Financial Sector's Cybersecurity: A Regulatory Digest*

July 2020

* This Digest is intended to be a live, periodically updated compilation of recent laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector. It is, therefore, organized in reverse chronological order, with the most recent document first. The Digest is not meant to be comprehensive of everything published by all jurisdictions and international bodies. The explanatory summaries are composed of text extracted from the documents and includes links to the original documents or websites that contained them at the time of including them in the Digest. An accompanying "Source Table" file includes the indexes of documents in the Digest and reference tables matching key concepts to documents.

The Digest has been compiled and it is being maintained by Aquiles A. Almansi (Lead Financial Sector Specialist, EECF2) and Yejin Carol Lee (Senior Financial Sector Specialist, EFNFS).

INTRODUCTION

The present document is the fifth edition of the World Bank's FinSAC Digest of Cybersecurity Regulations in the Financial Sector. The Digest is a periodically updated compilation of laws, regulations, guidelines, and other significant cybersecurity publications for the financial sector. The explanatory summaries contain text extracted from the documents and include links to the websites where published. Such content might appear as targeting a highly specialized audience of financial regulators, supervisors, and senior management of regulated institutions working on cyber risk or, more generally, operational risk. However, cyber risk is not a problem for IT specialists only; it is everybody's problem in any organization. Several documents in the Digest can help a much wider audience understand what cyber risk is, why it matters for financial stability and everyone's role in adequately managing it. The updates include new publications since the previous edition and older ones that FinSAC frequently finds with help from readers, who are strongly encouraged to keep letting us know anything they feel is missing.

This edition adds 20 documents to the 217 in the previous one. The WHAT's NEW? section below classifies the additions and briefly describes their content. The classification should help quickly discover which publications may be of interest, both for readers familiar with earlier editions and those who are not cyber-risk specialists. Each of the 20 additional documents falls in one of seven different thematic areas:

- **Cyber Risk and Financial Stability**. Policymakers in general, financial sector authorities, and senior management of regulated institutions need to understand cyber risk in an interconnected world, its increasing weight in the Value-at-Risk in financial institutions, and the central policy issues. Two working papers by the Monetary and Economic Department of the Bank of International Settlements (BIS), an Institute of International Finance-McKinsey survey, and publications by Brookings and the European Credit Research Institute (ECRI) address those central policy issues.
- **Cyber Resilience: Incident Response and Recovery**. Responding to cyber incidents is not just an engineering problem; it may also demand taking business continuity decisions that financial sector authorities and senior management of supervised institutions cannot delegate to IT specialists. The Financial Stability Board has developed an incident-response and recovery toolkit and describes the range of practices in different jurisdictions. The National Bank of Georgia's "Cybersecurity Management for Commercial Banks" provides an illustrative example. With its Cyber Resilience Oversight Expectations (CROE), the European Central Bank (ECB) provides a detailed methodology to assess the "Guidance on cyber resilience for financial market infrastructures" of the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO.
- **EBA Guidelines**. The "Guidelines on ICT and security risk management," which entered into force on June 30, 2020, detail how financial institutions should comply with the provisions of Article 74 of Directive 2013/36/EU (CRD) and Article 95 of Directive 2015/2366/EU (PSD2). This section also includes the

previous version applying to payment services providers and a table reflecting the actual or intended compliance in all EU national jurisdictions.

- **Red Team Tests and Simulations Exercises**. Red team tests are useful for identifying potential weaknesses in financial institutions' cyber protection, detection, and response capabilities to establish an effective remediation plan. The Financial Stability Institute (FSI) of the Bank of International Settlements (BIS), the Saudi Arabia Monetary Authority (SAMA), and the Association of Banks of Singapore (ABS) have published guidelines to prepare, execute, and evaluate these exercises.
- **Competency Standards for Cybersecurity Practitioners**. The Hong Kong Monetary Authority's (HKMA) "Enhanced Competency Framework on Cybersecurity" sets out competency standards for cybersecurity practitioners of IT Security Operations and Delivery, IT Risk Management and Control, and IT Audit in the banking industry.
- **Endpoint Security of Payments Systems**. An "endpoint" in the wholesale payments ecosystem is a point in place and time at which two parties exchange, on behalf of themselves or third parties, a payment instruction. The Committee on Payments and Market Infrastructures (CPMI) published a "toolkit" to support central banks wishing to reduce the risk of wholesale payments fraud related to endpoint security in their institutions and jurisdictions.
- **NIST Special Publications**. Technical examples of the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST) on how financial institutions can manage three critical matters using open source and commercially available software: IT assets, privileged accounts, and access rights.

Digest organization: The summaries in the DOCUMENTS section appear in reverse chronological order, identified by edition number (e.g. '05', for new additions in this edition) followed by document number in that edition (hence, '05_01' for the most recent addition). If there is more than one document hyperlinked within a particular theme, they appear with letters in sequence (i.e., '04_02b'). We encourage readers to download the separate "Source Table" (CyberDigest_Indexes_v5) database file to filter documents by jurisdiction, authoring institution, or date, and access them via hyperlinks. The Indexes file also contains index tables mapping concepts to the documents discussing them.

WHAT's NEW?

1. Cyber Risk and Financial Stability

1.1. The drivers of cyber risk[1]

Cyber risk commonly refers to the risk of financial loss, disruption, or reputational damage resulting from the failure of IT systems, including malicious cyber incidents where threat actors intend to do harm (e.g., ransomware attacks, financial or data theft by employees). Using a database of more than 100,000 cyber events across sectors, this Working Paper from the Monetary and Economic Department of the Bank of International Settlements (BIS) documents the characteristics of cyber incidents. It finds that while the financial sector faces a larger number of cyber-attacks, it suffers lower average costs thanks to higher investments in information technology (IT) security. The use of cloud services reduces the cost of small incidents but outsourcing those services from systemically important providers is likely to increase tail risks. Finally, it notes that crypto-related activities, mostly unregulated, have been particularly vulnerable to cyber-attacks.

1.2. Cyber Resilience Survey[2]

The Institute of International Finance (IIF) and McKinsey & Company collaborated on research to provide financial firms an understanding of how they can enable and strengthen cyber resilience, building on the current and planned practices of peer institutions. The research is survey-based, and the survey was partly mapped to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The main findings were:

- Firms with over $1 trillion in assets have better cyber resilience.
- The largest vulnerability could be supply chain/dependency management.
- Out-of-date infrastructures are at risk for hacking.
- 37% said it takes more than three months to remediate a vulnerability.
- Companies are willing to share information with peers.
- Many are willing to work together to raise resilience for all (e.g., 40% would do joint 3rd party/vendor due diligence).
- Many would also participate in public platforms or initiatives.
- 58% self-reported under-spending.
- The protect function gets the most resources, some others are lacking
- Cyber insurance levels are insufficient.
- Key challenges include cloud adoption, digital innovation, talent gap.
- Cloud adoption is both a challenge and an opportunity.
- Automation and artificial intelligence will see continued adoption.

1.3. Operational and cyber risks in the financial sector[3]

This Working Paper from the Monetary and Economic Department of the Bank of International Settlements (BIS), using cross-country data at the operational loss event

[1] Document 05_01a
[2] Document 05_03a
[3] Document 05_04a

level for the last 16 years for over 70 large banks, attempts to measure total operational risk and how much of it is for cyber risk. Operational value-at-risk estimates can vary substantially depending on the methodology. The average estimates for the financial institutions in the sample range from 6% to 12% of total gross income, depending on whether the method used is better able to capture the heavy-tailed nature of the data. Cyber losses can account for up to a third of the total operational value-at-risk.

1.4. The Future of Financial Stability and Cyber Risk[4]

This paper from the Cyber Project at Brookings considers how cyber risks differ from traditional financial shocks. In contrast to the financial and policy shocks that triggered the past financial crises, cyber-attacks are generally designed and initiated by actors pursuing specific malicious goals, including triggering broad financial system instability. The analysis addresses the following questions: 1) How might cyber risks and financial risks interact to cause systemic crises? 2) Is there anything fundamentally new or different about cyber risks?, and 3) How should economists, regulators, policymakers, and central bankers focused on financial stability incorporate cyber risks into their models and thinking? The paper identifies four major concerns:

- Increasingly knowledgeable and sophisticated adversaries might deliberately aim for (or unintentionally cause) financial instability and actively work to undermine the financial sector's response efforts.
- The dearth of information and analysis on the potential interactions of cyber risks, financial contagion channels, and possible "amplifiers" within those channels, such as single points of failure.
- Fragmentation of Efforts. Misalignment of cross-border policies, a divergence between industry and official sector work on cyber and financial stability risks, a lack of coordinated policies and regulations, and a range of standards and preparedness across different types of firms and markets.
- Even though the financial system's technology is already highly complex, it will continue to be transformed, especially with the explosive growth of fintech.

The paper concludes with four recommendations:

- Harmonize international regulations that foster resilience to cyber-attacks and mitigate risk in the event of an attack.
- Conduct additional research to identify data and facilitate the design of models to measure or quantify cyber risk, including developing a shared lexicon or taxonomy to discuss cyber risk as a factor in financial stability.
- Share and further develop maps of critical market structures, market processes, and conventions (both recent public and private sector efforts) and develop additional maps to understand better the overlay of cyber risk on the plumbing of markets and institutions.
- Conduct more exercises at the domestic and cross-border levels, especially to bridge between senior-level response executives from the financial stability and cybersecurity communities.

[4] Document 05_14a

1.5. Cybersecurity in Finance Getting the policy mix right![5]

To analyze the cyber issues relevant for the European financial sector, the European Credit Research Institute (ECRI), an independent think tank managed by the Centre for European Policy Studies (CEPS), organized a Task Force with experts from the financial industry, tech industry, national supervisors and European institutions, as well from one consumer association and one law firm. This report discusses in detail the nine main policy recommendations:

1. Convergence in the taxonomies of cyber-incidents is needed.
2. The framework for incident reporting needs to be significantly improved to fully contribute to the cyber-resilience of financial firms.
3. Authorities should assess how and to what extent the data held by the centralized hub should be shared with supervisors, firms, and clients.
4. Ambitious policies are needed to develop consistent, reliable, and exploitable statistics on cyber-trends.
5. Best practices for cyber-hygiene should be continuously enhanced by regulators and supervisors.
6. The European Cybersecurity Certification Scheme needs to be strengthened to contribute better to cybersecurity, cyber-risk management and capability.
7. In order to improve the processes of attribution and extradition, the reinforcement of cross-border cooperation and legal convergence remains a priority, both within the EU and more widely.
8. Best practices in remedies in case of cyberattacks need to be further encouraged.
9. Policymakers should further assess the pros, cons, and feasibility of creating an emergency fund in case of large cyberattacks.

2. Cyber Resilience: Incidents Management and Recovery

2.1. Effective Practices for Cyber Incident Response and Recovery[6]

Given the highly interconnected information systems of the financial sector, the Financial Stability Board (FSB) agreed in 2018 to develop a toolkit for financial institutions with a set of effective practices to respond to and recover from a cyber incident limiting financial stability risks. In the process of developing such a toolkit, the FSB published in April 2020 this Consultative Document. In its current state, the toolkit addresses in detail the following matters:

- Governance: the structures and roles in coordinating response and recovery across internal functions, business lines, firms, jurisdictions, or even sectors. It defines the decision-making framework, allocating responsibilities and accountabilities to the right stakeholders
- Preparation: establishing and maintaining capabilities to respond to cyber incidents, and to restore normal operations, critical functions, processes, activities, systems, and data affected by cyber incidents.

[5] Document 05_17a
[6] Document 05_2a

- Analysis: determining the severity, impact, and root cause of cyber incidents to drive the appropriate response and recovery activities.
- Mitigation: activities to prevent the aggravation of the situation and eradicate cyber threats in a timely manner to alleviate their impact on business operations and services.
- Restoration: repairing and restoring systems or assets affected, to resume delivery of impacted services safely.
- Improvement: learning from past cyber incidents and performing response and recovery exercises.
- Coordination and communication: communicating with trusted external stakeholders to maintain good cyber situational awareness, and during incidents with the level of detail, and language appropriate to each group of stakeholders.

The reader may also benefit from reflecting on at least some of the questions posed by this consultative document. In particular, the lessons for the cyber incident response and recovery practices from the response to the COVID-19 pandemic, and the role -if any- that financial sector authorities should play in supporting an organization's response and recovery activities.

2.2. Cyber Resilience for Financial Market Infrastructures[7]

In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the "Guidance on cyber resilience for financial market infrastructures." FMIs are required to comply with such Guidance, and supervisors must develop an oversight approach to assess compliance. To do that, supervisors need a detailed assessment methodology, comparable to the PFMIs methodology for assessing the compliance with the CPMI-IOSCO Principles for Financial Market Infrastructures. The European Central Bank (ECB) has developed a detailed methodology through its Cyber Resilience Oversight Expectations (CROE).

To develop the CROE, the ECB build pm existing international guidance documents and frameworks. In particular, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO/IEC 27002, COBIT 5, Information Security Forum's Standard of Good Practice for Information Security, and Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool. The CROE consists of eight chapters that outline five primary risk management categories and three overarching components that should be addressed by an FMI's cyber resilience framework. The risk management categories are: (i) governance; (ii) identification; (iii) protection; (iv) detection; and (v) response and recovery. The overarching components are testing, situational awareness, and learning and evolving.

[7] Document 05_07a

2.3. National Bank of Georgia's Regulation on Cybersecurity Management for Commercial Banks[8]

On March 20, 2019, the National Bank of Georgia issued a regulation requiring all commercial banks, both local and branches of foreign banks operating in Georgia, to establish a framework for cybersecurity management commensurate with the bank's size, complexity, and the nature of its business, and fully integrated into the bank's overall risk management process.

Following the logical structure of the NIST Cybersecurity Framework, the Georgian regulation addresses the following primary functions: a) Risk Identification, b) Protection, c) Discovery, d) Response, and e) Restoration. Additionally, the regulation requires annual self-assessments and independent audits.

2.4. Cyber-resilience: Range of practices[9]

Relying on input from its member jurisdictions in response to the survey conducted by the Financial Stability Board in 2017 (document 02_16b in this Digest), this Basel Committee on Banking Supervision (BCBS) report identifies, describes and compares regulatory and supervisory practices on cyber resilience for banks across different jurisdictions.

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. While regulators generally do not require a specific cyber strategy, all expect institutions to maintain the adequate capability in this area as part of their global strategies.

The report's main findings were:

- In most jurisdictions, broader IT and operational risk management practices are quite mature and are used to address cyber-risk and supervise cyber-resilience.
- Cyber-resilience is not always clearly articulated across the technical, business, and strategic lines.
- Skills shortage leads to recruitment challenges.
- Protection and detection testing are evolving and prevalent; **response and recovery less so**.
- Although an incident management framework is not required, incident response plans are.
- 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.
- Most observed information-sharing mechanisms involve bank-to-bank and bank-to-regulator communications, with the former mostly voluntarily.

[8] Document 05_10a
[9] Document 05_12a

- Regulatory frameworks for outsourcing activities across jurisdictions are quite established and share substantial commonalities.

3. EBA Guidelines

3.1. Guidelines on ICT and security risk management[10]

These guidelines, which entered into force on June 30, 2020 set out how financial institutions should manage the ICT and security risks that they face. Also, this guidance aims to provide the financial institutions to which the guidelines apply with a better understanding of supervisory expectations for the management of ICT and security risks. They integrate and are built on the requirements set out in the 'Guidelines on security measures for operational and security risks of payment services' (hereafter 'Guidelines on security measures'), which were published in December 2017 (EBA/GL/2017/17) and which have applied since January 2018 in fulfillment of the mandate in Article 95(3) of Directive 2015/2366/EU (PSD2). The text refers to 'ICT and security risk' instead of 'operational and security risk' to avoid confusion with broader operational risk issues, such as conduct risk, legal risk, and reputational risk. These guidelines consist of eight sections detailing how financial institutions should comply with addressing ICT and security risks, according to the provisions of Article 74 of Directive 2013/36/EU (CRD) and Article 95 of Directive 2015/2366/EU (PSD2).

3.2. Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)[11]

Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force in the European Union on January 12, 2016 and applied as of January 13, 2018. One of the 12 mandates conferred on the European Baking Authority (EBA), as specified in Article 95 of PSD2, requires the EBA to develop, in close cooperation with the European Central Bank (ECB), Guidelines (GL) on the security measures for operational and security risks of payment services. More specifically, PSD2 provides that payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. In fulfillment of this mandate, the too into account the existing EBA Guidelines on the Security of Internet Payments under PSD1 (EBA/GL/2014/12), and has also used as a basis existing standards and frameworks in other areas related to operational and security risks and adapted them where appropriate to the specificities of payment services. The EBA and the ECB have also carried out a risk analysis to determine the main threats and vulnerabilities to which PSPs are exposed.

[10] Document 05_05a
[11] Document 05_18a

3.3. Guidelines compliance table[12]

This table lists the competent authorities that comply or intend to comply with the EBA's Guidelines on Security Measures for Operational and Security Risks under PSD2.

4. Red Team Tests and Simulations Exercises

4.1. Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions[13]

The present paper by the Financial Stability Institute (FSI) of the Bank of International Settlements (BIS) describes key components of a red team testing framework, compares existing frameworks, outlines their benefits and challenges, and highlights potential cross-border issues relating to red team testing.

Red team tests are useful for identifying potential weaknesses in financial institutions' cyber protection, detection, and response capabilities to establish an effective remediation plan.

A red team test typically covers the entire financial institution, involving different teams, potentially including external hackers and threat intelligence providers. These tests run without the knowledge of those responsible for protecting the institutions from cyber-attacks.

