cyber risk resilience in a jurisdiction. The supervisory challenge is multifold in terms of subject matter knowledge, availability or transparency of information shared by the regulated firms, gaps in incident management and importantly, legal or policy hurdles to information interchange on cyber risk incidents.

Many of these challenges can be mitigated through establishing risk-based priorities to cyber risk supervision in the context of the supervisory approach, resources and processes; as well as sharing of information, experience and learning with other supervisory agencies.

While supervisory authorities may not be able to resolve all challenges in the short run, implementing a few well-directed measures can enhance supervision. For instance, resources can be augmented by targeted recruitment of cyber risk expertise; and where feasible, and cost effective, engaging third party services.

Importantly, there are significant opportunities for drawing upon the body of learning – including regulations, research, supervisory guidance and case studies – that are available in the public domain or through information exchange with peer supervisory agencies and international standard-setters and agencies like the FSB, BIS, World Bank or IMF. Some of the relevant and useful references are provided in this note.

Supervision of Cyber Risk: Elements & Approaches

The frequency and severity of cyber-attacks in the financial services sector have made it imperative to enhance the regulatory and supervisory oversight of cyber risk. Traditionally, regulatory oversight refers to rules and regulations that lay down expectations for acceptable behavior and conduct for financial institutions. Supervisory activities refer to the assessment of the firms for adherence to the expectations and enforcement of these rules and regulations. The "building blocks" for cyber risk supervision frameworks are typically rooted in the nature of the cyber risk, the existing supervisory regime or practices in a jurisdiction and, also, the state of the cyber risk management practices in the financial and IT industries.

Regulatory Expectations

Most jurisdictions address cyber security as a subset of broader technology risks, which in itself is a subset of operational risk. The regulatory expectations have been typically in the form of principles-based or risk-based guidance aligned with the risks in the industry and the jurisdiction. These guidelines, standards or regulations commonly address IT governance; technology risk assessment and risk management; operational or IT policies, procedures and controls; vulnerability assessments; information security; disaster recovery; business continuity planning; and outsourcing and third-party service provider risks.

The regulatory coverage is now being enhanced to focus on risk assessments and mitigation of specific cyber risks. Increasingly, the focus is now on developing specific guidance for technology risk management and laying down expectations on the role of Board of Directors with regards to enhancing its expertise, policy approvals, risk deliberations at Board/Committee forums and effective oversight of the institution's management.

There are specific expectations of regulated entities with regard to management and reporting of cyber risk incidents; regulatory reporting of data breaches; and oversight of third-party service providers and cloud computing services. Many supervisors have set expectations over IT governance[9] that may include establishing a dedicated management role and accountability for information security (i.e., Chief Information Security Officer or "CISO") as well as expectations for periodic independent testing of cyber threats and vulnerabilities.

Supervisory Approaches

The supervisory approaches have also been consequently enhanced. These include supervisory assessments by supervisors with subject matter expertise that cover various technology risk and cyber risk exposures and the manner in which they are managed.

Typically, this would include targeted assessments of cyber risks and supervisory reviews of:

- IT governance practices;
- effectiveness of Board/management engagement;
- cyber security policies and procedures; iv)
- characteristics and effectiveness of firm's monitoring, testing and internal/systems auditing practices; and
- data integrity and security controls.

The supervisory reviews have also evolved to include a financial institution's practices covering:

- incident management, recovery and reporting;

[9] IT Governance is a framework for organizations to ensure that their IT investment and oversight support the business objectives. IT governance is an integral to corporate governance and a firm's governance, risk and compliance processes.

- information sharing within the industry; and
- independent validation of threats, vulnerabilities, cyber security gap analyses and action plans for mitigations.

Emerging Framework for Cyber Risk Supervision

The FSI has published useful insights into the development and implementation of a policy framework for supervisory oversight of cyber risks.[10] There are several common themes highlighted by the authors' through their research and a survey of cyber risk oversight practices. These are of fundamental relevance in launching any supervisory initiatives to establish a framework for cyber risk supervision.[11] Broadly, the general observations highlighted include:

- Recent high-profile cyber-attacks on financial institutions have focused attention on the need to strengthen cyber-security, leading to various formal initiatives to address cyber-risk.

- This increased attention to cyber-risk is not confined to the larger economies.

- These cyber risk concerns are shared by the industry.

- Jurisdictions are putting in place national policies or frameworks for strengthening the cyber-security of critical sectors and institutions.

- The cross-border nature of cyber-threats requires a high degree of alignment in national regulatory expectations.