Unlike other risk assessment exercises, a successful red team test does not mean that a firm "passes" or "fails" it. To truly benefit from red team testing, working after the test on the remediation of any weaknesses found is more valuable than just focusing on the test outcomes.

4.2. Financial Entities Ethical Red-Teaming[14]

The Saudi Arabia Monetary Authority (SAMA) has published its "Financial Entities Ethical Red Teaming Framework" (FEER). It is a guide for Member Organizations in preparing and executing controlled attacks against their live production environment, without exposing sensitive information.

SAMA does not see red teaming as an audit but as a simulation seeking to provide insights on the resilience and effectiveness of existing cybersecurity controls and processes (i.e., detection and response). In contrast to penetration tests, in which one or more specific information assets are tested and assessed), red teaming focuses on replicating a targeted and realistic attack against the entire Member Organization.

[12] Document 05_18b
[13] Document 05_06a
[14] Document 05_09a

The Framework's audience consists of Senior and Executive Management, business owners, owners of information assets, CISOs, and those responsible for defining, implementing, and reviewing cybersecurity controls.

4.3. Red Team: Adversarial Attack Simulation Exercises[15]

The Association of Banks of Singapore (ABS) published its Guidelines for the Financial Industry on red teaming, referred to in Singapore as "Adversarial Attack Simulation Exercises" (AASE).

According to the ABS Guidelines, the goal of an exercise is not to identify and report vulnerabilities that a financial institution may have but to represent the goals that real-world adversaries may want to obtain or understand.

The Guidelines propose a methodology for planning, preparing, executing, and closing red teaming exercises. The closure should lead to a strategic remediation management action plan involving the necessary process changes, tightening of security controls, investments, end-user security training, architecture redesign, and any other required improvements. It should also identify the staff responsible for tracking and reporting to senior management the implementation. The Guidelines also envisions sharing with other members of the industry or a broader community the lessons learned, naturally redacting details that would otherwise expose sensitive information.

5. Competency Standards for Cybersecurity Practitioners

5.1. Updated guide to the Hong Kong Monetary Authority's Enhanced Competency Framework on Cybersecurity[16]

HKMA's Enhanced Competency Framework on Cybersecurity (ECF-C) sets out the competency standards for cybersecurity practitioners of IT Security Operations and Delivery, IT Risk Management and Control, and IT Audit in the Hong Kong banking industry. This update includes six additional certifications of the Certified Cyber Attack Simulation Professional (CCASP) under the HKMA's ECF-C. The CCASP is a certification scheme developed by the HKMA in collaboration with the Hong Kong Applied Science and Technology Research Institute and the Hong Kong Institute of Bankers, and the support of the Council of Registered Ethical Security Testers International. The six new certifications are: 1) CCASP Practitioner Security Analyst, 2) CCASP Registered Tester, 3) Certified Infrastructure Tester, 4) Certified Web Application Tester, 5) Certified Simulated Attack Specialist, and 6) Certified Simulated Attack Manager.

[15] Document 05_13a
[16] Document 05_11a

6. Endpoint Security of Payments Systems

6.1. Reducing the risk of wholesale payments fraud related to endpoint security[17]

The Committee on Payments and Market Infrastructures (CPMI) published a "toolkit" to support central banks wishing to reduce the risk of wholesale payments fraud related to endpoint security in their institutions and jurisdictions. It defines an endpoint in the wholesale payments ecosystem as a point in place and time at which two parties in the ecosystem exchange, on behalf of themselves or third parties, a payment instruction.

Given the interconnections among stakeholders in the wholesale payments ecosystem, fraud may not only result in financial and reputational losses at the compromised endpoint. In an extreme case and in the absence of appropriate arrangements within the ecosystem for preventing, detecting, responding, and communicating about fraud may also undermine confidence in the integrity of the entire system.

CPMI has developed a strategy with seven elements designed to address all areas relevant to preventing, detecting, responding to, and communicating about wholesale payment fraud.

This toolkit provides context for the CPMI strategy and identifies steps that central banks could take to implement the strategy in a chronological sequence: (i) promotion; (ii) initial stocktaking; (iii) engagement with stakeholders; (iv) development of an action plan; and (v) monitoring progress. This toolkit is a "living document." As experiences and emerging practices for achieving the intended outcomes of the strategy develop further, the toolkit will also evolve. Also, not all emerging practices will be appropriate for all jurisdictions, and there is no "one size fits all" approach to implement the strategy. Instead, this toolkit aids central banks understand which emerging practices are relevant and appropriate and form their judgment.

7. NIST Special Publications

7.1. IT Asset Management[18]

The National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example solution packaged as a "How To" guide that demonstrates, using open source and commercially available products, how financial services can implement standards-based cybersecurity technologies for a more secure and efficient way of monitoring and managing their many information technologies (IT) hardware and software assets.

[17] Document 05_08a
[18] Document 05_15a

7.2. Privileged Account Management for the Financial Services Sector[19]

Financial organizations rely on privileged accounts to enable authorized users, such as systems administrators, to perform essential duties that ordinary users are not authorized to perform. The lack of oversight and technical control of privileged accounts poses a substantial operational and financial risk for organizations. If misused, privileged accounts can cause much damage, including data theft, espionage, sabotage, or ransom. The combination of detection and prevention policies and technologies is referred to as Privileged Account Management (PAM). The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to manage and monitor the use of privileged accounts by authorized users as they perform their normal activities, as well as techniques to protect against and detect the unauthorized use of privileged accounts. The solutions built in the NCCoE lab are not the only combination of technologies that can address this issue. They are examples demonstrating that off-the-shelf and open-source technologies are available to implement PAM.

This NIST Cybersecurity Practice Guide intends to help organizations confidently:

- control access to, and the use of, privileged accounts (both on-premises and in the cloud)
- manage and monitor the activity of privileged accounts
- audit the activity of privileged accounts
- receive alerts or notifications when privileged accounts are used for unauthorized or out-of-policy activities
- encourage personal accountability among the users of privileged accounts
- enforce stringent policies for "least privilege" and separation of duties

7.3. Access Rights Management for the Financial Services Sector[20]

This guide shows how financial sector companies can implement an Access Rights Management (ARM) platform using commercially available products. An ARM system enables a company to give the right person the right access to the right resources at the right time, thereby reducing the risk of unauthorized access caused by malicious actors or human error. The guide references NIST guidance, ISO/IEC standards, and Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT).

[19] Document 05_16a
[20] Document 05_19a

CONTENTS

DOCUMENTS
(in reverse chronological order)

05_01. BIS Working Paper No 865 – Drivers of cyber risk (May 2020)

This Working Paper publishes analyses using a database of over 100,000 cyber events across sectors. The paper notes following characteristics of cyber incidents: "Cyber costs are higher for larger firms and for incidents that impact several organisations simultaneously. The financial sector is exposed to a larger number of cyber attacks but suffers lower costs, on average, thanks to proportionately greater investment in information technology security. The use of cloud services is associated with lower costs, especially when cyber incidents are relatively small. As cloud providers become systemically important, cloud dependence is likely to increase tail risks. Crypto-related activities, which are largely unregulated, are particularly vulnerable to cyber attacks."

05_02. FSB Effective Practices for Cyber Incident Response and Recovery - Consultative Document (Apr 2020)

The Financial Stability Board (FSB) released Effective Practices for Cyber Incident Response and Recovery (CIRR) consultative document, intended to be a toolkit to assist organizations in their CIRR activities. This work comes after its stock taking publication of Cybersecurity Regulations, Guidance and Supervisory Practices in 2017, its development of a Cyber Lexicon in 2018. The FSB is collecting responses to the consultative document until 20 July 2020.

The toolkit is organized into seven components (Governance; Preparation; Analysis; Mitigation; Restoration; Improvement; and Coordination and Communication), which "comprises 46 effective practices that organisations have adopted while taking into account jurisdictions' legislative, judicial and regulatory frameworks, the size of the organisation affected by a cyber incident and the type of organisation that is affected."

The executive summary also notes that it "does not constitute standards for organisations or their supervisors and is not a prescriptive recommendation for any particular approach." It is meant to evolve over time, envisioned to "serve as a toolkit of options rather than applied in a one-size-fits-all manner, as not all practices are applicable to every organisation or in every cyber incident" and "may also be useful for authorities as they consider the approaches they may undertake with respect to regulation or supervision, or in responding to a cyber incident within the sector."

05_03. IIF/McKinsey Cyber Resilience Survey Cybersecurity posture of the financial services industry (Mar 2020)

"The Institute of International Finance (IIF) and McKinsey & Co. have completed a joint survey and research project around cyber resilience to provide an understanding of current

and planned practices that financial firms are undertaking to enable and strengthen firm-level and sector-level cyber resilience. 27 globally active firms participated in the survey and more than 50 companies participated in group discussions in meetings we convened with CRO's in the Americas, Asia, Europe and the Middle East.

The report "IIF/McKinsey Cyber Resilience Survey: Cybersecurity posture of the financial services industry" focuses on four different areas: firm-level cyber resilience, sector-level cyber resilience, costs and FTEs and next-generation trends. A key theme is around building up cyber security controls around supply chains, including third- or fourth-party risks, in areas such as vendor remote access management, activity monitoring and concentration risk.

Challenges reported by firms are regulations, cloud adoption, digitization and the talent gap. Firms said they are active in platforms to share threat intelligence and participate frequently in sector-wide cyber exercises. Automation is seeing extensive adoption soon to be followed by elements of cognitive computing. The document also includes a number of recommendations and industry practices, collected through the survey, that companies can draw on to enhance their cybersecurity posture."

05_04. BIS Working Paper No 840 - Operational and cyber risks in the financial sector (Feb 2020)

This Working Paper publishes analyses using cross-country data at the operational loss event level for the last 16 years for over 70 large banks. Conclusions include the following:

- After a spike in operational losses in the immediate aftermath of the [Great Financial Crisis], operational losses have declined in general since 2014. The post-crisis spike is to a large extent accounted for by the severity of losses related to improper business practices that occurred in large banks in the run-up to the crisis, which materialised only later.
- There is a substantial lag between the dates of discovery and recognition of loss events, which on average, exceeds one year, but it varies across regions, business lines, event types, and bank size.
- Authors show that operational value-at-risk can vary substantially for the FIs in the sample (6 to 12% of total gross income) depending on how the method captures the heavy-tailed nature of the data.
- They show that operational losses are higher after credit booms and after periods of excessively accommodative monetary policy. They also associate higher quality of financial regulation and supervision with lower operational risk losses and find that periods of increased bank competition lead a reduction in operational losses.
- Authors analyze losses from cyber events as a subset of operational events and find they are a small portion of overall operational risk losses, especially in frequency. They however recognize notable increases in loss amounts with a strong peak in 2016. This declined afterwards, which they say could be associated

with increased resources and higher quality of financial regulation and supervision in cyber security. Despite representing a relatively minor share of operational losses, cyber losses can account for up to a third of total operational value-at-risk.

05_05. EBA Final Report on Guidelines on ICT and security risk management (Nov 2019)

EBA published its "Guidelines on ICT and security risk management".

"The scope of application of the guidelines covers payment service providers (PSPs) for their payment services (any reference to 'payment services' includes 'issuing of electronic money'), credit institutions for all activities beyond their payment services and also investment firms for all activities...

These guidelines integrate the 'Guidelines on security measures for operational and security risks of payment services' under Article 95 of Directive 2015/2366/EU (PSD2), which were published in December 2017 (EBA/GL/2017/17), and elaborate further on certain topics that contribute to mitigating ICT and security risks in financial institutions. These guidelines therefore contribute to a level playing field for all financial institutions. The guidelines also address the European Commission (the Commission) request set out in the Commission's financial technology (FinTech) action plan published in March 2018, which requests that European Supervisory Authorities develop guidelines on ICT risk management and mitigation requirements in the EU financial sector."

"These guidelines specify the risk management measures that financial institutions (as defined in paragraph 9 below) must take in accordance with Article 74 of the CRD to manage their ICT and security risks for all activities and that payment service providers (PSPs as defined in paragraph 9 below) must take, in accordance with Article 95(1) of PSD2, to manage the operational and security risks (intended as 'ICT and security risks') relating to the payment services they provide. The guidelines include requirements for information security, including cybersecurity, to the extent that the information is held on ICT systems…

These guidelines are addressed to financial institutions, which for the purposes of these guidelines refers to (1) PSPs as defined in Article 4(11) of PSD2, and (2) to institutions, meaning credit institutions and investment firms as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013. The guidelines also apply to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013, including the European Central Bank with regard to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to competent authorities under PSD2, as referred to in point (i) of Article 4(2) of Regulation (EU) No 1093/2010.

The Guidelines address the following areas:

1. Proportionality;
2. Governance and strategy
3. ICT and security risk management framework
4. Information security

5. ICT operations management
6. ICT project and change management
7. Business continuity management
8. Payment service user relationship management

These guidelines will apply from 30 June 2020, repealing the "Guidelines on security measures for operational and security risks of payment services under PSD2" issued in 2017. Competent authorities must notify the EBA on compliance.

05_06. FSI Insights on Policy Implementation: Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions (Nov 2019)

The Financial Stability Institute (FSI) published its FSI Insights on policy implementation No. 21 "Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions".

"This paper aims to facilitate deeper understanding by financial sector authorities on different existing approaches that authorities have pursued in establishing red team testing frameworks. The paper is based on information provided by eight financial authorities and selected private sector players. It describes key components of a red team testing framework, compares existing frameworks, outlines the benefits and challenges of such frameworks, and highlights potential cross-border issues relating to red team testing."

05_07. FIGI-ECB-WB Cyber Resilience for Financial Market Infrastructures (Nov 2019)

"This document presents a methodology developed by the European Central Bank to operationalize the CPMIIOSCO Guidance on Cyber Resilience for FMIs (Guidance), which could be used by FMIs to comply with the Guidance and by authorities (supervisors and overseers) to assess their FMIs against the Guidance, hence enhancing the overall cyber resilience of financial market infrastructures critical for financial stability and financial inclusion." Summary can be found under the ECB's ECB-Cyber Resilience Oversight Expectations (CROE) of December 2018.

05_08. CPMI Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit (Oct 2019)

"The Committee on Payments and Market Infrastructures (CPMI) has prepared this "toolkit" to support central banks that wish to reduce the risk of wholesale payments fraud related to endpoint security in their institutions and jurisdictions. The CPMI has developed a strategy to reduce this risk that is composed of seven elements designed to work holistically to address all areas relevant to preventing, detecting, responding to and communication about wholesale payment fraud.

This toolkit provides context for the CPMI strategy and identifies steps that central banks could take to operationalise the strategy in a chronological sequence… Central banks may choose to operationalise individually, as part of a regional effort, or both.

This is a "living document". As central banks, operators, participants, and other stakeholders progress, and as their experiences and emerging practices for achieving the intended outcomes of the strategy develop further, the toolkit will also evolve."

04_01. IMF Department Paper No. DP/19/15 Cybersecurity Risk Supervision (Sep 2019)

The IMF's Monetary and Capital Markets Department published a Paper on Cybersecurity Risk Supervision.

"This paper highlights emerging supervisory approaches with the intention of promoting good practices. The paper draws on technical assistance work conducted by the IMF and on multilateral outreach with constituents and standards-setting bodies. Importantly, the paper identifies priorities for agencies in the process of establishing a regulatory and supervisory framework for supervision of cybersecurity risk, with a view to implementation that can overcome challenges typically faced by lower-income and lower-capacity supervisory agencies."

The paper covers 'The Nature of Risk' and 'Achieving Cyber Resilience', with Appendices on Cyber Insurance and Cyber Mapping.

04_02. Carnegie Endowment - Capacity-Building Tool Box for Cybersecurity and Financial Organizations (Jul 2019)

The Carnegie Endowment and partners published this toolkit (Full Report; Supplementary Report) on its website.

"To enhance the cyber resilience of financial institutions, the Carnegie Endowment for International Peace has partnered with the International Monetary Fund, the SWIFT Institute—the original sponsor of this project, the Financial Services Information Sharing and Analysis Center (FS-ISAC), Standard Chartered, the Cyber Readiness Institute, and the Global Cyber Alliance to develop this capacity-building tool box.

This website offers a series of action-oriented, easy-to-use one-page guides; complementary checklists; and a comprehensive, supplementary report detailing how financial institutions, particularly small- and mid-sized organizations as well as those that are less cyber mature, can enhance their own security as well as that of their customers and third parties. The guides and checklists are available in multiple languages (Arabic, Dutch, English, French, Portuguese, Russian, and Spanish.)"

04_03. FSB Cyber Incident Response and Recovery - Survey of Industry Practices (Jul 2019)

FSB launched an online survey of industry practices to help to identify effective practices at financial institutions.

The FSB is developing a toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident. The toolkit aims to provide financial institutions and authorities with a set of effective practices and will be based on the shared experience and diversity of perspectives gathered by the FSB, including through responses to its survey.

This survey is a key element of the FSB's outreach strategy with external stakeholders to gather views on effective practices relating to financial institutions' response to, and recovery from, a cyber incident. The development of the toolkit will also be informed by a review of publicly available documents on how firms have responded to and recovered from past cyber incidents and a stock-take of relevant publicly released guidance issued by national authorities and international organisations.

The survey closed on Wednesday, 28 August. A public consultation on the report will be launched in early 2020, with a view to finalising the toolkit of effective practices in late 2020.

05_09. SAMA Financial Entities Ethical Red-Teaming Framework (May 2019)

Saudi Arabian Monetary Authority (SAMA) published a Financial Entities Ethical Red-Teaming Framework (FEER) to guide Saudi Arabian financial entities "on how to conduct the red teaming activities and how to test the detection and response capabilities of the Member Organization against real sophisticated and advanced attacks and enhance the knowledge of the involved stakeholders. Likewise, the Framework aims to support the sharing of threat intelligence and lessons learned with the Member Organizations that will contribute to the cyber resilience of the Saudi Arabian Financial Sector. The Framework will ensure that the red teaming exercise is executed in a controlled manner..."

The Framework is mandated by SAMA and applies to all Member Organizations in the Financial Sector regulated by SAMA... Any Member Organization regulated by SAMA might be selected for red team exercise. Any organization can also choose to do a red team exercise. "However, as minimum, Domestic Systemic important entities will be subject to testing once every three (3) years, in line with this framework."

SAMA IT Risk of Financial Sector Supervision department has primary responsibility for overseeing the Red Teaming exercise and thus provides the Green Team, which appoints the Test Manager for each red teaming test. The Test Manager is responsible for guiding and supporting the White Team through the red teaming exercise. The Green Team approves the selection of Red Teaming Provider and provides – when applicable – additional or specific threat intelligence for the Financial Sector.

04_04. G7 2019 Conference "Cybersecurity: Coordinating efforts to protect the financial sector in the global economy" (May 2019)

Under the French G7 Presidency, Banque de France and the French Ministry for Economy and Finance organized a high-level conference on: Cybersecurity: Coordinating efforts to protect the financial sector in the global economy, on Friday 10 May 2019, Paris.

Concluding remarks by François Villeroy de Galhau - Governor, Banque de France, focuses on the importance of coordination across jurisdictions, sectors, and authorities with national security agencies. He also proposes three areas for improvement: regulation and supervision, information, and preparation, including large scale crisis simulation exercises, like the one coordinated by the Banque de France at the level of G7 joint crisis management exercise, to be held in early June, 2019.

04_05. FSB Progress Report to G20 on Cyber Incident Response and Recovery (May 2019)

Financial Stability Board (FSB) progress report summarises the work to date of its working group on Cyber Incident Response and Recovery (CIRR) and its workplan for developing effective practices for cyber incident response and recovery. The report was prepared for the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019.

The report notes the following: The development of the toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident will be done in two phases: 1) Identification and development of effective practices. Started in January 2019, to continue until October 2019. 2) Drafting of the toolkit. Likely start from November 2019, and subsequently involve a public consultation to be conducted in early 2020.

Background: "At the October 2018 Plenary meeting, the FSB agreed on the importance of having in place effective practices relating to a financial institution's response to, and recovery from, a cyber incident. In this regard, the FSB established a working group on Cyber Incident Response and Recovery (CIRR). The mandate of the CIRR is to develop a toolkit of effective practices to assist financial institutions, as well as for supervisors and other relevant authorities, in supporting financial institutions, before, during and after a cyber incident. The toolkit is not intended to be an international standard nor a prescriptive approach for financial institutions or their supervisors…"

04_06. CBR Regulation No. 683-P. Data protection at credit institutions (Apr 2019)

Central Bank of Russia released CBR Regulation No. 683-P "On Mandatory Requirements for Credit Institutions to Ensure Data Protection in Banking to Counter Unauthorised Funds Transfers". (Russian Only)

04_07. CBR Regulation No. 684-P. Data protection at non-credit institutions (Apr 2019)

Central Bank of Russia released CBR Regulation No. 684-P "On Mandatory Requirements for Non-Credit Financial Institutions to Ensure Data Protection with Regard to Operations in the Financial Markets in Order to Counter Illegal Financial Transactions" (Russian Only)

04_08. G7 Foreign Ministers Meeting - Dinard Declaration on the Cyber Norm Initiative (Apr 2019)

The G7 Foreign Ministers released the Dinard Declaration, establishing the Cyber Norm Initiative (CNI) from the G7 meeting in Biarritz, France, April 5-6, 2019.

The declaration notes that the CNI would be "dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, nonbinding norms of responsible State behavior. …contribute to the work by the UN Open-ended Working Group and Group of Governmental Experts, and by regional organizations, and would aim to demonstrate strong examples of adherence to these norms."

03_01. EC EU Cybersecurity Act (Apr 2019)

The European Council adopted the EU Cybersecurity Act. The Act gives a permanent mandate to the European Union Agency for Network and Information Security (ENISA) as Europe's Cybersecurity Agency and establishes an EU cybersecurity certification framework. It was proposed in September 2017.

03_02. ESAs Joint Advice on the costs and benefits of a coherent cyber resilience testing framework (Apr 2019)

European Supervisory Authorities (ESAs[21]) published a Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.

The publication is in response to a request to ESAs made by the European Commission in its March 2018 Fintech Action Plan.

The publication release states "that the ESAs see clear benefits of such a framework. However, at present there are significant differences across and within financial sectors as regards the maturity level of cybersecurity. In the short-term, the ESAs advise to focus on

[21] European Supervisory Authorities (ESAs[21]) consist of the following: European Banking Authority (EBA); European Insurance and Occupational Pensions Authority (EIOPA); and European Securities and Markets Authority (ESMA)

achieving a minimum level of cyber-resilience across the sectors, proportionate to the needs and characteristics of the relevant entities. Furthermore, the ESAs propose to establish on a voluntary basis an EU wide coherent testing framework together with other relevant authorities taking into account existing initiatives, and with a focus on Threat Lead Penetration Testing (TLPT). In the long-term, the ESAs aim to ensure a sufficient cyber maturity level of identified cross-sector entities.

To implement the proposed actions, the ESAs highlight the required legal basis and explicit mandate, which is necessary for the development and implementation of a coherent resilience testing framework across all financial sectors by the ESAs in cooperation with other relevant authorities."

03_03. ESAs Joint Advice on the need for legislative improvements relating to ICT risk management requirements (Apr 2019)

European Supervisory Authorities (ESAs) published a Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the European Union (EU) financial sector.

The publication is in response to a request by the European Commission in its March 2018 Fintech Action Plan to ESAs "to map, by Q1 2019, the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate a) to consider issuing guidelines aimed at supervisory convergence and enforcement of ICT risk management and mitigation requirements in the EU financial sector and, b) if necessary, provide the Commission with technical advice on the need for legislative improvements."

The document includes analysis of existing (EU) legislative requirements regarding ICT governance and security measures in the different sectors of the ESAs and detailed proposals both sectoral and cross-sectoral. ESAs highlight ICT incident reporting and appropriate oversight framework for critical third-party service providers as areas that may benefit from further action at EU-level.

The publication release states that "in developing the Joint Advice the ESAs' objective was that every relevant entity should be subject to clear general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. Guided by this objective, the proposals presented in the Advice aim at promoting stronger operational resilience and harmonization in the EU financial sector by applying changes to their respective sectoral legislation. Incident reporting is highly relevant to ICT risk management and allows relevant entities and authorities to log, monitor, analyze and respond to ICT operational, ICT security and fraud incidents. Therefore, the ESAs call for streamlining aspects of the incident reporting frameworks across the financial sector. Furthermore, the ESAs suggest that a legislative solution for an appropriate oversight framework to monitor the activities of critical third-party service providers should be considered."

05_10. NBG Regulation on Cybersecurity Management Framework of Commercial Banks (Mar 2019)

National Bank of Georgia (NBG) issued its regulation on Requirements for the Establishment of a Cybersecurity Management Framework by Commercial Banks, to be in force from April 1, 2019.

It requires all commercial banks (both resident and branches of non-resident foreign banks) operating in Georgia to establish a framework for cybersecurity management "appropriate and commensurate with the bank's size and complexity and the nature of its business" and "fully integrated into the bank's overall risk management process".

The regulation requires that the framework address five primary functions (Risk Identification; Protection; Discovery; Response; and Restoration) and goes on to describe the requirements in each function. The regulation further obliges the bank management to 1) regularly check the efficiency of the organization's cybersecurity / information security program; 2) conduct annual self-assessment of cyber security; 3) conduct a penetration test at least once a year, which includes all the information systems of the Bank that are connected to the network, and 4) conduct an annual independent audit of all components of the Bank's Cyber Security Management Framework. The information security audit must include risks associated with confidentiality, integrity and availability of systems.

04_09. ITU Global Cybersecurity Index (GCI) 2018 Survey (Mar 2019)

The United Nations International Telecommunications Union (ITU) published its latest Global Cybersecurity Index (GCI), which ranks 194 ITU member countries on their cybersecurity posture, places countries in three (high, medium, and low) levels of commitment to cybersecurity, and includes analysis based on the 2018 survey.

"The GCI is rooted in the ITU Global Cybersecurity Agenda (GCA) that was launched in 2007, and reflects its five pillars: legal, technical, organizational, capacity building, and cooperation. The GCI combines 25 indicators into one benchmark measure to monitor the cybersecurity commitment of 193 ITU Member States and the State of Palestine to the five pillars endorsed by the Global Cybersecurity Agenda (GCA).

The index uses data collected through an online survey. For each pillar, questions have been developed to assess commitment. Through consultation with a group of experts, the questions are weighted in order to generate an overall GCI score.

The overall result shows improvement and strengthening of all five pillars of the cybersecurity agenda in various countries in all regions. It should be noted, however, that the gap in the level of cybersecurity engagement between different regions is still present and visible. Besides providing the GCI score, this report also provides information on national practices that give insight to the progress achieved."

"These five designated areas form the basis of the indicators for GCI because they shape the inherent building blocks of a national cybersecurity culture:

1. Legal: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. Technical: Measures based on the existence of technical institutions and framework dealing with cybersecurity.
3. Organizational: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. Capacity building: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building.
5. Cooperation: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

03_04. EBA Guidelines on outsourcing arrangements (Feb 2019)

The European Banking Authority (EBA) published its Final Report on Guidelines on outsourcing arrangements**,** "setting out specific provisions for the governance frameworks of all financial institutions within the scope of the EBA's mandate with regard to their outsourcing arrangements and related supervisory expectations and processes. The aim of the Guidelines is to establish a more harmonised framework for these financial institutions, namely credit institutions and investment firms subject to the Capital Requirements Directive (CRD), as well as payment and electronic money institutions…

The new Guidelines, which are consistent with the requirements on outsourcing under the Payments Services Directive (PSD2), the Markets in Financial Instruments Directive (MiFID II) and the Commission's Delegated Regulation (EU) 2017/565 [on investment firms], aim at ensuring that institutions can apply a single framework on outsourcing for all their banking, investment and payment activities and services. Such a framework also ensures a level playing field between different types of financial institutions."

The Guidelines clarifies that the management body of each financial institutional remain responsible, among others, for overseeing all risks and managing outsourcing arrangements and ensuring compliance with EU legislation and regulatory requirements of service providers located in third countries. It helps differentiate which third party arrangements are to be considered outsourcing, and which of those are critical and important and as such are subject to stricter requirements. It also places requirements on competent authorities to effectively supervise financial institutions' outsourcing arrangements, with reliance on comprehensive documentation compiled by financial institutions themselves.

These Guidelines enter into force on 30 September 2019, with "some transitional periods for implementing a register of all outsourcing arrangements and to agree on cooperation agreements between competent authorities or to reintegrate outsourced functions or move them to other service providers, if the requirements of the guidelines can otherwise not be met."

05_11. HKMA Update on Guide to Enhanced Competency Framework on Cybersecurity (Jan 2019)

Hong Kong Monetary Authority updated its Guide to Enhanced Competency Framework on Cybersecurity (ECF-C), which sets out the competency standards for cybersecurity practitioners in the Hong Kong banking industry. The ECF on Cybersecurity (hereinafter referred to as "ECF-C") is a non-statutory framework, with objectives to "(a) to develop a sustainable talent pool of cybersecurity practitioners for the workforce demand in this sector; and (b) to raise and maintain the professional competence of cybersecurity practitioners in the banking industry."

The update includes six new certifications of the Certified Cyber Attack Simulation Professional (CCASP) under the HKMA's Cybersecurity Fortification Initiative (CFI) as additional options available to banking practitioners for meeting the ECF-C. The CFI was launched in 2016 to enhance HK banking sector's cyber resilience and includes introducing a common risk-based assessment framework for Hong Kong banks, a professional training and certification program that aims to increase the supply of qualified professionals, and a cyber-intelligence sharing platform."

The ECF-C Guide sets out a list of global and locally recognised certificates as qualifications to perform roles of 1) IT Security Operations and Delivery; 2) IT Risk Management and Control; and 3) IT Audit. The new CCASP is a localised certification scheme developed by the HKMA in collaboration with the Hong Kong Applied Science and Technology Research Institute and the Hong Kong Institute of Bankers. Others listed are the certification programs of the ISACA including Cybersecurity Nexus (CSX), the Global Information Assurance Certification (GIAC), the ISC^2, and locally, the Hong Kong Institute of Bankers (HKIB).

04_10. CBR Regulation No. 672-P – Data Protection in the Bank of Russia Payment System (Jan 2019)

Central Bank of Russia released CBR Regulation No. 672-P "On Requirements for Data Protection in the Bank of Russia Payment System". (Russian Only)

05_12. BIS Cyber-resilience: Range of practices (Dec 2018)

The Basel Committee on Banking Supervision published this report, which "identifies, describes and compares the range of observed bank, regulatory, and supervisory cyber-resilience practices across jurisdictions… rel[ying] on input from its member jurisdictions in response to a survey conducted by the Financial Stability Board (FSB) in April 2017."

The report discusses and makes some key observations in the following areas:

- current approaches taken by jurisdictions to issue cyber-resilience guidance standards;
- range of practices regarding governance arrangements for cyber-resilience;

- current approaches on cyber-risk management, testing, and incident response and recovery;
- various types of communications and information-sharing; and
- expectations and practices related to interconnections with third-party services provides in the context of cyber-resilience.

04_11. ECB TIBER-EU White Team Guidance (Dec 2018)

"The Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework enables European and national authorities to work with financial infrastructures and institutions… to put in place a programme to test and improve their resilience against sophisticated cyber attacks.

The ECB published the TIBER-EU Framework (TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming) and TIBER-EU Services Procurement Guidelines, respectively. This TIBER-EU White Team Guidance ("Guidance") is referred to in, and is an integral part of, the TIBER-EU Framework.

TIBER-EU is an instrument for red team testing, designed for use by core financial infrastructures, whether at national or at European level, which can also be used by any type or size of entity across the financial and other sectors. At the same time, TIBER-EU is designed to be adopted by the relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool, for financial stability purposes, or as a catalyst.

TIBER-EU facilitates red team testing for entities which are active in more than one jurisdiction and fall within the regulatory remit of several authorities. TIBER-EU provides the elements allowing either collaborative cross-authority testing or mutual recognition by relevant authorities on the basis of different sets of requirements being met.

When an authority adopts TIBER-EU, tests will only be considered TIBER-EU tests when they are conducted in accordance with the TIBER-EU Framework, including the TIBER-EU Services Procurement Guidelines and the TIBER-EU White Team Guidance.

The team that manages the test, in accordance with the TIBER-EU Framework, within the entity that is being tested, is called the White Team. The purpose of this document is to provide further guidance about the roles and responsibilities of the White Team."

04_12. COBIT 2019 (Dec 2018)

COBIT 2019 (Toolkit zip with Overview) was released, updating 2012's COBIT 5 in four core publications.

"COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise. COBIT defines the components and design factors to build and sustain a best-fit governance system.

The globally recognized COBIT 2019 Framework helps ensure effective EGIT, facilitating easier, tailored implementation—strengthening COBIT's continuing role as an important driver of innovation and business transformation….

COBIT 2019 Framework: Introduction and Methodology – an introduction to the key concepts of COBIT 2019.

COBIT 2019 Framework: Governance and Management Objectives – comprehensively describes the 40 core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks.

COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution – this guide explores design factors that can influence governance and includes a workflow for planning a tailored governance system for the enterprise.

COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution – this title represents an evolution of the COBIT 5 Implementation guide and develops a road map for continuous governance improvement. It may be used in combination with the COBIT 2019 Design Guide.

The COBIT 2019 product family is open-ended. Development of new guidance, training and resources to support the COBIT 2019 product family will be continuously assessed based on market demand and managed through ISACA's product roadmap."

03_05. ECB Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures: (Dec 2018)

On 3 December, ECB published the final cyber resilience oversight expectations (CROE) for financial market infrastructures. CROE is based on the Guidance on cyber resilience for financial market infrastructures by Committee on Payments and Market Infrastructures and the Board of the International Organisation of Securities Commissions (CPMI-IOSCO), published in June 2016.

CROE is meant to serve three key purposes: to provide 1) "…FMIs with detailed steps on how to operationalise the guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; 2) …overseers with clear expectations to assess FMIs under their responsibility; and 3)… the basis for a meaningful discussion between the FMIs and their respective overseers."

"The document had undergone public consultation which closed 5 June, 2018, by which responses were received from 20 entities, including FMIs, banks, banking communities and associations.

Comments in the public consultation mostly focused on four aspects:

- The level of prescriptiveness of the expectations;
- The three levels of cyber maturity and how these correspond to other international cybersecurity frameworks which also have maturity models;
- The process for oversight assessments against the cyber resilience oversight expectations; and
- The need for harmonisation across different jurisdictions and amongst regulators, to reduce the fragmentation of regulatory expectations and facilitate oversight convergence."

03_06. ENISA Cyber Europe 2018 After Action Report (Dec 2018)

ENISA published its After Action Report for Europe-wide Cybersecurity Exercise. This run of the bi-annual exercise by ENISA was focused on the Aviation industry, unlike earlier iterations.

The two-day exercise involving all 28 EU Member States as well as two European Free Trade Association (EFTA) countries, Norway and Switzerland involved 900 participants, from the public authorities and private companies, mainly from Aviation.