- While cyber-risk is a major concern for most bank supervisors, only a handful of jurisdictions have specific regulatory and supervisory initiatives to address banks' cyber-risk.

Some of the themes cited by the FSI that influence the development of a regulatory framework for cyber risk are as follows:

- There are two extreme views on the regulation of banks' cyber-risk: one which sees no need for specific regulations, and the other which favours specific regulations. Many supervisory jurisdictions view cyber risk as any other emerging or evolving risks and rely on conventional practices for assessing the risk – governance, role of Board/Senior Management, controls, policies etc. On the other hand, there are many jurisdictions that choose to establish specific expectations and supervisory regime to mitigate the exposure to reputation and systemic impact of cyber risk incidents.

- One potential benefit of regulation is that it can help ensure board and management buy-in. This is demonstrated where the Board and Senior Management are increasingly aware of the growing cyber risks and impact on reputation and customer confidence on their institutions.

- The risk for the regulators exists that if regulation becomes too prescriptive, it may fall behind both the constantly evolving threat from cyber-risk and advances in cyber-risk management.

- Existing technical standards on cyber and information security could be a valuable starting point for any cyber risk supervision guideline. International standard setters in this area namely, the US

[10] Crisanto and Premio, *Regulatory Approaches to Enhance Banks' Cyber-security Frameworks*.
[11] The observations and narrative on pages 7 and 8 are drawn from *ibid*.

National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS) and the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC - 27000 series) have all developed cyber security frameworks in close cooperation with the private and public sectors.

Supervisors are converging towards a more risk-based but threat-informed or intelligence-led testing framework for assessing cyber-risk vulnerability and resilience. The underlying concept is to pursue accurate intelligence on the most likely and significant threats to a financial institution, and conducting, as feasible, a simulated cyber attack, with a view to getting a clear understanding of risk exposure and the firm's cyber security controls and resilience. While a threat-informed or intelligence-led supervisory approach is not expressly mandated, except in very few jurisdictions, it is emerging as a leading practice for building an effective cyber risk supervisory approach.

For example, UK's CBEST[12] program is essentially based on this threat-informed and intelligence-led testing of security. The CBEST framework facilitates targeted intelligence-led cyber security tests. The tests are designed to represent the possible behaviours of players who may pose a genuine threat to systemically important financial institutions. The CBEST approach comprising threat intelligence provides for the penetration testing of cyber security controls that is more representative of real-world threats.

Cyber Risk Supervision Framework and Processes

Alignment with Risk-Based Supervision Framework

Generally, the supervision of cyber risk is closely aligned with the jurisdiction's own Risk-Based Supervision (RBS) framework[13]. A clear alignment of cyber risk supervision within the RBS framework provides for a more efficient and effective implementation of a supervisory program for cyber risk compared to a segregated oversight regime for this emerging risk.

Typically, in the context of cyber risk supervision, the constituent elements of RBS (referenced above), may include:

- "Area of Focus" which may focus on cyber risk supervisory assessment in a specific institution or as a thematic area of focus across a financial services segment. Cyber risk can also be looked at as a distinct area of focus within a business line or as an area of focus within an assessment of a function such as online commercial banking.

- "Inherent Risks" where cyber risk is typically viewed/risk-rated as inherent "Operational Risk" i.e. risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

- "Risk Management and Governance" where the risk management and control functions for cyber risk are generally are assessed as constituent elements of "Board", "Senior Management", "Internal Audit" and "Risk Management". Again, the control functions in the context of cyber risk can be assessed as a distinct area of focus within a business line or as an area of focus within an assessment of a function such as information technology operations.

[12] Refer to Bank of England, *CBEST Intelligence-Led Testing: CBEST Implementation Guide, Version 2.0*, 2016, https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf.
[13] Please refer to Paul Wright, *Risk-Based Supervision*, TC Note (Toronto: Toronto Centre, March 2018), https://www.torontocentre.org/index.php?option=com_content&view=article&id=82:risk-based-supervision&catid=10&Itemid=101

The specific supervisory processes for cyber risk within the overall RBS framework can be adapted to the financial services sector and technical characteristics of cyber risk exposures. Using information technology industry standards like the US National Institute of Standards and Technology (NIST)[14] or COBIT [15]cyber security model provides a useful reference point for developing a wide range of supervisory expectations and processes for prudential oversight of cyber risk.