"The exercise simulated an intense realistic crisis caused by a large-number (over 600 hundred) of cybersecurity incidents… The exercise was built on three main pillars: The sound use of business continuity and crisis management plans within an organization; National-level cooperation and use of contingency plans; Cross-country cooperation and information exchange.

In addition, the exercise gave the opportunity to the technical teams to test their skills in cybersecurity with a vast variety of technical challenges, including malware analysis, forensics, mobile malware, APT attacks, network attacks, IoT device infection, etc. The exercise brought up the importance of cooperation between the different actors (victims and authorities) of simulated cybersecurity incidents, security providers and national authorities. It proved to the participants that only by information exchange and collaboration, it is possible to respond to such extreme situations with a large number of simultaneous incidents…."

The report details key findings and recommendations. Observations include that EU-level cooperation has improved over the last years, particularly that "introduction of the CSIRTs Network (CNW) as defined in the NIS directive has provided EU Member States with an effective formal structure to exchange technical information but also to collaborate in order to resolve complex, large-scale incidents." It notes that operational-level cooperation was tested to a lesser extent and will be included more in future exercises.

While vast public-private and private-private coordination occurred, "the level of preparedness varied significantly between participants, the information flow felt sometimes to be unidirectional and structured private-public cooperation procedures were immature or non-existent. The EU Network and Information Security (NIS) directive

identifies many of the associated shortcomings and proposes measures to improve the situation."

03_07. ECB "UNITAS" Crisis communication exercise report (Dec 2018)

The Eurosystem's Market Infrastructure and Payments Committee (MIPC) carried out a market-wide crisis communication exercise in late June 2018 and released a post-exercise report summarizing the objectives of the exercise, the scenario, the key conclusions and the next steps.

"The exercise was conducted in the form of a facilitated discussion around a hypothetical scenario based on a cyber attack on major financial market infrastructures (FMIs), market infrastructures and service providers (collectively "financial infrastructures") resulting in a loss of data integrity.

The exercise was intended to: (i) raise awareness of data integrity issues and the implications for financial infrastructures; (ii) discuss how impacted financial infrastructures could cooperate and collaborate with each other and other relevant stakeholders on a pan-European basis; and (iii) assess the need for developing external public communication strategies.

…The name "UNITAS" was chosen to reflect the core theme of the exercise, which was to promote collaboration and a united approach in managing cyber attacks affecting financial infrastructures in Europe."

Participants consisted of the following: 1) Payment Systems (TARGET2; EURO1; STEP2-T; CORE(FR); EMZ; SNCE; equensWorldline; BI-Comp); 2) Central securities depositories (CSDs) and central counterparties (CCPs) (Euroclear; Clearstream Banking AG (CBF); Monte Titoli; Eurex Clearing; LCH SA); 3) Service providers and market infrastructures (SWIFT; SIA-Colt; T2S); and 4) Central bank overseers (European Central Bank; Banque de France; Nationale Bank van België/Banque Nationale de Belgique; Deutsche Bundesbank; De Nederlandsche Bank; Banca d'Italia; Banco de España).

The following were Observers: 1) European Securities and Markets Authority (ESMA); 2) European Union Agency for Network and Information Security (ENISA); 3) Eurosystem Internal Auditors Committee representatives; and 4) MIPC members.

05_13. ABS Red Team: Adversarial Attack Simulation Exercise. Guidelines for the Financial Industry in Singapore (Nov 2018)

The Association of Banks in Singapore (ABS) published a Guideline for Adversarial Attack Simulation Exercises (AASE), otherwise known as Red Team (RT) Exercises.

"This guideline is intended to support FIs within Singapore… provides guidance on best practices and recommendations on how to adopt them partially or in full, and depending

on the maturity of the FI's capability in conducting these exercises. This document aids in planning and executing such exercises but should not be relied on solely to achieve compliance with regulations. It is expected that the objectives, test scenarios and the report structure will be tailored according to the FI's scale, operations, external threat landscape and risk appetite…"

The Guideline explains AASEs against other simulations such as Penetration tests or real-life attacks. Then explains guiding principles for success of the exercise: 1) that the exercise goals should be from the point of view of the attacker (e.g. financial gain, to effect an unauthorized fund transfer), not from the point of view of the financial institution (e.g. to find vulnerabilities of the FI); 2) "The scope, nature and timing of the exercise should be kept secret to adequately assess the effectiveness of security defences and response to cyber-attack scenarios."; 3) "Exercise scenarios should be designed to target Critical Functions of the organisation and in a manner that is aligned with the motives of expected adversaries (in the production environment).; 4) "Exercises should be conducted periodically. In each iteration of the exercise, the scenarios and sophistication of the TTPs used could be adjusted with the improvements made in the organisations cyber preparedness, security operations, as well as variations in the threat landscape."; and 5) "Exercise duration will be determined by the complexity of the attack scenarios, and the scale of the organisation being examined."

It goes on to describe the Methodology in detail through phases of Planning, Preparation, Execution, and Closure.

03_08. FSB Cyber Lexicon (Nov 2018)

On 12 November, FSB published the final Cyber Lexicon, after a draft released 2 July went through a public consultation period until 20 August. A summary overview of the responses to the public consultation was also published.

This delivery follows the FSB Stocktake Report delivered in October 2017; both are in response to G20 Finance Ministers and Central Bank Governors.

"The lexicon comprises a set of approximately 50 core terms related to cyber security and cyber resilience in the financial sector.

The Cyber Lexicon is intended to support the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions and international standards organisations, to address financial sector cyber resilience. The lexicon could be useful to support work in the following areas:

- Cross-sector common understanding of relevant cyber security and cyber resilience terminology;
- Work to assess and monitor financial stability risks of cyber risk scenarios;
- Information sharing as appropriate; and

- Work by the FSB and/or standard-setting bodies to provide guidance related to cyber security and cyber resilience, including identifying effective practices.

For example, the Cyber Lexicon will be used to support work on a recently announced FSB project to develop effective practices relating to a financial institution's response to, and recovery from, a cyber incident. A progress report on this project will be published by mid-2019."

05_14. Brookings Institute - The Future of Financial Stability and Cyber Risk (Oct 2018)

This paper "considers the ways in which cyber risks differ from traditional financial shocks. In contrast to the financial and policy shocks that have triggered past financial panics, cyber attacks are generally designed and initiated by sentient adversaries in aggressive pursuit of specific malicious goals. If one of those goals is broad financial system instability, a cyber attack may pose unique challenges.

Unfortunately, the interactions between the financial contagion channels and the technological and operational risk channels of cyber attacks have not been examined carefully. For example, a sustained attack on a large global financial institution could be contagious across both dimensions, but where and how the contagion channels might feed on each other and accelerate risk is an important area for future work. This paper starts by examining traditional risks to financial stability, such as contagion from excessive leverage. It also examines the current regulatory frameworks and partnerships, both domestic and international, established to increase the resilience of the financial system to cyber risk. The analysis concludes with major concerns and potential gaps in understanding and mitigating cyber risks to financial stability."

04_13. G7 Fundamental Elements for Threat-Led Penetration Testing (Oct 2018)

The G-7 published its guidance "Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT)", as part of its efforts "to promote the development of frameworks to enhance public and private sector approaches to strengthening cyber resilience of critical entities in the financial system"

In 2016, it published the publication G-7 Fundamental Elements of Cybersecurity for the Financial Sector ("G7FE"), followed by the G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector ("G7FE-Assessment"), published in 2017.

This new guidance seeks to "provide entities with a guide for the assessment of their resilience against malicious cyber incidents through simulation and a guide for authorities considering the use of Threat-Led Penetration Testing (TLPT) within their jurisdictions. These fundamental elements are intended to complement a wider suite of cyber resilience

assessment tools and techniques, and are not meant to be considered as a singular approach.

The core objectives of the G7FE-TLPT are to enhance and assess the cyber resilience of entities and the financial sector more generally, by:

- Providing core elements of and approaches for the conduct of TLPT across G-7 jurisdictions. The G7FE-TLPT aim to facilitate greater compatibility among TLPT approaches, whilst also encouraging flexibility and local tailoring based on the unique markets and regulations within each jurisdiction;
- Providing a guide to authorities considering the use of TLPT within their jurisdiction;
- Providing a guide to entities with respect to conducting their own TLPT assessments; and
- Supporting cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results…."

03_09. G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector (Oct 2018)

The G7 governments released Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.

Earlier, the G7 published G-7 Fundamental Elements of Cybersecurity for the Financial Sector in October 2016, and the G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector in October 2017.

As those that came before it, "this is a set of Fundamental Elements for entities to tailor, as appropriate, to their specific risk profiles, operational and threat landscape, role in the sector, and legal and regulatory frameworks. The elements are non-binding and do not invalidate existing frameworks or prevent their continuous adaptation.

The following Fundamental Elements consider the Third-Party Cyber Risk Management Life Cycle within an individual entity and system-wide monitoring of cyber risk. Entities and third parties can use them as part of their cyber risk management toolkit… Authorities within and across jurisdictions can use the Fundamental Elements to inform their public policy, regulatory and supervisory efforts to address third party cyber risks."

Third Party Cyber Risk Management Life Cycle

- Element 1: Governance - *Entities' governing bodies are responsible and accountable for effective oversight and implementation of third-party cyber risk management.*
- Element 2: Risk Management Process for Third Party Cyber Risk - *Entities have an effective process for managing third party cyber risks through the entire third-party risk management life cycle.*

- Element 3: Incident Response - *Entities establish and exercise incident response plans that include critical third parties.*
- Element 4: Contingency Planning - *Entities have appropriate contingency plans in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber risks outside the entity's risk appetite.*

System-wide Monitoring of Cyber Risk and Cross Sector Coordination Management

- Element 5: Monitoring for Potential Systemic Risks - *Third party relationships across the financial sector are monitored and sources of third-party cyber risk with potential systemic implications are assessed.*
- Element 6: Cross-sector coordination - *Cyber risks associated with third party dependencies across sectors are identified and managed across those sectors.*

03_10. CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Services Providers (Oct 2018)

Central Bank of Nigeria (CBN) released risk-based cybersecurity framework and guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), to be complied with by January 1, 2019. The release outlines the minimum cybersecurity baseline, providing guidance in the implementation of their cybersecurity programmes towards enhancing their resilience.

"Resilience provides an assurance of sustainability for the organisation using its governance, interconnected networks and culture. DMBs/PSPs should note that for a cybersecurity programme to be successful, it must be fully integrated into their business goals and objectives, and must be an integral part of the overall risk management processes.

The framework provides a risk-based approach to managing cybersecurity risk. The document comprises five parts: Cybersecurity Governance and Oversight, Cybersecurity Risk Management System, Cybersecurity Operational Resilience, Metrics, Monitoring & Reporting and Compliance with Statutory and Regulatory Requirements."

It includes such requirements for DMBs and PSPs to "establish an information security steering committee that shall be responsible for the governance of the cybersecurity programme" to be headed by the Chief Information Security Officer (CISO), and definition of cyber-incident as that resulting in a significant financial loss, defined as "loss that exceeds 0.01% of shareholders' funds unimpaired by losses."

03_11. US FSSCC Financial Services Sector Cybersecurity Profile (Oct 2018)

The Financial Services Sector Coordinating Council (FSSCC) has published a "Financial Services Sector Cybersecurity Profile", which NIST describes as the "customization of the NIST Cybersecurity Framework that financial institutions can use for internal and

external cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks."

The FSSCC site explains: "What It Is: The Profile is a scalable and extensible assessment that financial institutions of all types can use for internal and external (i.e., third party) cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks (a "common college application for regulatory compliance") both within the United States and globally.

Why It Was Created: When surveyed two years ago, Chief Information Security Officers from financial institutions indicated that nearly 40% of their time, and their teams' time, was spent reconciling various cybersecurity and regulatory frameworks.

For financial institutions, if the Profile approach is implemented, accepted by regulators for use, and maintained, the benefits of focusing cybersecurity experts time on protecting global financial platforms, rather than compliance activity, will be significant. For an industry already burdened by a shortage of adequately skilled individuals, reducing this percentage by streamlining compliance is a tremendous benefit.

For the regulatory community, Profile usage will enhance their visibility across firms, subsectors, third parties, and other sectors, which will enable better analysis and mitigation of systemic and concentration risks."

The Profile Downloads consist of the following: 1) the MS-Excel based Profile All-In-One Assessment Tool; 2) Profile Overview and User Guide; 3) Profile Impact Tiering Questionnaire; 4) Profile Diagnostic Statements and Mapping-only Spreadsheet on MS-Excel; and 5) The Roadmap Forward**.**

Background: The Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security, is a member organization in the U.S. established in 2002. Its website describes that has "70 members consist[ing] of financial trade associations, financial utilities, and the most critical financial firms. FSSCC partners with the public sector on policy issues concerning the resilience of the sector. Over the years, the FSSCC has built and maintained relationships with the U.S. Treasury and Homeland Security Departments, all the federal financial regulatory agencies (e.g., Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, Office of Comptroller of the Currency, Securities and Exchange Commission), and law enforcement agencies (e.g., Federal Bureau of Investigation, U.S. Secret Service). Through these relationships, the FSSCC directly assists the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types."

03_12. Bank of Ghana Cyber & Information Security Directive (Oct 2018)

Bank of Ghana released a Cyber and Information Security Directive, which "provides a framework for establishing Cyber and Information Security protocols and procedures for; routine and emergency scenarios, delegation of responsibilities, inter- and intra-company communication and cooperation, coordination with government authorities, establishment

of reporting mechanisms, physical security measures for IT Datacentres and Control Rooms, and assurance of data and network security."

The Directive is applicable to all entities regulated by the Bank of Ghana and lists obligations including that "All institutions supervised by the BoG shall be ISO270011 certified and should adopt ISO27032."; "Institutions that handle, process, store, or transmit debit card, credit card, prepaid card, e-purse, ATM cards, and/or POS) and related information shall be PCI-DSS2-certified."; and "The methodology for managing and handling cyber and information security events shall comply with international standards such as National Institute of Standards and Technology (NIST) and ISO 27001."

The document is arranged into the following sections: 1) Preliminary Matters; 2) Governance; 3) CISO; 4) Cyber Security Risk Management; 5) Asset Management; 6) Cyber Defence; 7) Cyber Response; 8) Employee Access to ICT Systems; 9) Electronic Banking Services; 10) Training, Awareness and Competence; 11) External Connections; 12) Cloud Services; 13) Banks with International Affiliation; 14) Physical Security; 15) Human Resource Management; 16) Contractual Aspects; 17) Interpretation (definitions); 18) Implementation Schedule (ranging from six to 24 months); 19) Enhanced Competency Framework; and 20) (Reporting) Return on Cyber Security Incidents.

05_15. NIST Cybersecurity Practice Guide, IT Asset Management (Sep 2018)

The NIST Cybersecurity IT Asset Management Practice Guide (final) SP1800-5 is "a proof-of-concept solution demonstrating commercially available technologies that can be implemented to track the location and configuration of networked devices and software across an enterprise. Our example solution spans traditional physical asset tracking, IT asset information, physical security, and vulnerability and compliance information. Users can now query one system and gain insight into their entire IT asset portfolio.

This guide:

▪ maps security characteristics to guidance and best practices from NIST and other standards organizations, including the Payment Card Industry Data Security Standard (PCI DSS)

▪ provides: a detailed example solution with capabilities that address security controls; instructions for implementers and security engineers, including examples of all the necessary components for installation, configuration, and integration

▪ is modular and uses products that are readily available and interoperable with your existing IT infrastructure and investments."

(The NIST Special Publication 1800 series target specific cybersecurity challenges in the public and private sectors, maps capabilities to the NIST Cyber Security Framework, and details the steps needed for another entity to recreate the example solution. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity.)

05_16. NIST Special Publication (SP) 1800-18 Privileged Account Management for the Financial Services Sector (Sep 2018)

This Guide (draft) outlines reference design and example solutions for privileged account management (PAM) for the financial services sector.

"Financial organizations rely on privileged accounts to enable authorized users, such as systems administrators, to perform essential duties that ordinary users are not authorized to perform… Privilege misuse is a major contributor of reported cyber incidents… Privileged accounts pose significant operational, legal, and reputational risk to organizations if not secured effectively."

"Organizations must harden themselves against these operational and reputational risks by implementing policies and technologies that detect and prevent the misuse of privileged accounts by external and internal actors. This combination of detection and prevention technologies and policies is referred to as privileged account management (PAM)… After reading this NIST Cybersecurity Practice Guide, an organization should be able to implement a PAM system that effectively monitors and manages privileged accounts."

(The NIST Special Publication 1800 series target specific cybersecurity challenges in the public and private sectors, maps capabilities to the NIST Cyber Security Framework, and details the steps needed for another entity to recreate the example solution. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity.)

(The public comment period closed on November 30, 2018 - no final version yet available at time of Digest 5th edition publication.)

03_13. California Law on Security of Connected Devices (Sep 2018)

Senate Bill No. 327, Information privacy: connected devices, was signed into law – the first such law in the U.S. covering security of connected/ 'smart' devices (IoT). Coming into effect on 1 January 2020, the manufacturer of a device (selling in California) connecting "directly or indirectly" to the internet must ensure "reasonable" security features: "to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure". Further, it provides that if the device can be connected outside a local area network, it is required to come with a password unique to each device or require the user to set a password at first use, in contrast to being given industry default, easily hackable, passwords.

03_14. CBK Draft Guidelines on Cybersecurity for Payment Service Providers (Aug 2018)

Central Bank of Kenya (CBK) has developed a draft Cyber Security Guidelines for Payment Service Providers. "The objective is to create a safer and more secure cyberspace that underpins information system security priorities, to promote stability of the Kenyan payment system sub-sector. The Guidelines sets the minimum standards that PSPs should adopt to develop effective cybersecurity governance and risk management frameworks in order to maintain a sound, secure and efficient National Payment System."