The World Bank Group, through its Financial Sector Advisory Center, has published "Financial Sector's Cybersecurity: A Regulatory Digest" which is a comprehensive compilation of recent laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector.[16] The digest provides a global view of regulatory and supervisory initiatives and is a valuable resource for any jurisdiction seeking to build its supervisory processes based on international practices.

A useful operating model included in the World Bank compilation has been established by the G7. It outlines fundamental elements of cybersecurity for the financial sector[17] to "serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, …as well to guide their public policy, regulatory, and supervisory efforts."

The model consists of eight elements representing what are effectively the high-level objectives and supervisory expectations of any financial institution in managing cyber risk exposure. These are:

- **Cybersecurity Strategy and Framework:** Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines;

- **Governance:** Define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority;

- **Risk and Control Assessment:** Identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks. Identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority;

- **Monitoring:** Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises;

- **Response:** In a timely manner (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party

[14] The National Institute of Standards and Technology (NIST) is an agency of the US Department of Commerce. Its mission is to promote innovation and industrial competitiveness that includes establishing standards for information technology. These are widely recognized and applied internationally.
[15] 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.
[16] World Bank, *Financial Sector's Cybersecurity: A Regulatory Digest*, October 2017, http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.
[17] *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, October 2016, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5.

service providers, and customers as appropriate); and (d) coordinate joint response activities as needed;

- **Recovery:** Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally;

- **Information Sharing:** Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning;

- **Continuous Learning:** Review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

The G7 model covers the key aspects of cyber risk governance, risk identification and resilience and can be used as a reference tool. Again, it is important to assess the specific elements of any model in terms of its applicability and relevance to the local supervisory considerations in the jurisdiction.

Supervision of cyber risk is essentially aimed at a financial institution's ability to identify gaps in cyber risk governance, to make informed risk assessment of threats and vulnerabilities unique to cyber risk and to build capacity for cyber resilience. These are now outlined in the next few paragraphs as fundamental elements for supervision of the cyber risks encompassing governance, risk identification, resilience and reporting.

Cyber Risk Governance

In the case of the banking industry, Basel Core Principle 25 requires supervisors to verify that a bank's strategies, policies and processes for the management of operational risk are approved and regularly reviewed by the Board; and that the Board oversees their effective implementation.

Based on this core principle, supervisory expectations specific to cyber risks, typically require that the Board of supervised institutions:

- approve a written Information, Communications and Technology (ICT) strategy aligned with the institution's overall business strategy;
- approve a comprehensive ICT risk management framework; and
- oversee senior management's role in effective implementation of both the strategy and risk management framework.

In context of cyber risk, the governance expectations of the Board have been set higher. As part of the World Economic Forum's Initiative on the Digital Economy and Society, the Forum partnered with the Boston Consulting Group and Hewlett Packard Enterprise to identify a comprehensive framework that boards of directors can use to integrate cyber-risk and resilience into their firms' business strategy.

Termed as the "Board principles for cyber-resilience"[18] this framework consists of ten broad principles. Aligning supervisory practices to these principles is a useful approach to development of an effective supervisory regime and setting "tone from the top" expectations at the Board level for overseeing cyber risk.

Principle 1 – Responsibility for cyber-resilience. The board as a whole takes ultimate responsibility for oversight of cyber-risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. the risk committee) or a new committee (e.g. a cyber-resilience committee).

Principle 2 – Command of the subject. Board members receive cyber-resilience orientation on joining the board and are regularly updated on recent threats and trends.

Principle 3 – Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organisation's capability to manage cyber-resilience and progress in implementing cyber-resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfill these duties.

Principle 4 – Integration of cyber resilience. The board ensures that management integrates cyber-resilience and cyber-risk assessment into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5 – Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber- resilience and ensures that this is consistent with corporate strategy and risk appetite.

Principle 6 – Risk assessment and reporting. The board holds management accountable for reporting a quantified and comprehensible assessment of cyber-risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber-Risk Framework.

Principle 7 – Resilience Plans. The board ensures that management supports the officer accountable for cyber- resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonised across the business.

Principle 8 – Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber-resilience.

Principle 9 – Review. The board ensures that a formal, independent cyber-resilience review of the organisation is carried out annually.

Principle 10 – Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Many supervisors have set increased expectations of the Board's role, going beyond the approvals of strategy, policies and procedures. These governance expectations also include, for example:

- Receiving reports on significant cyber risk events.

[18] World Economic Forum, *Advancing Cyber Resilience - Principles and Tools for Boards*, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

- Assessing the characteristics and effectiveness of Board and Senior Management oversight of cyber risks

- Ensuring appropriate updates cyber risk exposure.