Specific Requirements consist of areas of delineating Categories of Payment Service Providers; Governance of PSPs; General Risk Management Requirements for PSPs; Dependency Risk Management Strategies & Cyber Resilience, including incident response; Regular Independent Assessment and Testing; Outsourcing; and Training/Awareness.

Reporting requirements consisted of the following: 1) All PSPs to submit their Cybersecurity Policy, strategies and frameworks to the Central Bank of Kenya by August 31, 2018; 2) Reporting to CBK within 24 hours of any Cybersecurity incidents…; and 3) a quarterly reporting to CBK regarding occurrence and handling of Cybersecurity incidents.

Public comments were due by September 14, 2018.

02_01. ECB TIBER-EU Framework & Services Procurement Guidelines: (Aug 2018 & May 2018)

In May, ECB released a single Europe-wide framework for controlled cyber hacking to test resilience of financial market entities called "TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming". A related Services Procurement Guideline followed in August.

"The TIBER-EU framework facilitates a harmonised European approach towards intelligence-led tests which mimic the tactics, techniques and procedures of real hackers who can be a genuine threat. TIBER-EU based tests simulate a cyber attack on an entity's critical functions and underlying systems, such as its people, processes and technologies. This helps the entity to assess its protection, detection and response capabilities against potential cyber attacks..."

The Framework is "designed for national and European authorities and entities that form the core financial infrastructure, including entities with cross-border activities which fall within the regulatory remit of several authorities. The framework can be used for any type of financial sector entity, as well as entities in other sectors.

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 a higher level of cyber maturity."

Given the risks to such tests, the ECB further published Services Procurement Guidelines: "To ensure a controlled and safe test, one prescribed control is the use of specialist external threat intelligence (TI) and red team (RT) providers, which have the highest level of skills and expertise, and have the requisite experience in threat intelligence and red team testing in the financial services industry..."

The Guidelines "set out the requirements and standards that must be met by TI and RT providers to deliver recognised TIBER-EU tests; offer guiding principles and selection criteria for entities, as they look to procure services from prospective providers; and provide questions and agreement checklists that could be used when entities undertake their due diligence and look to formalise the procurement process with the TI/RT providers."

02_02. IIF Cloud Computing paper (Part 1) (Aug 2018)

The Institute of International Finance (IIF) published the first part of its 3-part series on Cloud technology in the financial services industry. "This paper examines the key opportunities and risks (and mitigants) of migrating to cloud, as well as simultaneously looking at the business and operational risks that arise for firms with not moving to cloud. Given these business drivers, it observes that as financial institutions are defining their strategy on cloud, the decisions are increasingly more in the order of "how," rather than merely in whether to pursue cloud.

The subsequent parts in this series will explore some of the hurdles (both regulatory and non-regulatory in nature) to cloud adoption, with recommendations for how these can be addressed, as well as analysis of the role of Cloud Services Providers (CSPs) for the sector, including issues such as concentration risk and critical dependency."

02_03. NIST Small Business Cybersecurity Act (Aug 2018)

The National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act introduced March 2017 became law in August 2018. The Act will be "… require the Director of the National Institute of Standards and Technology to disseminate guidance to help reduce small business cybersecurity risks …"

04_14. FSISAC CERES Forum (Jul 2018)

Financial Services Information Sharing and Analysis Center (FS-ISAC) announced the launch of the CERES (CEntral banks, REgulators and Supervisory entities) Forum effective July 1, 2018. The CERES Forum is set to be "a new information sharing group

for central banks, regulators and supervisors to share information impacting global security and resiliency and guard against ever-growing cyber and physical threats." CERES Forum is membership based, independent from FS-ISAC (a non-profit corporation that was established in 1999 and is funded by its 7,000 member firms headquartered in 44 countries with users in 72 countries). Forum membership is to provide "top-down information from FS-ISAC, [and] a means of discussing current threats, trends, best practices and solutions with your peers in financial oversight institutions…. Information sharing among CERES Forum members occurs through a secure portal, coordinated conference calls, live events and focused email distribution lists."

05_17. CEPS-ECRI Cybersecurity in Finance Getting the policy mix right! (Jun 2018)

Following the European Commission's "Cybersecurity package: 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'" adopted September 2017, CEPS-ECRI organised a Task Force in order to analyse the issues that are considered to be relevant to financial fields (retail banking, corporate banking, capital markets, financial infrastructure and insurance). This report publishes the work of the Task Force, with a group of experts from the financial industry, tech industry, national supervisors and European institutions, as well from one consumer association and one law firm. The European Credit Research Institute (ECRI), managed by the Centre for European Policy Studies (CEPS), is an independent think tank that carries out research and contributes to the policy debate on financial services in Europe.

It recommends nine policy issues that "need to be further addressed in order to bolster the financial industry's cyber-resilience against current and future threats…

Main policy recommendations

1. Convergence in the taxonomies of cyber-incidents is needed.
2. The framework for incident reporting needs to be significantly improved to fully contribute to the cyber-resilience of financial firms.
3. Authorities should assess how and to what extent the data held by the centralised hub should be shared with supervisors, firms and clients.
4. Ambitious policies are needed to develop consistent, reliable and exploitable statistics on cyber-trends.
5. Best practices for cyber-hygiene should be continuously enhanced by regulators and supervisors.
6. The European Cybersecurity Certification Scheme needs to be strengthened to contribute better to cybersecurity, cyber-risk management and capability.
7. In order to improve the processes of attribution and extradition, the reinforcement of cross-border cooperation and legal convergence remains a priority, both within the EU and more widely.
8. Best practices in remedies in case of cyberattacks need to be further encouraged.
9. Policy-makers should further assess the pros, cons and feasibility of creating an emergency fund in case of large cyberattacks."

03_15. California Consumer Privacy Act of 2018 (Jun 2018)

Assembly Bill No. 375, i.e. California Consumer Privacy Act of 2018, passed into law, which will be in effect beginning 1 January 2020.

"…it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights: …to know what personal information is being collected about them; …to know whether their personal information is sold or disclosed and to whom; …to say no to the sale of personal information; …to access their personal information; …to equal service and price, even if they exercise their privacy rights."

03_16. CSA Singapore Cyber Landscape (Jun 2018)

The Cyber Security Agency of Singapore (CSA) published its "second edition of the Singapore Cyber Landscape reviews the cybersecurity situation in 2017 against the backdrop of global trends and events. Through case studies of incidents in Singapore, the publication aims to offer insights and practical lessons to mitigate and recover from cyber-attacks. This edition also features some emerging trends and issues that Singapore is watching closely."

The Cyber Security Agency of Singapore (CSA) is the national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information.

02_04. UK Minimum Cyber Security Standard (Jun 2018)

The UK government released a "UK Minimum Cyber Security Standard", which "defines the minimum security measures that Departments shall implement with regards to protecting their information, technology and digital services to meet their [Security Policy Framework] and National Cyber Security Strategy obligations."

The Standard includes ten requirements of all Departments (including "organisations, agencies, Arm's Length Bodies and contractors"), split into five areas:

"IDENTIFY

1. Departments shall put in place appropriate cyber security governance processes.
2. Departments shall identify and catalogue sensitive information they hold.
3. Departments shall identify and catalogue the key operational services they provide.
4. The need for users to access sensitive information or key operational services shall be understood and continually managed.

PROTECT

5. Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems.

6. Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.
7. Highly privileged accounts should not be vulnerable to common cyber-attacks.

DETECT

8. Departments shall take steps to detect common cyber-attacks.

RESPOND

9. Departments shall have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.

RECOVER

10. Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise."

As the first technical standard (which will be incorporated into the Government Functional Standard for Security once published), the Minimum Cyber-security Standard references the National Cyber Security Strategy and the HMG Security Policy Framework (SPF). The SPF, published in final version in May 2018, provides the mandatory protective security outcomes that all Departments are required to achieve in the following areas: Good Governance; Culture and Awareness; Risk Management; Information; Technology and Services; Personnel Security; Physical Security; Preparing for and Responding to Security Incidents. It details the Policy Priorities in three areas: Information Security; Physical Security; and Personnel Security and National Security Vetting. Further, it notes:

"HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure, National Cyber Security Centre, and other sources of good practice to shape their business specific approaches, mindful that:

- Government organisations know their own business best, including how local risks should be managed to support operations and services.
- Permanent Secretaries/Heads of Department are accountable to Parliament for the security of their organisations.
- An annual reporting process (the Security Risk Management Overview) will ensure compliance and an appropriate level of commonality across government."

02_05. Canada's updated Cyber Security Strategy (Jun 2018)

Canada's new National Cyber Security Strategy, published in June 2018, replaced the 2010 Strategy. Renewing its commitment to strong cyber security, it recognizes "evolving threats, emerging opportunities, and the need for collaborative action" in three thematic areas:

- "Security and Resilience: Through collaborative action with partners and enhanced cyber security capabilities, we will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems.

- Cyber Innovation: By supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge, the federal government will position Canada as a global leader in cyber security.
- Leadership and Collaboration: The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

The update comes after an online public consultation which was undertaken by the Government in 2016, with a report published in January 2017. "… three ideas were consistently raised as being important and relevant to cyber security in Canada: privacy, collaboration, and using skilled cyber security personnel. Across the full range of consultation topics, participants stressed the need to uphold all Canadians' privacy rights, the need for stakeholders to collaborate with one another (i.e., governments, private sector, law enforcement, academia, non-profit organizations), and the need to rely on cyber security experts. In addition to these three ideas that permeated the results, the Government of Canada cyber security consultation yielded recommendations on specific areas for action, needs and means, and barriers and constraints…" There was also an Action Plan covering the years 2010-2015 stemming from the Strategy. (FSB-ST[i])

03_17. Estonia Cybersecurity Act (May 2018)

Estonia passed into law its Cybersecurity Act, which transposes into local law the EU Directive 2016/1148 on security of network and information systems (NIS Directive) by the deadline of 9 May 2018.

The Act "provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents."

Among other things required by Directive 2016/1148, it designates the Estonian Information System Authority (RIA) as the computer incident response team and specifies other roles such as "ensuring cybersecurity and preventing and resolving a cyber incident". It requires digital service provider to take measures to ensure security of a system and to notify the RIA of cyber incident within certain parameters.

03_18. CPMI Reducing the risk of wholesale payments fraud related to endpoint security (May 2018)

The Committee on Payments and Market Infrastructures (CPMI) published a document to address fraud in the wholesale payment ecosystem, in particular caused by weaknesses in security at one endpoint in the ecosystem.

It is "a strategy to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud related to endpoint security. The strategy is composed of seven elements designed to work holistically to address all areas relevant to preventing, detecting, responding to and communicating about fraud.

Successful operationalisation of the strategy depends on operators, participants and other relevant private sector and public sector stakeholders in each jurisdiction engaging actively in and taking ownership of developing and carrying out an appropriate action plan for their respective jurisdictions. Accordingly, the CPMI has set out a plan to promote, support and monitor local and global progress in operationalising the strategy. Each CPMI member central bank, and the CPMI as a whole, is committed to acting as a catalyst for effective and coherent operationalisation of the strategy within and across jurisdictions and systems and will monitor progress throughout 2018 and 2019 to determine the need for further action."

- Element 1: Identify and understand the range of risks
- Element 2: Establish endpoint security requirements
- Element 3: Promote adherence
- Element 4: Provide and use information and tools to improve prevention and detection
- Element 5: Respond in a timely way to potential fraud
- Element 6: Support ongoing education, awareness and information-sharing
- Element 7: Learn, evolve and coordinate

04_15. G7 Ise-Shima Cyber Group - Chair's Report of the Meeting (Apr 2018)

Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group was published at the G7 Foreign Ministers meeting in Toronto, April 23, 2018. G7 Ise-Shima Cyber Group was established in May 2016.

"All G7 partners reiterated their shared vision of an accessible, open, interoperable, reliable and secure cyberspace the benefits of which can be enjoyed by all… G7 partners emphasised the importance of developing policies to promote digital security and to ensure trust and stability in cyberspace, taking into account the responsibility of all actors, including those from the government and private sector, to contribute to this effort… The rising sophistication and cost of cybercrime was also discussed, including the increasing role of transnational organized crime and the links with state actors…

…Partners expressed regret that the most recent United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was unable to adopt a consensus report in 2017 when some countries' experts walked back from previous reports' statements on the applicability of international law to states' activities in cyber space; an outcome which should concern all those committed to security and stability in cyber space. They emphasized that despite this outcome, the recommendations contained in the 2010, 2013 and 2015 UN GGE reports remain valid. They decided to continue to support efforts, at the UN and elsewhere,

to promote affirmation of the applicability of existing international law to states' cyber activities – including the UN Charter and customary international law, and notably international humanitarian law and international human rights law as well as the promotion and implementation of certain voluntary, non-binding peace-time norms of responsible state behaviour…"

03_19. EC IACS Cybersecurity Certification Framework (ICCF): Lessons from the 2017 study of the state of the art (Apr 2018)

The European Commission published a report on European industrial automation and control systems (IACS) Cybersecurity Certification Framework (ICCF): Lessons from the 2017 study of the state of the art (Apr 2018). See the introduction paper to the ICCF here.

"Abstract: The principal goal of this report is to present the experiments of the industrial automation and control systems (IACS) component Cybersecurity Certification Framework (ICCF) performed in 2017 by the national exercise teams (NETs) of several Member States, namely France, Poland and Spain. Based on real-life cases of use and simulations of ICCF activities, this report documents the current practices of these countries and NET members' views in relation to IACS products' cybersecurity certification. These studies have led to a series of findings that will be useful for the future of the ICCF in the context of the European Cybersecurity Certification Framework. In conclusion, a plan of action is proposed for the 2018-2019 period."

02_06. FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs (Apr 2018)

The Federal Financial Institutions Examination Council (FFIEC) members released a statement "to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs". It states that "while cyber insurance may be an effective tool for mitigating financial risk associated with cyber incidents, it is not required by the agencies. Purchasing cyber insurance does not remove the need for a sound control environment."

The statement suggests items to consider in the following areas while assessing cyber insurance benefits: 1) Involving multiple stakeholders in the cyber insurance decision; 2) Performing proper due diligence to understand available cyber insurance coverage; and 3) Evaluating cyber insurance in the annual insurance review and budgeting process.

02_07. IIF Staff Paper on Addressing Cybersecurity Regulatory Fragmentation (Apr 2018)

This Institute of International Finance (IIF) staff paper "Addressing regulatory fragmentation to support a cyber-resilient global financial services industry" evaluates the

regulatory approaches in the cyber arena that are being introduced around the world, identifies areas where regulatory fragmentation is occurring and discusses how a consistent and coordinated global regulatory landscape could be designed to help both reduce the current fragmentation and avoids creating new sources of it.

The paper also advocates for the Financial Stability Board "to play a predominant role in creating that regulatory landscape, which should ideally be built around a principles-based and risk-based global framework that would provide a common approach for all the cyber-related areas where public and private incentives are aligned. In the cases where incentives are not fully aligned, further regulations might be needed, but in that case, they should be developed in coherence with the framework and in accordance with leading practices that avoid creating fragmentation."

02_08. NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Apr 2018)

The National Institute of Standards and Technology (NIST) released the final Version 1.1 of its "Framework for Improving Critical Infrastructure Cybersecurity" also known as the NIST Cybersecurity Framework. This often-referenced work refines, clarifies, and enhances Version 1.0, which was issued in February 2014 and incorporates two drafts revised during 2017 and 2018.

The Framework is intended to be implemented by first-time and current Framework users, with explicit objective to be compatible to Version 1.0 "with minimal or no disruption". It makes the following updates: "Clarified that terms like compliance can be confusing and mean something very different to various Framework stakeholders; A new section on self-assessment; Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes; Refinements to better account for authentication, authorization, and identity proofing; Better explanation of the relationship between Implementation Tiers and Profiles; and Consideration of Coordinated Vulnerability Disclosure."

02_09. Swiss national strategy for protection against cyber risks (Apr 2018)

In April 2018, the second national strategy for protection of Switzerland against cyber risks (NCS) was published by the Federal Council covering 2018 to 2022. "It builds on the first NCS implemented from 2012 to 2017; further develops it in line with Switzerland's vulnerabilities, the significantly changed and intensified threat situation since 2012, and the foreseeable future development thereof; and it supplements it with further measures. It thus provides the strategic framework for improving prevention, early identification, response, and resilience in all areas relevant to cyber risks."

The strategic goals of the NCS is to support cooperation between public authorities, the private sector and operators of critical infrastructure in order to ensure early identification

of cyber threats, improve the resilience of critical infrastructure and minimize cyber risks. (FSB-ST[i])

04_16. Russian National Standard GOST R 57580.2-2018 (Mar 2018)

The Russian Federal Agency on technical regulation and metrology published a National Standard on "Security of Financial (Banking) Operations. Information Protection of Financial Organisations. Conformity Assessment Methods" (Russian only)

"This Standard establishes requirements for the methodology and design of the results of the assessment of conformity of information protection (ZI) of a financial organization when choosing and implementing organizational and technical measures of ZI in accordance with the requirements of GOST R 57580.1. applied by a financial institution to implement the requirements for providing ZI. established by regulatory acts of the Bank of Russia."

02_10. Singapore Cybersecurity Act (Mar 2018)

Cyber Security Agency (CSA) of Singapore announced passing of the Government's Cybersecurity Act, which "establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore.

Its four key objectives are to:

1. Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks… The Act provides a framework for the designation of CII, and provides CII owners with clarity on their obligations to proactively protect the CII from cyber-attacks… The CII sectors are: Energy, Water, Banking and Finance**,** Healthcare, Transport (which includes Land, Maritime, and Aviation), Infocomm, Media, Security and Emergency Services, and Government.

2. Authorise CSA to prevent and respond to cybersecurity threats and incidents. The Act empowers the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents to determine their impact and prevent further harm or cybersecurity incidents from arising. The powers that may be exercised are calibrated according to the severity of the cybersecurity threat or incident and measures required for response. This assures Singaporeans that the Government can respond effectively to cybersecurity threats and keep Singapore and Singaporeans safe.

3. Establish a framework for sharing cybersecurity information. The Act also facilitates information sharing, which is critical as timely information helps the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request information, and for the protection and sharing of such information.

4. Establish a light-touch licensing framework for cybersecurity service providers. CSA adopts a light-touch approach to license only two types of service providers currently, namely penetration testing and managed security operations centre (SOC) monitoring. These two services are prioritised because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in our market and hence have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cybersecurity ecosystem…

Part 1 introduces the fundamental concepts used in the Act and provides for the application of the Act.
Part 2 provides for the administration of the Act and the appointment of a Commissioner of Cybersecurity (Commissioner) and other officers for the purposes of the Act.
Part 3 provides for the designation of CII and the regulation of owners of CII with regard to the cybersecurity of the CII.
Part 4 provides for the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore.
Part 5 provides for the licensing of providers of licensable cybersecurity services.
Part 6 contains general provisions."

03_20. BNR Rwanda Regulation No 02/2018 OF 24/01/2018 on Cybersecurity (Feb 2018)

National Bank or Rwanda published its Regulation on Cybersecurity, aimed at "establishing minimum prudent standards to banks for their protection against cybersecurity threats; and promoting the protection of customer information as well as the information technology systems of banks"

After setting some definitions, it notes "Any bank lincensed by the Central Bank must maintain its primary data on the territory of the Republic of Rwanda." It moves on to Chapter II on Regulatory Requirements, with articles on the following: Board and Senior Management Cybersecurity Responsibilities; Cybersecurity Strategy and Program; Cybersecurity Policy; Penetration Testing and Vulnerability Assessments; Audit Trail; Alternative Delivery Channels (ADC) Security Management; Risk Management; Third Party Service Provider; Limitations on Data Retention; User Training and Monitoring; Encryption of Non-public information; Incident Response and Business Continuity Management; Notices to the Central Bank; and Confidentiality.

Banks are given 18 months from Jan 2018 to comply to the physical location requirement, and maximum of six months to comply with certain basic articles (Board and Senior Management Cybersecurity Responsibilities; Cybersecurity Strategy and Program; and Cybersecurity Policy).

03_21. US SEC Guidance on Public Company Cybersecurity Disclosures (Feb 2018)

U.S. Securities and Exchange Commission's 2018 guidance focuses on cyber security policies and procedures that cover incident response, disclosure and more robust and integrated risk management programs.

"This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies. While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff's 2011 guidance. In addition, we address two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context."

02_11. BaFin specifies BAIT (Feb 2018)

The German Federal Financial Supervisory Authority (BaFin) published a more robust version of its supervisory requirements for IT in financial institutions (BAIT, released in November 2017), setting up its requirements in a 'modular' format. It explains: "The BAIT have now become the cornerstone of IT supervision for all credit and financial services institutions in Germany. The requirements are directed at the management boards of such companies.

The objective of the BAIT is to create a comprehensible and flexible framework for the management of IT resources, information risk and information security. They also aim to contribute towards increasing awareness of IT risks throughout the institutions and in relation to external service providers. Furthermore, they provide transparency about what banking supervisors expect from the institutions with regard to the management and monitoring of IT operations, including the user access management that this necessitates as well as requirements for IT project management and application development. Overall, the BAIT address those subject areas which BaFin has identified as particularly important based on its experience of IT inspections."

04_17. ITU Guide to Developing a National Cybersecurity Strategy (Jan 2018)

The UN's International Telecommunication Union (ITU) published a Guide to Developing a National Cybersecurity Strategy, developed by twelve partners from Intergovernmental and International Organizations, private sector, as well as academia and civil society[22], and "provides a framework that has been agreed on by organisations

[22] Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Deloitte, the Geneva Centre for Security Policy (GCSP), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the International Telecommunication Union (ITU), Microsoft, the NATO Cooperative Cyber Defence Centre Of

with demonstrated and diverse experience in this topic area and builds on their prior work in this space. As such, it offers the most comprehensive overview to date of what constitutes successful national cybersecurity strategies."

The guide aims to provide a useful, flexible and user-friendly framework to set the context of a country's socio-economic vision and current security posture and to assist policy-makers in the development of a Strategy that takes into consideration a country's specific situation, cultural and societal values, and that encourages the pursuit of secure, resilient, information and communications technologies (ICTs)-enhanced and connected societies.

Structured as a resource to help government stakeholders in preparing, drafting and managing their National Cybersecurity Strategy, the content is organised to follow the process and order of a Strategy development:

- Introduction: provides an overview of the subject of the Guide with related definitions;
- Strategy development lifecycle: details the steps in the development of a Strategy and its management during its full lifecycle (i.e. the process and aspects related to the development of a National Cybersecurity Strategy (such as preparation, drafting, implementation and long-term sustainability);
- Overarching principles for a Strategy: outlines the cross-cutting, fundamental considerations to be considered during the development of a Strategy;
- Focus areas and good practices: identifies the key elements and topics that should be considered during the development of a Strategy; and
- Supporting reference materials: provides further pointers to relevant literature that stakeholders can review as part of their drafting effort.

04_18. EU Euro Cyber Resilience Board - Mandate ECRB (Jan 2018)

The EU released the mandate of the newly formed Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures. "The ECRB's objective is to enhance the cyber resilience of financial market infrastructures, which are active in the EU on a cross-border basis and clear and/or settle in euro, of their critical service providers and of the wider EU financial sector by:

(a) fostering trust and collaboration among pan-European financial market infrastructures and critical service providers, on the one side, and among them and authorities on the other side; and
(b) catalysing joint initiatives aiming at (i) increasing the cyber resilience capabilities and capacities of the financial sector including joint solutions and awareness, and ii) reinforcing the operational resilience of the financial sector generally.
Through the accomplishment of its objective, the ECRB contributes to the overall stability of the

Excellence (NATO CCD COE), the Potomac Institute for Policy Studies, RAND Europe, The World Bank and the United Nations Conference on Trade and Development (UNCTAD).

EU financial system…"

The ECRB, chaired by the ECB, will have no formal powers to impose binding measures and will not make supervisory judgements. Members commit voluntarily abide by its common positions, statements and strategic views.

"ECRB is composed of the members, which are representatives of pan-European financial market infrastructures and of their critical service providers. Initial list of the [member] institutions… includes the main institutions relevant for the objective of the ECRB and is deemed to fairly represent the financial infrastructure sector…": TARGET2/Target2Securities; EBA CLEARING (EURO1, STEP2-T); STET; equensWorldline; Iberpay; RPS/EMZ; Euroclear Group; London Stock Exchange Group (Monte Titoli , LCH Clearnet); BME Group; KDPW; EuroCCP; NasdaqClearing; Deutsche Börse Group (Eurex Clearing, Clearstream); SWIFT; SIA; Mastercard; Visa.

"In addition to the members, seven national central banks (NCBs) and the ECB, being the Eurosystem lead overseers of the [member] institutions…, take part in the meetings as active participants, but without taking a position when a final conclusion or consensus is adopted or reached. Additionally three ESCB NCBs take part as active participants on a rotational basis. Furthermore, the European Commission, the European Union Agency for Network & Information Security, the European Banking Authority, the Single Supervisory Mechanism, the European Securities & Markets Authority, Europol, and the ECB Information System function are invited to join the ECRB as observers."

02_12. EBA Final Report – Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (Jan 2018)

European Banking Authority (EBA)'s Final Report of the Guidelines, published first in May 2017, went into application from 1January 2018. Authorities indicated compliance by 13 November 2017 (compliance table).

"These Guidelines set out the requirements competent authorities should apply in their assessment of ICT focusing on the general provisions and application of scoring as part of the SREP assessment of risks to capital (Title 1), assessment of institutions' governance and strategy on ICT (Title 2); and assessment of institutions' ICT risk exposures and controls (Title 3).

In particular, Title 1 of these Guidelines explains how the assessment of ICT risk contributes to the overall SREP assessment of an institution, noting that the assessment of ICT risk would contribute (1) to the assessment of operational risk, which is assessed as part of the assessment of risks to capital (Title 6 of the EBA SREP Guidelines), (2) the assessment of institutions' governance and strategy on ICT would feed into the assessment of internal governance and institution-wide controls under Title 5 of the EBA SREP Guidelines, and (3) the assessment of all aspects of ICT covered by these Guidelines would also inform the business model analysis performed in accordance with Title 4 of the EBA SREP Guidelines…"

01_01. ECB (SSM) Cyber Incident Reporting Framework (2017)

The European Central Bank (ECB) is finalizing a reporting framework for significant cyber incidents which was piloted in 2016, with plans to be rolled out to all significant institutions from the 19 euro area countries in the third quarter of 2017. "The reporting framework for significant cyber incidents is designed to collect and store information on cybercrime incidents that have an impact on significant institutions. This will require incidents to be reported as soon as the banks detect them. The information will be used to identify and monitor trends in cyber incidents affecting significant institutions and will facilitate a fast reaction by the ECB in the event that a major incident affects one or more significant banks…" A pilot exercise has resulted in improvements to the framework including incident definitions, the reporting template, and the reporting instructions.

05_18. EBA Guidelines on the security measures for operational and security risks of payment services under PSD2 (Dec 2017)

EBA, in close cooperation with the European Central Bank (ECB), developed the Guidelines (GL) on the security measures for operational and security risks of payment services, under Directive (EU) 2015/2366 (PSD2), which entered into force in the EU on 12 January 2016 applied as of 13 January 2018.

More specifically, PSD2 provides that payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide.

"These resultant Guidelines set out the requirements that PSPs should implement in order to mitigate operational and security risks derived from the provision of payment services. GL 1 defines a general principle on proportionality. This is then followed by GL 2 to GL 9, which cover governance, including the operational and security risk management framework, the risk management and control models, and outsourcing; risk assessment, including the identification and classification of functions, processes and assets; and the protection of the integrity and confidentiality of data and systems, physical security and access control. Furthermore, the Guidelines cover the monitoring, detection and reporting of operational or security incidents; business continuity management, scenario-based continuity plans including their testing and crisis communication; the testing of security measures; situational awareness and continuous learning; and the management of the relationship with payment service users (PSUs)."

The Guidelines accounted for "existing EBA Guidelines on the Security of Internet Payments under PSD1 (EBA/GL/2014/12), and has also used as a basis existing standards and frameworks in other areas related to operational and security risks and has adapted them where appropriate to the specificities of payment services. The EBA and the ECB have also carried out a risk analysis to determine the main threats and vulnerabilities to which PSPs are exposed…" and carried out a public consultation on a Draft.

Competent authorities must notify the EBA on compliance. A compliance table was updated January 2020.

(These Guidelines (EBA-GL-2017-17) are to be repealed as of June 30, 2020, upon application of EBA/GL/2019/04.)

03_22. EBA Recommendations on outsourcing to cloud service providers (Dec 2017)

The European Banking Authority (EBA) published its Final Report on Recommendations on outsourcing to cloud service providers. In this document, the EBA provides additional guidance for the specific context of institutions that outsource to cloud service providers, while the Committee of European Banking Supervisors guidelines on outsourcing (in place since 2006) remain applicable to general outsourcing by credit institutions and investment firms as defined in the Capital Requirements Regulation – CRR.

The EBA states "the aims of these recommendations are to: (a) provide the necessary clarity for institutions should they wish to adopt and reap the benefits of cloud computing while ensuring that risks are appropriately identified and managed; (b) foster supervisory convergence regarding the expectations and processes applicable in relation to the cloud."

The recommendations applied from July 2018 and a Compliance table of competent authorities was also published.

03_23. ENISA Recommendations on European Data Protection Certification (Nov 2017)

The European Union Agency For Network and Information Security (ENISA) published its Recommendations on European Data Protection Certification in preparation for the General Data Protection Regulation (EU) 679/2016 (GDPR) becoming the main data protection legal framework in the EU directly applicable in all Member States, repealing the Data Protection Directive 95/46/EC from 25 May 2018.

"The objective of this report is to identify and analyse challenges and opportunities of data protection certification mechanisms, including seals and marks, as introduced by the GDPR, focusing also on existing initiatives and voluntary schemes. More specifically the report aims at:

- Elaborating on the main aspects of certification, seals and marks in personal data protection.
- Identifying existing certifications in the greater area of privacy and/or data protection.

- Identifying the main challenges and opportunities, both at organizational and technological level, of data protection certification regime under GDPR with a look towards a common EU data protection certification framework.
- Making proposals for future steps, both at technological and organisational level, towards data protection certification that would be a contributor to greater compliance with data protection rules in the EU."

02_13. BaFin Banking Supervisory requirement for IT of banks (Nov 2017)

The German Federal Financial Supervisory Authority (BaFin) published circular 10/2017, laying out a principles-based guidance for banking institutions, Bankaufsichtliche Anforderungen an die Its (BAIT). The Circular is based on the German Banking Act and the Minimum Requirement for Risk Management, which deals with banks' operational risk.

"This Circular provides a flexible and practical framework for institutions' technical and organisational resources on the basis of section 25a (1) of the German Banking Act (Kreditwesengesetz) – in particular for IT resource management and IT risk management. Moreover, it specifies the requirements laid down in section 25b of the Banking Act (outsourcing of activities and processes)… This is without prejudice to the requirements contained in the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – MaRisk), which are fleshed out in this Circular."

02_14. DNB TIBER-NL Guidance 2.0 (Nov 2017)

De Nederlandsche Bank (the Dutch Central Bank/DNB) published its guidance on how to conduct a Threat Intelligence-based Ethical Red teaming: the TIBER-NL test. The DNB was charged by the Dutch Financial Stability Committee to lead the implementation of the TIBER-NL framework, a joint effort of all Dutch Financial Core Infrastructure (FCI) institutions, which officially started on 30 June 2016.

"TIBER tests mimic potential attacks from real threat actors. The test mimics high level threat groups only (organised crime groups / state proxy/ nation state attackers) and thereby tests whether defensive measures taken are effective (capability assessment), supplementing the present periodic information security audits (process assessments) by e.g. supervisors and overseers. The tests also supplement current penetration tests and vulnerability scans executed within FCI parties. Test scenarios will draw on current commercially obtained threat intelligence that will where possible be enriched and reviewed with Governmental Intelligence (GI). This testing method aims to determine, and importantly serves to improve the capabilities of targeted institutions. The TIBER-NL framework is intended to improve their cyber resilience and ultimately, the cyber resilience of the FCI as a whole. TIBER-NL testing will be a recurrent exercise.

A TIBER test can therefore be defined as: the highest possible level of intelligence-based red teaming exercise using the same Tactics, Techniques and Procedures (TTPs) as real adversaries, against live critical production infrastructure, without the foreknowledge of the organisation's defending Blue Team (BT). As such, the BT is unaware of the TIBER-NL test. The actual test consists of time boxed phases (recon, in, through, out). As a consequence, existing controls, prevention measures, and security detection and response capabilities against advanced attacks can be tested throughout all phases of the attack. It also helps identify weaknesses, errors or other security issues in a controlled manner.

The test phase is followed by full disclosure and a replay (that may include purple teaming) between the Red Team and the Blue Team to identify gaps, address findings and improve the response capability. During the test a White Team consisting of only the smallest necessary number of the FI's security and business experts will monitor the test and intervene when needed, e.g. when the test seems to lead to critical impact (during a test, business impact is allowed to a level agreed on beforehand, critical impact is not). The White Team will be in close contact with the TIBER-NL Test Manager from DNB's TIBER-NL Cyber Sector Team (TCST), who convoys the TIBER-NL test process.

This guide has been developed by the TCST from the Dutch Central Bank in close cooperation with all institutions from the Dutch FCI. It is meant to serve these TIBER-NL participants and their cyber security service providers. It explains the key phases, activities, deliverables and interactions involved in a TIBER-NL test."

02_15. SFC Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Oct 2017)

The Hong Kong Securities and Futures Commission (SFC), after a period of consultation, published a Guideline for Licensed Companies setting out the baseline requirements to reduce or mitigate hacking risks associated with internet trading.

The guideline is organized in three parts:

- Protection of clients' internet trading accounts (two-factor authentication; implementing a surveillance system; prompt notification to customers; data encryption; stringent password and session time-out policies);
- Infrastructure security management (network segmentation; user access management; remote access security; patch management; end-point protection; prevention of unauthorized installations; physical security; system and data backups; contingency planning for cybersecurity scenarios; and third party service providers); and
- Cybersecurity management and supervision (Roles and responsibilities of cybersecurity management; incident reporting; training for internal users; and alert and reminder to clients).

Compliance with the Guidelines is required from 27 July 2018 (except for two-factor authentication, to be effective in April 2018). (FSB-ST[i])

02_16. FSB Stocktake and Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices (Oct 2017)

The Financial Stability Board (FSB), as tasked by the G20 meeting in Baden-Baden (March 2017), published the results of a Stocktake and Summary Report on cybersecurity regulations, guidance and supervisory practices (publicly issued) at the meeting of the G20 Finance Ministers and Central Bank Governors in Washington DC.