- Assessing the underlying scenarios, development and testing of disaster recovery and business continuity plans.

- The Monetary Authority of Singapore (MAS) [19] also requires that Board "should have in place a comprehensive technology risk and cybersecurity training program for the Board…..to help equip the Board with the requisite knowledge to competently exercise its oversight function, and appraise the adequacy and effectiveness of the financial institution's overall cyber resilience program."

Cascading from the Board's role for cyber risk, there are expectations of Senior Management's accountabilities across the enterprise. These would include, for example:

- Creating the cyber risk management framework and overseeing its implementation.

- Formulating the corporate cyber defence policy.

- Allocating sufficient resources.

- Monitoring the effectiveness of the cyber defence.

- Coordinating with internal and external stakeholders.

- Receiving periodic reports on relevant, internal and external cyber incidents and their implications as well as reporting to the Board.

Cyber Risk Identification

A financial institutions' assessment of its own cyber risk threats and vulnerabilities is a key input to forming a supervisory view of the cyber risk exposure and controls to prevent or mitigate these risks. Threats are events that could cause harm to the confidentiality, integrity, or availability of information or systems. Vulnerabilities can be weaknesses in a system, or control gaps that, if exploited, could result in unauthorized disclosure, misuse, alteration, or destruction of information or systems. Supervisors should assess if firms use scenarios to assess the probability of threats and vulnerabilities.

Supervisory oversight of firms' risk identification is built on the assessment of whether and how the financial institutions maintain an ongoing cyber risk assessment program that effectively:

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, current state of security controls and processes; and related security standards and requirements.

[19] Monetary Authority of Singapore, *Technology Risk Management Notice and Guidelines*, http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx.

- Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets.

- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls and assurance necessary for effective mitigation.

Gathering data and information for cyber risk identification is key to the supervisory process. Supervisory assessments are more effective when the data gathering by the firm for cyber risk identification includes:

- Current and detailed knowledge of the firm's operating and business environments.

- Both technical and non-technical information. Technical information may include network maps detailing internal and external connectivity, hardware and software inventories, databases and files containing critical and/or confidential information, etc.; and non-technical information may include policies, standards, and procedures, vendor contracts, personnel security training and expertise, insurance coverage, etc.

- Information on control effectiveness compiled from security monitoring, self-assessments, incident metrics, audit reports and independent tests.

- Employee security privileges profiling staff access, use, and dissemination of information.

- Practices around information storing, transmitting, and disposal of media; as well as authorizing and authenticating information received (paper and electronic).

Supervisory assessment may also seek to verify firms' effectiveness in:

- Organizing information and systems within a logical framework that recognizes that not all threats and risks are equal, and that firms' finite managerial and financial resources are deployed effectively.

- Assigning a probability or likelihood of a security risk event occurring, and the impact on the firm, typically expressed as "High," "Medium," or "Low" levels of risk ratings.

- Assigning probabilities, rating risks and segregating risks that the firm is willing to accept and those that need to be mitigated.

- Identifying and documenting inadequate controls that are addressed or mitigated in action plans to improve controls.

- Engaging Board guidance in such segregation of security risks.

Cyber Risk Resilience

One of the essential supervisory processes is to assess the characteristics and the effectiveness of cyber risk controls to inform the supervisors of the firm's cyber risk resilience. This section also deals with reporting of cyber risk events.

Risk Controls

The cyber risk controls are generally categorized by their timing (preventive, detective, or corrective) or by nature (administrative, technical, or physical). It is important to recognize that enterprise cyber security controls are not likely to be always effective; there is always a likelihood of some failure some of the time. Measures of control effectiveness can be demonstrated by the firms from a well-planned and executed cyber resilience and security monitoring programs. Supervisory assessment includes firms' monitoring program and processes to identify controls that will mitigate the impact or likelihood of each identified threat agent exploiting a specific vulnerability.

Consistent with the approach established in Basel Committee guidance[20] supervisors can assess the characteristics and effectiveness of all the three lines of defence in context of cyber risk, where:

- The first line of defence is the front line of business line management and the underlying systems, controls environment for managing operational risks.
- The second line of defence is provided by the risk management and compliance functions that include policies, procedures and oversight functions.
- The third line of defence is the independent internal audit and assurance function that tests if the risk management framework is working as designed.

In the course of supervisory examinations of cyber risks associated with third-party service providers and outsourcers, supervisors can assess whether the firms retain the ultimate responsibility for cyber risk controls for all outsourced operations, including processes/data storage in the 'Cloud'. Operationally, while the third-party service providers do have proprietary tools and manage the cyber risks and associated controls, client financial firms need to determine that the service provider is able to meet the firm's security policies and the supervisors' concerns with emphasis on:

- Confidentiality, security and separation of firm's property.
- Contingency planning.
- Location of records, access and audit rights.
- Engagement and familiarity of the client firm.
- Threats and vulnerabilities assessments.
- Independent attestations, as required.
- Subcontracting, if any.
- Monitoring the material outsourcing arrangements.

Reporting and Information Sharing

Supervision of cyber risk is significantly enhanced by incorporating regulatory expectations for reporting of specific cyber risk events, regulated entities' response and recovery efforts and also, information

[20] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011, https://www.bis.org/publ/bcbs195.pdf. See paragraphs 14-20.

sharing, as appropriate. Supervisory reporting provides a view of timeliness of incident detection and response; and also, cyber risk exposure and emerging trends based on the nature, scope, and impact of the cyber incident(s) being reported.

Assessments of individual firm's recovery experience helps enhancement of cyber risk supervision programs in terms of enterprise-wide identification of threats and vulnerabilities, remediation of vulnerabilities, stakeholders' and service providers' responses and technical support, if any; and importantly, crisis communications to address systemic cyber risk events. Moreover, cyber risk incident reporting enforces a higher level of awareness and engagement on the part of firm's Board and Management to oversee cyber risk.

There is a range of practice in setting out reporting obligations. Certain jurisdictions have no specific reporting requirements and leave it for the regulated entities to report. Many jurisdictions, on the other hand, apply what can be described as a "zero tolerance" approach to reporting of cyber risk and/or privacy breach incidents. MAS for example has a very stringent regime for incident notification. Notice[21] on Technology Risk Management requires financial institutions to notify MAS ***as soon as possible, but not later than 1 hour***, upon the discovery of an incident. The information, reportable on structured templates, includes specific details on the relevant incident, such as: What happened; When did it happen; How did it happen; Where did it happen; and What was the impact? Apart from the initial incident report, MAS notice requires a root-cause and impact analysis report ("IT incident report") to be submitted to MAS, ***within 14 days or such longer period as MAS may allow***, from the discovery of the relevant incident.

Broadly speaking, cyber risk exposures and associated technical or operational controls are more generic across all industries. As the nature and the scale of cyber risk increases, it is beneficial to have adequate measure of information sharing under the auspices of industry bodies, technical agencies, domestic or international regulatory organizations on threats, vulnerabilities, incidents and responses to enhance situational awareness and broaden learning.

Concluding Remarks

Cyber risk has emerged as a major risk category that is truly ubiquitous and pervasive across all industries. Financial services are particularly vulnerable to cyber risks, particularly banking and investment services which offer increasingly sophisticated online banking platforms relying on connectivity with global banking and payments networks. The risk profiles of the regulated industries are transforming as cyber risk is not confined to any local domain and where the risk origin is not traceable to any single identifiable source.

The risk will only be further compounded with increasing deployment of smaller, purpose-built FinTech solutions operated by third-party service providers. The rapid expansion of FinTech (or InsurTech) to the insurance sector and complex service offerings on emerging technologies like crypto-currencies, driverless transportation, customized/automated healthcare delivery, 3-D printing will further amplify the cyber risk impact to financial services.

Inevitably, the prudential regulatory agencies that oversee financial services sector will have to respond to ever-increasing calls for more comprehensive regulatory frameworks, clarity (or specificity) in setting out supervisory expectations as well as resources, technical expertise and authority to assess and enforce leading practices for cyber risk oversight. The standard setters like FSB, BIS, CPMI-IOSCO, IAIS as well

[21] Monetary Authority of Singapore, *Instructions on Incident Notification and Reporting to MAS*, http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx.

as bodies like World Bank and IMF will be taking a more proactive and collaborative role in harmonizing some of these expectations and also, provide its own perspectives through their respective assessments of jurisdiction's progress on overseeing cyber risk.

Appendix: International Supervisory Practices

Certain international and regional standard setters and financial jurisdictions have taken proactive steps at developing frameworks for overseeing cyber risks. Guidelines issued by Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) and recently, by the European Banking Authority (EBA) address a wide spectrum of cyber risk issues. Jurisdictions that are notably leading in developing their regulatory and supervisory frameworks include Hong Kong, UK and Singapore. The next few pages in this note provide a brief overview of each of the supervisory approaches with a view to exploring the diversity as well as the common elements of oversight on cyber risk.