"The reports are informed by the responses of [all 25] FSB member jurisdictions and [nine] international bodies to a survey conducted by the FSB. The summary report also sets out key themes raised in an FSB workshop in September that brought together public and private sector participants to discuss cybersecurity in the financial sector.

FSB member jurisdictions have been active in addressing cybersecurity, with all member jurisdictions having released regulations or guidance that address cybersecurity for the financial sector. Findings of the FSB stocktake include:

- All FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards when developing their own regulatory or supervisory schemes for the financial sector.
- Two thirds of reported regulatory schemes take a targeted approach to cybersecurity and/or information technology risk and one-third address operational risk generally.
- Some elements commonly covered by regulatory schemes targeted to cybersecurity include risk assessment, regulatory reporting, role of the board, third-party interconnections, system access controls, incident recovery, testing and training.
- Jurisdictions remain active in further developing their regulation and guidance. Seventy-two per cent of jurisdictions report plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year.
- International bodies also have been active in addressing cybersecurity for the financial sector. There are a number of similarities across the international guidance issued by different sectoral standard-setting bodies and other international organisations. Many of the same topics are addressed, including governance, risk analysis and assessment, information security, expertise and training, incident response and recovery, communications and information sharing, and oversight of interconnections.

Private sector participants at the workshop emphasised that effective cybersecurity requires a strategic, forward-looking, fluid and proactive approach and noted the importance of integrating security with business operations, as well as the importance of governance and communication with a firm's board. They expressed support for

principles-based, risk-based and proportional regulation, and also stressed the importance of a globally consistent approach that avoids multiple, potentially conflicting regulatory schemes."

*The FSB Stocktake document includes summaries of the FSB Cybersecurity Survey responses, providing a concise reference for these 25 jurisdictions. This valuable resource has enriched the current update of the Digest in its mirrored effort to collect cybersecurity regulation and guidance for the financial sector. The documents owing their coverage in the Digest to the FSB Cybersecurity Survey will be cited with the notation "*FSB-ST*".*

02_17. G-7 Follow-up guidance on Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (Oct 2017)

Building upon prior year's guidance of the same title, the finance ministers and central bank governors of the G-7 countries (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) released a follow-up guidance.

Described as "nonbinding, high-level building blocks that provide the foundation for private and public entities, as they develop their approach to cybersecurity, supported by their risk management and culture", the document specifically provides:

A) Five "desirable outcomes" based on the G7 Fundamental Elements, "encouraging entities to continue developing their cybersecurity, and providing further characteristics to assess the effectiveness of cybersecurity capabilities (the 'what')". They are:
   1. The Fundamental Elements (G7FE) are in place.
   2. Cybersecurity influences organizational decision-making.
   3. There is an understanding that disruption will occur.
   4. An adaptive cybersecurity approach is adopted.
   5. There is a culture that drives secure behaviors.

B) Five "assessment components" which assessors can use to develop their approach to assessing progress as entities build and enhance their cybersecurity. "Together, they help the assessment by describing the effectiveness of cybersecurity assessments (the 'how')." They are:
   1. Establish clear assessment objectives.
   2. Set and communicate methodology and expectations.
   3. Maintain a diverse toolkit and process for tool selection.
   4. Report clear findings and concrete remedial actions.
   5. Ensure assessments are reliable and fair.

04_19. G7 ICT and Industry Ministers' Declaration: Making the Next Production Revolution Inclusive, Open and Secure (Sep 2017)

G7 Ministers of ICT and Industry published a declaration resulting from their meeting in Torino, aimed at "further[ing] dialogue and cooperation, building on the outcomes of the 2016 G7 ICT Ministers' Meeting held in Japan, the 2016 G20 Leaders' Summit and Science Technology and Innovation (STI) Ministers meeting held in China and the 2017 G20 meeting of the Ministers responsible for the digital economy held in Germany."

Furthermore, we are responding to the G7 Leaders who met in Taormina in May 2017, who in their Declaration and annex "G7 People-Centred Action Plan on Innovation, Skills and Labor" called upon the G7 ICT and Industry Ministers to further elaborate on the Innovation in Production pillar, using as a starting point the set of three Key Policy Priorities of Inclusiveness, Openness and Security as well as on Key Policy Priority 7 on NPR-enabling quality infrastructures. [NPR: Next Production Revolution]…

The Declaration has three Annexes:

- Annex 1: G7 Common Policy Approaches for SMEs' Competitiveness and Inclusiveness in the NPR;
- Annex 2: G7 Multistakeholder Exchange on Human Centric AI for Our Societies
- Annex 3: G7 Actions for Enhancing Cybersecurity for Businesses, which lays out their intentions and actions on Objective 1: Developing and implementing appropriate cyber security risk management practices and Objective 2: Enhancing Cooperation.

02_18. EC Legislative proposal on a Framework for Free Flow of Non-Personal Data in the EU (Sep 2017)

Pursuing the objectives set out in the European Commission's Digital Single Market Strategy, "the proposal aims to address the following issues:

- Improving the mobility of non-personal data across borders in the single market, which is limited today in many Member States by localisation restrictions or legal uncertainty in the market;
- Ensuring that the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, remain unaffected; and
- Making it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market."

"This proposal focuses on provision of data hosting (storage) and other processing services, and is coherent with existing legal instruments. The initiative pursues the creation of an effective EU single market for such services. It is thus consistent with the E-commerce Directive which aims at a comprehensive and effective EU single market for

the broader categories of information society services, and with the Services Directive which furthers the deepening of the EU single market for services in a number of sectors…"

02_19. EC Legislative proposal on ENISA and cybersecurity certification framework (Sep 2017)

The European Commission published a Proposal for "Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")".

As summarized in the "Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", the proposal includes a permanent mandate of the European Union Agency for Network and Information Security (ENISA, whose current mandate is set to expire in June 2020) to be designated the "EU Cybersecurity Agency", giving it a stronger and more central role.

The proposal delineates scope of mandate for ENISA in the following areas: EU policy development and implementation; capacity building (including contributing to the establishment of Information Sharing and Analysis Centres (ISACS) in various sectors); knowledge and information, awareness raising; research and innovation; operational cooperation and crisis management (including pan-European cybersecurity exercises (Cyber Europe) to be run on an annual basis); the EU cybersecurity "Blueprint"; and Market related tasks (standardisation, cybersecurity certification).

The Communication summarizes the "Blueprint" as a document which is "to provide an effective process for an operational response at Union and Member State level to a large-scale cyber incident. The Blueprint presented in a Recommendation in this package explains how cybersecurity is mainstreamed to existing Crisis Management mechanisms at EU level and sets out the objectives and modes of cooperation between the Member States as well as between Member States and relevant EU Institutions, services, agencies and bodies when responding to large scale cybersecurity incidents and crises. The Recommendation also requests Member States and EU institutions to establish an EU Cybersecurity Crisis Response Framework to operationalise the Blueprint. The Blueprint will be regularly tested in cyber and other crisis management exercises and updated as necessary."

The proposal includes a creation of a **EU certification framework** for ICT security products: "The Framework would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering products, services and/or systems, which adapt the level of assurance to the use involved (be it critical infrastructures or consumer devices). It would bring clear benefits to businesses by avoiding the need to go through several certification processes when trading across borders, thereby limiting administrative and financial costs. The use of schemes developed under this Framework would also help build consumers' confidence, with a certificate of conformity to inform and reassure purchasers and users about the security properties of the products and services they buy and

use. This would make high standards for cybersecurity a source of competitive advantage. The result would build increased resilience as ICT products and services would be formally evaluated against a defined set of cybersecurity standards, which could be developed in close connection with the broader ongoing work on ICT standards.

The Framework's schemes would be voluntary and would not create any immediate regulatory obligations on vendors or service providers. The schemes would not contradict any applicable legal requirements, such as the EU legislation on data protection."

An EC website for the proposal includes the relevant documents including the proposal, an annex, and related impact assessments.

01_02. AU - Banking Executive Accountability & Related Measures Bill (Sep 2017)

Australian Treasury released a Banking Executive Accountability and Related Measures amendment bill for consultation. The Banking Executive Accountability Regime (BEAR) was introduced earlier in the 2017-18 Budget announcement of the Treasury.

"This Bill amends the Banking Act 1959 to establish the Banking Executive Accountability Regime (BEAR). The BEAR is a strengthened responsibility and accountability framework for the most senior and influential directors and executives in authorized deposit-taking institutions (ADI) groups. It requires them to conduct themselves with honesty and integrity and to ensure the business activities for which they are responsible are carried out effectively." The BEAR provisions are due to apply from 1 July 2018. Consultation period ended September 29.

05_19. NIST Cybersecurity Practice Guide, Access Rights Management for the Financial Services Sector, SP 1800-9. Draft (Aug 2017)

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), recently released a draft of the NIST Cybersecurity Practice Guide, Access Rights Management (ARM) for the Financial Services Sector, SP 1800-9.

"The NCCoE has developed an example implementation that demonstrates ways in which a financial services company can improve their information system security by limiting employee access to only the information they need to do their job, at the time they need it, and nothing more…

In collaboration with experts from the financial services sector and technology collaborators that provided the requisite equipment and services, we developed representative use-case scenarios to describe user access security challenges based on normal day-to-day business operations. The use cases include user access changes (e.g., promotion or transfer between departments), new user onboarding, and employees leaving an institution."

(The NCCoE is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing

cybersecurity issues. The NIST Special Publication 1800 series target specific cybersecurity challenges in the public and private sectors, maps capabilities to the NIST Cyber Security Framework, and details the steps needed for another entity to recreate the example solution. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity.)

(The public comment period was open for 60 days and closed on October 31, 2017. The project team is now reviewing comments and will incorporate feedback into the final practice guide. - no final version yet available at time of Digest 5th edition publication.)

04_20. Russian National Standard GOST R 57580.1-2017 (Aug 2017)

"The GOST R 57580.1-2017 'Financial (Bank) Transaction Security. Data Protection in Financial Organisations. Core Arrangements and Controls' national standard of the Russian Federation has been approved. The Bank of Russia website published a copy of Rosstandart Order No. 822-st, dated 8 August 2017. (Russian only) The standard will become effective from 1 January 2018.

The document covers requirements for all core data protection processes, including protection against malicious codes, data leaks and compromised IT infrastructure integrity. Special focus is given to requirements for data protection during remote access from mobile devices.

The standard provides for a comprehensive approach to planning, implementation, control and development of the data protection process in financial organisations. The document also contains requirements for data protection at all lifecycle stages of automated systems and applications used by companies and banks. The new standards will allow financial organisations to enhance protection against cyber-crimes and ensure stable and uninterrupted customer service."

04_21. WB Combatting Cybercrime: Tools and Capacity Building for Emerging Economies (Aug 2017)

"This Toolkit, Combating Cybercrime: Tools and Capacity Building for Emerging Economies, aims at building capacity to combat cybercrime among policy-makers, legislators, public prosecutors and investigators, as well as among individuals and in civil society at large in developing countries by providing a synthesis of good practices in the policy, legal and criminal-justice aspects of the enabling environment necessary to combat cybercrime. Included in this Toolkit is an Assessment Tool that enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities (discussed in more detail in chapter 7, and included in appendix 9 E). The Toolkit is also accompanied by a Virtual Library, with materials provided by participating organizations and others…

- Introductory chapter - examines the current landscape of cybercrime and some of the challenges are to combatting cybercrime.
- Chapter 2 - looks at some foundational issues including what is meant by and what constitutes cybercrime, and then looks at procedural, evidentiary, jurisdictional and institutional issues.
- Chapter 3 – considers formal and informal measures of international cooperation.
- Chapter 4 - explores national legal frameworks.
- Chapter 5 - examines in detail at due process, data protection and freedom of expression safeguards.
- Chapter 6 – looks at different aspects of capacity-building.
- Chapter 7 - explores various assessment tools, including the Assessment Tool.
- Chapter 8 - concluding observations.
- Appendices regarding cybercrime cases, multilateral instruments, national legal frameworks and the various assessment tools.

03_24. CBK Guidance Note on Cybersecurity (Aug 2017)

Central Bank of Kenya published a Guidance Note on Cybersecurity for all institutions licensed under Kenya's Banking Act, and "sets the minimum standards that institutions should adopt to develop effective cybersecurity governance and risk management frameworks" to be "documented and made available for review by external auditors and CBK. Specific Requirements consist of areas of Governance; Regular Independent Assessment and Test to be done at least once a year; Outsourcing; and Training/Awareness.

Reporting requirements consisted of the following: 1) All institutions to submit their Cybersecurity Policy, strategies and frameworks to the Central Bank of Kenya by November 30, 2017; 2) Reporting to CBK within 24 hours of any Cybersecurity incidents…; and 3) a quarterly reporting to CBK regarding occurrence and handling of Cybersecurity incidents.

01_03. US NIST Cybersecurity Workforce Framework (Aug 2017)

The US National Institute of Standards and Technology (NIST)'s National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework aims to provide organizations with a common vocabulary when describing the role, area of specialty, category of work, and the knowledge, skills, and abilities (KSA) of cybersecurity professionals.

01_04. US SEC Cybersecurity Examination Initiative Risk Alert (Aug 2017)

The US Securities and Exchange Commission (SEC)'s Office of Compliance Inspections and Examinations (OCIE) published its Risk Alert on its findings from Cybersecurity Examinations (Cybersecurity 2 Initiative), as part of its Cybersecurity Examination

Initiative announced in 2014 after its Cybersecurity Roundtable. This second round covered examinations conducted between September 2015 and June 2016 of 75 regulated entities (registered broker-dealers, investment advisers, and investment companies).

The newly published Risk Alert reported mixed progress of the regulated entities. It noted: The examinations focused on the firms' written policies and procedures regarding cybersecurity, including validating and testing that such policies and procedures were implemented and followed. In addition, the staff sought to better understand how firms managed their cybersecurity preparedness by focusing on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

The Risk Alert announcing the OCIE Cybersecurity Initiative noted that the initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

01_05. FSI Insights: Regulatory approaches to enhance banks' cyber-security frameworks (Aug 2017)

In this FSI Insights on policy implementation No 2, after a discussion on the question of "developing specific regulations for cyber-risk", the authors introduce "existing key regulatory requirements relating to cyber-risk" and "supervisory frameworks and tools", to then make their "observations about the implementation of cyber-risk regulations by the banking industry", and finally closing with "some policy considerations".

01_06. IMF WP- Cyber Risk, Market Failures, and Financial Stability (Aug 2017)

The IMF published Working Paper - Cyber Risk, Market Failures, and Financial Stability:

"This paper considers the properties of cyber risk, discusses why the private market can fail to provide the socially optimal level of cybersecurity, and explore how systemic cyber risk interacts with other financial stability risks. Furthermore, this study examines the current regulatory frameworks and supervisory approaches, and identifies information asymmetries and other inefficiencies that hamper the detection and management of systemic cyber risk. The paper concludes discussing policy measures that can increase the resilience of the financial system to systemic cyber risk."

04_22. CSA Security Guidance for Critical Areas of Focus in Cloud Computing (Jul 2017)

The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 ("Guidance v4.0") is licensed by the Cloud Security Alliance (CSA), an "organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment..." It "provide[s] a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem" and "operates the most popular cloud security provider certification program…"

"Cloud Security Alliance promotes implementing best practices for providing security assurance within the domain of cloud computing and has delivered a practical, actionable roadmap for organizations seeking to adopt the cloud paradigm… This version incorporates advances in cloud, security, and supporting technologies; reflects on real-world cloud security practices; integrates the latest Cloud Security Alliance research projects; and offers guidance for related technologies…"

It is organized into 14 'domains' in detail: 1) Cloud Computing Concepts and Architectures; 2) Governance and Enterprise Risk Management; 3) Legal Issues, Contracts and Electronic Discovery; 4) Compliance and Audit Management; 5) Information Governance; 6) Management Plane and Business Continuity; 7) Infrastructure Security; 8) Virtualization and Containers; 9) Incident Response; 10) Application Security; 11) Data Security and Encryption; 12) Identity, Entitlement, and Access Management; 13) Security as a Service; and 14) Related Technologies.

01_07. SWIFT Customer Security Program (Jul/ May /April 2017)

As part of its roll out of the SWIFT Customer Security Programme (CSP) requirement announced in September 2016, SWIFT launched the KYC Registry Security Attestation Application (KYC-SA) – "a central application for users to self-attest their level of compliance with SWIFT's Customer Security Controls Framework. The KYC-SA application also enables users to securely exchange their security status information with selected counterparties, supporting cyber risk management, transparency and business due diligence."

In April and May, SWIFT issued its new mandatory Customer Security Controls Framework and published further details of the related attestation policy and process as announced in September 2016 in the SWIFT Customer Security Controls Policy document.

SWIFT's *Customer Security Controls Framework* is presented via three objectives (*Secure your Environment*, *Know and Limit Access*, and *Detect and Respond*), eight principles within those objectives, and 27 (16 mandatory and 11 advisory) controls organized under those principles. These controls are intended to help customers to safeguard their local environments and reinforce the security of the global financial community.

Customers will be required to provide an annual self-attestation against the mandatory controls from Q2 2017, by December 31, 2017. From January 2018, SWIFT will flag those users that have not submitted a self-attestation on time to their regulators. As from January 2019 onwards, SWIFT's reporting right will also cover users that have failed to self-attest full compliance with all mandatory security controls in a timely manner or that connect through a non-compliant service provider. Thereafter, SWIFT will provide ongoing updates to local supervisory bodies.