CPMI-IOSCO

The Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) jointly issued their "Guidance on cyber resilience for financial market infrastructures" in 2016.

The framework seeks to inform and guide a very large segment of financial services including securities industry and entities constituting payments and financial market infrastructures. The framework is comprehensive as it covers all of the key functional components of cyber risk including identification of risks; protection of information/technology assets; detection of vulnerabilities; incident response; and recovery. At the core the framework sets out the essential governance expectations for the Board and Senior Management.

Identification

- Baseline situation – threat profile, risk exposure and expected losses

Protection

- Increase third party security capabilities
- Internal and third-party patches to ensure security and functionality of the application environment

Detection

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

Response

- Incident response capabilities across pre-determined threat scenario of a threat to assess incident response readiness and effectiveness (war gaming)

Recovery

- Stakeholders' response preparedness and effectiveness of business continuity plans
  Initiation of action plans and mobilization of resources to remediate following a cyber incident[22]

[22] Adapted from Crisanto and Prenio, *Regulatory Approaches to Enhance Banks' Cyber-security Frameworks*.

European Banking Authority (EBA): ICT Guidelines

In 2017, the European Banking Authority (EBA) published its final Guidelines[23] on the assessment of the Information and Communication Technology (ICT) risk in the context of the Supervisory Review and Evaluation Process (SREP). These Guidelines are addressed to competent authorities within EU and aim at promoting common procedures and methodologies for the assessment of ICT risk.

The Guidelines, effective 2018, are structured around the assessment of the financial institution's ICT governance and strategy; as well as the assessment of ICT risk and the controls in place in the context of risks to capital. These ICT Guidelines are effectively integrated in EBA's Supervisory Review and Evaluation Process (SREP) Guidelines on the assessment of operational risk.

The two key emerging trends that are specifically recognized in these ICT Guidelines include

- Emergence of (new) cyber risks together with the increased potential for cybercrime and the appearance of cyber terrorism; and

- Increasing reliance on outsourced ICT services and third party products, often in the form of diverse packaged solutions resulting in manifold dependencies and potential constraints and new concentration risks.

The ICT/SREP guidelines encompass a very comprehensive assessment of ICT elements including ICT risk taxonomy, governance, ICT risks, controls, ICT outsourcing risks, alignment of risks/outcomes with ICT strategy. It also incorporates risk-scoring methodologies.

These EBA guidelines sets out requirements for European bank supervisors to map identified ICT risks into the following five risk categories –

- **Availability and continuity risk:** the risk that the performance and availability of systems and data are adversely impacted, including the inability to timely recover due to a failure of hardware or software, management weaknesses, or any other event.

- **Data integrity risk:** the risk that data stored and processed are incomplete, inaccurate or inconsistent across different systems.

- **Change risk:** the risk arising from the inability of the institution to manage system changes in a timely and controlled manner.

- **Outsourcing risk:** the risk that engaging a third party, or another group entity (intra-group outsourcing), to provide systems or related services, adversely impacts the institution's performance and risk management.

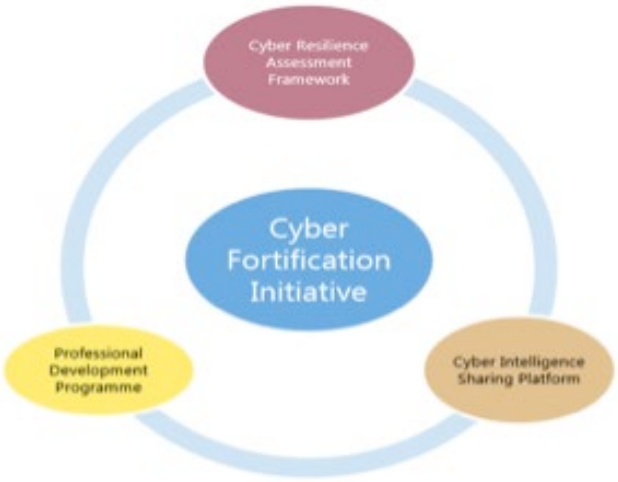
- **Security risk:** the risk of unauthorized access to systems from within or outside the institution.

The taxonomy and ICT methodology include "attacks performed from the Internet or outside networks for different purposes (e.g. fraud, espionage, activism / sabotage, cyber terrorism) using a variety of techniques

[23] European Banking Authority, *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)*, May 2017, https://eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a.

(e.g. social engineering, intrusion attempts through the exploitation of vulnerabilities, deployment of malicious software) resulting in taking control of internal ICT systems. EBA's ICT risk assessment framework now enables a dedicated methodology harmonized supervisory expectations managing and supervising IT and cyber risks. Over the long term, it is expected the ECB may also consider establishing a cyber resilience testing framework for banks similar to the UK CBEST program.

Hong Kong: Fortification Initiative



The HKMA's Cybersecurity Fortification Initiative (CFI) has three elements:

Cyber Resilience Assessment Framework – includes an inherent risk assessment, maturity assessment, and an intelligent-led cyber-attack simulation testing (iCAST);

Professional Development Program- seeks to increase supply of qualified cyber-security professionals in Hong Kong; HKMA is working with the HK Institute of Bankers and the HK Applied Science and Technology Research Institute (ASTRI) to develop a localized certification scheme and training program for cyber-security professionals; and

Cyber Intelligence Sharing Platform – seeks to provide an effective infrastructure for sharing intelligence on cyber-attacks, being set up by the HKMA together with the HK Association of Banks (HKAB) and ASTRI.

Source: HKMA: Cybersecurity Fortification Initiative. 24 May 2016; Graphic by FSI

United Kingdom: CBEST

Effective 2016, United Kingdom, the under the auspices of Bank of England, launched its CBEST[24] program. CBEST is now widely considered as a world-leading framework for intelligence-led threat and vulnerability analyses as well as penetration testing of systemically critical organizations. The key components of CBEST framework include:

[24] Bank of England, *CBEST Intelligence-Led Testing: CBEST Implementation Guide, Version 2.0*, 2016, https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf.

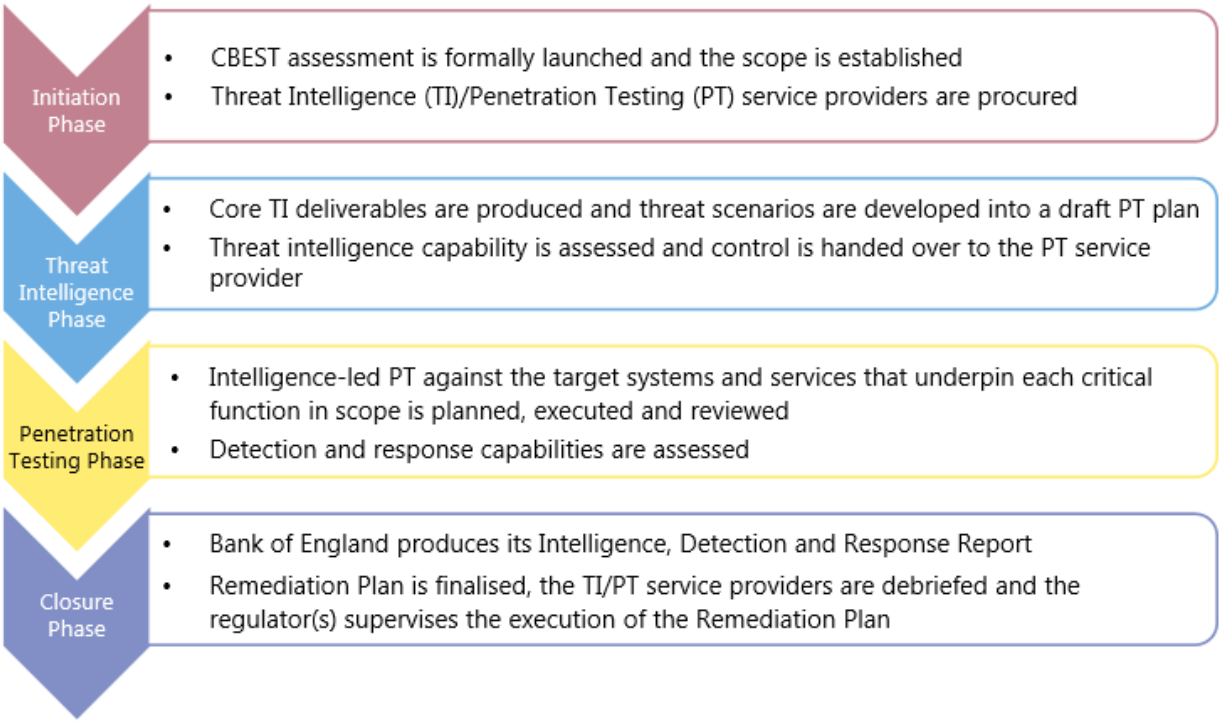
- Access to considered and consistent cyber threat intelligence, ethically and legally sourced from organizations that have been assessed against rigorous standards;
- Access to knowledgeable, skilled and competent cyber threat intelligence analysts who have a detailed understanding of the financial services sector;

- Realistic penetration tests that replicate sophisticated, current attacks based on current and targeted cyber threat intelligence;

- Standard key performance indicators that can be used to assess the maturity of the organization's ability to detect and respond to cyber attacks; and

- Access to benchmark information that can be used to assess other parts of the financial services industry.