Also in May, it launched the *SWIFT Information Sharing and Analysis Centre*, SWIFT ISAC, global portal, a key part of its Customer Security Program to facilitate information sharing among its community. "...existing intelligence bulletins will now be stored in the SWIFT ISAC portal, in a readily readable and searchable format, aligned with standardised templates... This information includes malware details such as file hashes and YARA rules, Indicators of Compromise, as well as details on the Modus Operandi used by the cyber-criminals. The information, which is particularly relevant to SWIFT customers, can also be downloaded as PDF reports or as machine-readable files in OpenIOC format, an XML-based file format that is commonly used by the cyber-security industry."

There had been multiple incidents involving fraudulent transfers through the SWIFT messaging system, although incidents stemmed from breaches within locally managed infrastructure at the customer level and not that of SWIFT's own network or software.

Documents are available through customer login at www.swift.com.

01_08. UK FCA Consultation - Individual Accountability Regime (Jul 2017)

The UK Financial Conduct Authority (FCA) commenced a consultation period for CP17/25: Individual accountability - extending the Senior Managers and Certification Regime to all FCA firms. Consultation period will close in November 2017, and a Policy Statement is expected by Summer of 2018.

"The Senior Managers and Certification Regime (SM&CR) currently applies to deposit takers and, following the Bank of England and Financial Services Act 2016, is now being extended to FCA solo-regulated firms. It replaces the current Approved Persons Regime, changing how individuals working in financial services are regulated... This consultation paper sets out our proposed approach to the extension of the SM&CR as well as some minor proposals relating to the existing banking regime."

02_20. ENISA Cyber Europe 2016: After Action Report (Jun 2017)

European Union Agency for Network and Information Security (ENISA) published "Cyber Europe 2016: After Action Report – Findings from a cyber crisis exercise in Europe". Cyber Europe 2016 was the fourth pan-European cyber crisis exercise organised by ENISA. Over 1,000 participants working mostly in the ICT sector, from public and private organisations from all 28 Member States of the European Union and two from the European Free Trade Association (EFTA), joined in a programme of activities ranging

from training sessions and communication checks to technical competitions and cooperation exercises.

Cyber Europe was launched in 2010 by ENISA, as a bi-annual exercise. The 5th iteration "CE2018" will be focused on a scenario revolving around the Aviation industry. The 4th in 2016 revolved around IT, telecommunications and cybersecurity industries, while the prior exercises were not industry specific.

01_09. Singapore Association of Banks' Guidelines on control objectives and procedures for outsourced service providers (Jun 2017)

The Association of Banks in Singapore (ABS) published the version 1.1 of its "Guidelines on control objectives and procedures for outsourced service providers" based on the MAS Guidelines on Outsourcing (issued on 27 July 2016) and industry feedback. In July 2015, it had first issued the earlier version 1.0 of the Issuance of initial Guidelines on control objectives and procedures for outsourced service providers"

"…the Association of Banks in Singapore ("ABS") has established these Guidelines on Control Objectives and Procedures for the FIs' Outsourced Service Providers ("OSPs") operating in Singapore. These Guidelines form the minimum/baseline controls that OSPs which wish to service the FIs should have in place. However, FIs with specific needs should continue to liaise with their OSPs on a bilateral basis to impose any additional specific requirements...

By complying with the Guidelines, OSPs can assure the FIs that their controls are designed and operating effectively to meet the control objectives that are relevant in the provision of the outsourced services.

SCOPE: These Guidelines should be adopted by all OSPs in Singapore that undertake material outsourcing arrangements for FIs in Singapore."

01_10. People Republic of China Cyber-Security Law (Jun 2017)

The Cyber-security Law (unofficial English version) of the People's Republic of China (PRC) took effect on 1 June 2017 (published November 2016 (Official Chinese version)). The law applies to everyone who operates networks in the PRC and will affect multinational corporations. The Cyberspace Administration of China (CAC) has issued a series of regulations implementing the law. The public has been asked for comments on other proposed implementing rules, including measures affecting the transfer of personal data outside the PRC.

The Cybersecurity Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization. "The Cybersecurity Law

applies with respect to the to the construction, operation, maintenance and usage of networks and the supervision and management thereof. It provides, among other things, that the State formulates cybersecurity strategy and policy; adopts measures to monitor, defend against and deal with cybersecurity risks and attacks; actively launches international exchange and cooperation in the areas of cyberspace governance, research and development of network technologies, and attacking cybercrime."

02_21. SAMA Cyber Security Framework (May 2017)

Saudi Arabian Monetary Authority (SAMA) published a Cyber Security Framework document, applicable to all of the following institutions operating in Saudi Arabia: banks; Insurance and/or Reinsurance Companies; Financing Companies; Credit Bureaus; and The Financial Market Infrastructure.

"SAMA established a Cyber Security Framework ("the Framework") to enable Financial Institutions regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

The objective of the Framework is as follows: 1. To create a common approach for addressing cyber security within the Member Organizations. 2. To achieve an appropriate maturity level of cyber security controls within the Member Organizations. 3. To ensure cyber security risks are properly managed throughout the Member Organizations.

The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the cyber security controls at Member Organizations, and to compare these with other Member Organizations. The Framework is based on the SAMA requirements and industry cyber security standards, such as NIST, ISF, ISO, BASEL and PCI.

The Framework supersedes all previous issued SAMA circulars with regard to cyber security." (FSB-ST[i])

The framework is part of the initiatives of SAMA's cybersecurity strategy (unavailable).

01_11. G-7 - fundamental elements for effective cybersecurity assessment (May 2017)

The G7 Communique reflected the discussions on cyber-security at the G7 Meeting of Finance Ministers and Central Banks' Governors in Bari, Italy May 12-13, 2017.

On top of highlighting the importance of developing "common and shared practices to help timely detection of vulnerabilities in the financial system" they raised the need for current assessment approaches to be "enhanced and be complemented by practices that are tailored to bolster cyber resilience, including regular cyber exercises and simulations as well as

consideration of how to most effectively leverage penetration tests" in response to rapidly evolving nature of cyber risks.

Most importantly, the G7 Cyber Expert Group (G7 CEG) was mandated to develop a set of high level and non-binding fundamental elements for effective assessment of cybersecurity by October 2017.

They also specified the following areas for future further work:

"...task the G7 CEG to advance work on the third-party risks and the coordination with other critical sectors....
...encourage international coordination and knowledge sharing.
...explore other issues of interest related with cybersecurity as directed and prioritised by G7 Finance Ministers and Central Banks Governors.
...call on the International Organizations and governmental institutions in partnership with the private sector to enhance sharing of cybersecurity information. Definitions, collection methodologies and data sharing, when appropriate, should be coordinated and consistent across countries and sectors, so that results are comparable. Sharing national experiences and best practices among all stakeholders on optimal cybersecurity legislation or relevant regulatory initiatives would be highly beneficial."

The communique also informed that the G7 is following the development of a cyber insurance market and the ongoing work by OECD, notably its report *Supporting an Effective Cyber Insurance Market*.

01_12. EBA ICT risk guidelines (May 2017)

The EBA finalized its Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP).

The EBA launched a consultation on its draft Guidelines on the assessment of information and communication technology (ICT) risk in the context of the supervisory review and evaluation process (SREP). These draft Guidelines are addressed to competent authorities and aim at promoting common procedures and methodologies for the assessment of ICT risk.

The requirements to assess ICT risks consist of:

- ICT governance (risks at senior management level and management body level);
- ICT strategy and its alignment with an institution's business strategy; and
- ICT risk exposures and controls.

These Guidelines build on existing references to ICT risk in the EBA SREP guidelines providing the scope and methodology for the assessment of ICT risk within an institution and are structured around three main parts:

- setting the context and scope of the ensuing assessment;
- addressing what competent authorities should expect to see about management of ICT risks at senior management level and management body level, as well as the

assessment of an institution's ICT strategy and its alignment with the business strategy; and
- covering the assessment of the institution's ICT risk exposures and the effectiveness of controls.

The assessment contained in these guidelines feeds into the EBA SREP methodology more generally, therefore, they should be read along with the EBA SREP Guidelines, which continue to remain applicable as appropriate. The appendix lists and provides examples of the different type of ICT risks.

01_13. EU Report on influence of tech on future of financial sector (May 2017)

The EU Parliament's Committee on Economic and Monetary Affairs (ECON) published a Report on the influence of technology on the future of the financial sector. The report calls on the EU Commission to develop an action plan to enable new and innovative technologies to develop in the framework of the Capital Markets Union and Digital Single Market.

The report outlines key priorities such as:

- cyber-security and data protection;
- interoperability and passporting of fintech services within the EU;
- providing a level playing field for traditional companies and start-ups; and
- controlled experimentation with new technologies and fostering financial education and IT skills.

01_14. FFIEC Cybersecurity Assessment Tool (May 2017)

The US Federal Financial Institutions Examination Council (FFIEC) members published an updated Cybersecurity Assessment Tool (CAT), originally released in 2015. The CAT remains "a voluntary tool that institution management may use to determine the institution's inherent risk and cybersecurity preparedness."

The CAT document includes in its appendix a resource which helps Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework.

From its Overview: "The content of the Assessment is consistent with the principles of the FFIEC Information Technology Examination Handbook (IT Handbook) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as industry accepted cybersecurity practices. The Assessment provides institutions with a repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness."

The Assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components,

and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. While management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.

To complete the Assessment, management first assesses the institution's inherent risk profile based on five categories:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Management then evaluates the institution's Cybersecurity Maturity level for each of five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

FFIEC consists of the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

02_22. Report of India's Working Group for Setting up of a financial sector CERT (May 2017)

A working group, chaired by Indian computer emergency response team (CERT-In), set up for the formulation of a CERT in the financial sector (CERT-Fin), released a report with recommendations to India's Financial Stability & Development Council, chaired by the Minister of Finance. (FSB-ST[i])

02_23. SARB Guidance to banks on cyber resilience (May 2017)

South African Reserve Bank (SARB) issued a Guidance Note on the applicability of the CPMI-IOSCO Guidance on cyber resilience for FMIs to banks, controlling companies and branches of foreign institutions. It specified that "This office will in future, as part of its supervisory review and evaluation process, assess the adequacy of banks' policies, processes and practices related to cyber risk and cyber resilience, based on, among other things, the practices contained in the aforementioned CPMI-IOSCO guidance document... As such, banks are requested to assess the adequacy and robustness of their current

policies, processes and practices against the CPMI-IOSCO cyber resilience guidance principles." (FSB-ST[i])

04_23. G7 Foreign Ministers Declaration on Responsible States Behaviour in Cyberspace (G7 Lucca Declaration) & Joint Communiqué (Apr 2017)

The G7 Foreign Ministers (of Canada, France, Germany, Italy, Japan, the United Kingdom, the United States of America and the High Representative of the European Union) published a Joint Communique from their meeting in Lucca, Italy on 10-11 April, covering a number of major international issues that impact global peace and security.

They also adopted the Lucca Declaration on Responsible States Behaviour in Cyberspace and endorsed the G7 Statement on Non-proliferation and Disarmament.

The Lucca Declaration builds on the "The Principles and Actions on Cyber" endorsed by the G7 in Ise-Shima on 26 and 27 May 2016, in which the G7 set an ambitious course in promoting security and stability in cyberspace and the protection of human rights. It states: "We encourage all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT. Cooperative approaches would also contribute to the fight against the use of cyberspace by non-State actors for terrorist and other criminal purposes... We continue to call upon all States to be guided in their use of Information and Communications Technologies (ICTs) by the cumulative reports of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN-GGE). Reaffirming our commitment to contribute to international cooperative action and the protection against dangers resulting from the malicious use of ICTs, we support the following Declaration…"

04_24. US CERT Federal Incident Notification Guidelines (Apr 2017)

The United States Computer Emergency Readiness Team (US-CERT) published a Guidance to US Federal Government departments and agencies (D/As); state, local, tribal, and territorial government entities; Information Sharing and Analysis Organizations; and foreign, commercial, and private-sector organizations for submitting incident notifications to the National Cybersecurity and Communications Integration Center (NCCIC)/US-CERT.

When "the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised", agencies must report the incident to the NCCIC/US-CERT with the required data elements (or best estimates, to be updated as it becomes available) specified in the Guidelines and any other available information, within one hour of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department. The Guideline also states that within one hour of receiving the report, the NCCIC/US-CERT will provide the agency with: A tracking

number for the incident and A risk rating based on the NCCIC Cyber Incident Scoring System (NCISS).

These guidelines support US-CERT in executing its mission objectives and provide the following benefits:

- Greater quality of information – Alignment with incident reporting and handling guidance from NIST 800-61 Revision 2 to introduce functional, informational, and recoverability impact classifications, allowing US-CERT to better recognize significant incidents.
- Improved information sharing and situational awareness – Establishing a one-hour notification time frame for all incidents to improve US-CERT's ability to understand cybersecurity events affecting the government.
- Faster incident response times – Moving cause analysis to the closing phase of the incident handling process to expedite initial notification.

02_24. Australia's Cyber Security Strategy First Annual Update (Apr 2017)

First Annual Update for Australia's four-year Cyber Security Strategy, published in April 2016 to cover up to 2020, reports on the status of "the Government's promise of improving the security of Australia's online environment, and enabling innovation, growth and prosperity." It reports 'strong progress' against the 33 initiatives set out in 2016, and highlights the "momentum and established a platform for more direct, deeper and richer conversations between governments, business and the public." (FSB-ST[i])

02_25. ASX 100 Cyber Health Check Survey Report (Apr 2017)

The Australian Securities Exchange (ASX) 100 Cyber Health Check, a voluntary survey of the top100 listed companies in Australia (76 responded between November 2016 and January 2017), is "the first attempt to gauge how the boards of Australia's largest listed companies view and manage their exposure to cyber risk. It is an industry-led initiative that forms part of the Australian Government's Cyber Security Strategy…

The report demonstrates a high level of risk awareness at the top levels of corporate Australia and a commitment to take further action. The report also provides a framework for all Australian businesses to better evaluate their own effectiveness in addressing cyber risk and identifying opportunities to improve their cyber resilience." (FSB-ST[i])

02_26. IRDAI Guidelines on Information and Cyber Security for insurers (Apr 2017)

Insurance Regulatory and Development Authority of India (IRDAI) issued a Circular with a detailed control check list for the effective implementation of these guidelines.

With various timelines until end of March 2018, the IRDAI requires the following: 1) Appointment/ designation a suitably qualified and experienced Senior Level Officer exclusively as Chief Information Security Officer (CISO) who will be responsible for articulating and enforcing the policies to protect their information assets and formation of Information Security Committee (ISC); 2) Preparation of Gap Analysis report; 3) Formulation of Cyber Crisis Management Plan; 4) Finalization of Board approved Information and Cyber Security Policy; 5) Formulation of Information and Cyber Security assurance programme (implementation plan / guidelines) in line with Board approved Information and Cyber security policy; and 6) Completion of first comprehensive Information and Cyber Security assurance audit. (FSB-ST[i])

01_15. ESAs Report on main risks for the EU Financial System (Apr 2017)

The Joint Committee of the European Supervisory Authorities (ESAs: EBA, EIOPA, and ESMA) published its spring 2017 Report on risks and vulnerabilities in the European Union's financial system.

The report focuses on continued challenges highlighted in the August 2016 report, but also highlights increasing challenges posed by rapid advances in information and communication technologies (ICT), including cyber-risks.

The Report highlights among others the rising operational risks related to information and communication technologies that are increasingly requiring supervisory attention.

The ESAs are responding to cyber-and IT-related risks by, e.g., drafting Guidelines on ICT risk assessment for supervisors, assessing cyber-security capabilities of central counterparties (CCPs) and assessing the potential accumulation of risk at insurers deriving from newly developed cyber-security coverages.

01_16. AICPA SOC for Cybersecurity (Apr 2017)

The American Institute of Certified Public Accountants (AICPA) finalized the guidance for Systems and Organization Controls (SOC) for Cybersecurity.

"In recognition of the needs of management and boards of directors of diverse organizations, and for the benefit of the public interest, the American Institute of CPAs (AICPA) has developed a cybersecurity risk management reporting framework. Using it, organizations can communicate pertinent information regarding their cybersecurity risk-management efforts and educate stakeholders about the systems, processes and controls they have in place to detect, prevent and respond to breaches. The reporting framework also enables a CPA to examine and report on the management-prepared cybersecurity information, thereby increasing the confidence that stakeholders may place on an organization's initiatives. other words, this provides clear guidance for CPAs to provide assurance on cybersecurity."

"The AICPA determined that the entity reporting framework should be developed first.... The AICPA is in the process of revising the SOC 2 R guide for service organizations. Once that project has been completed, the AICPA will develop a new supply-chain/vendor-risk management guide to address the supply-chain level."

02_27. PRC International Strategy of Cooperation on Cyberspace (Mar 2017)

China released its first strategy on cyberspace cooperation regarding the virtual domain. The International Strategy of Cooperation on Cyberspace (unofficial English version) provides a comprehensive explanation of China's policy and position on cyber-related international affairs as well as the basic principles, strategic goals and plan of action in its external relations. It aims to guide China's participation in international exchange and cooperation in cyberspace, and encourage the international community to come together to enhance dialogue and cooperation and build a peaceful, secure, open, cooperative and orderly cyberspace and a multilateral, democratic and transparent global Internet governance system. (FSB-ST[i])

01_17. NY cyber-security requirements for financial services companies (Mar 2017)

The new Requirements on cyber-security from the New York Department of Financial Services (NY DFS) took effect on 1 March 2017.

The regulation requires banks, insurance companies, and other financial services institutions regulated by the NYDFS to establish and maintain a cyber-security program designed to protect customer information as well as the information technology systems of these regulated entities. The proposed requirements for regulated financial institutions include, among others:

- Establishment of a cyber-security program;
- Adoption of a written cyber-security policy;
- Designation of a Chief Information Security Officer responsible for implementing, overseeing and