The Bank of England's CBEST Framework



Singapore: Technology Risk Management Notice and Guidelines

Monetary Authority of Singapore (MAS) is a leading jurisdiction that recognizes the underlying risk exposure to cyber risk and the severity of the impact. In this regard, MAS has been at the forefront in issuance of its Technology Risk Management Notice and Guidelines. These guidelines, which set out supervisory expectations, seek to address the increased technology risks (including cyber risks) faced by the regulated financial institutions. The MAS guidelines are comprehensive and combine principle-based with specific guidance on good practices. MAS' supervisory processes ensure strict adherence to these expectations. Key supervisory expectations that are spelt out in the Technology Risk Management Notice and Guidelines include[25]

[25] Adapted from Monetary Authority of Singapore, *Technology Risk Management Notice and Guidelines*.

- MAS clarifies that more attacks may be targeted at the institutions' Internet systems as financial services are increasingly provided online and more customers transact on this platform. MAS expects that each institution devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.
- It is expected that financial institutions provide its customers and users of its Internet services the assurance that online login access and transactions performed over the Internet are adequately protected and authenticated.

- Every institution must properly evaluate security requirements associated with its Internet systems and adopt encryption algorithms, which are of well- established international standards and subjected to rigorous scrutiny.

- The institution should ensure that information processed, stored or transmitted between the institution and its customers is accurate, reliable and complete.

- The financial firm should implement physical and logical access security to allow only authorized staff to access its systems and implement appropriate processing and transmission controls to protect the integrity of systems and data.

- The firm has to implement monitoring or surveillance systems so that it is alerted to any abnormal system activities, transmission errors or unusual online transactions.

- Also, the firm has to maintain high resiliency and availability of online systems and supporting systems; and should put in place measures to plan and track capacity utilization as well as guard against online attacks like denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

- MAS mandates the deployment of two-factor authentication at login for all types of online financial systems and transaction-signing for authorizing transactions.

- MAS expects firms to develop technology refresh plan to ensure that IT infrastructure is up-to-date thereby reducing security risk from outdated infrastructure.

- The firms are expected to take appropriate measures to minimize exposure to other forms of cyber attacks such as middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

- MAS considers mobile online services and payments as extensions of the conventional online financial services and payments services. It is expected that all institutions implement security measures that are similar to those of online financial and payment systems on the mobile online services and payment systems.

- The firms should conduct a risk assessment to identify possible fraud scenarios and put in place appropriate measures to counteract payment card fraud via mobile devices.

Key References

Crisanto, Juan Carlos and Jermy Premio. *Regulatory Approaches to Enhance Banks' Cyber-security Frameworks*. Financial Stability Institute. FSI Insights on Policy Implementation no. 2. August 2017. https://www.bis.org/fsi/publ/insights2.htm

European Banking Authority. *Guidelines on ICT Risk Assessment Under the Supervisory Review and Evaluation Process (SREP).* May 2017. https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf

Federal Financial Institutions Examination Council. *FFIEC Cybersecurity Assessment Tool.* May 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Monetary Authority of Singapore. *Technology Risk Management Notice and Guidelines.* http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx

World Bank. *Financial Sector's Cybersecurity: A Regulatory Digest*. October 2017. http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf

Wright, Paul. *Risk-Based Supervision*. TC Note. Toronto: Toronto Centre, March 2018. https://www.torontocentre.org/index.php?option=com_content&view=article&id=82:risk-based-supervision&catid=10&Itemid=101

Additional Readings

Financial Stability Board. *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practice.* October 2017.
http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/

Bank of England. *CBEST Intelligence-Led Testing: CBEST Implementation Guide, Version 2.0.* 2016.
https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

Nieles, Michael, Kelley Dempsey and Victoria Yan Pilliteri. *An Introduction to Information Security*. National Institute of Science and Technology. NIST Special Publication 800-12. June 2017.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

World Economic Forum. *Advancing Cyber Resilience - Principles and Tools for Boards.* January 2017.
http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf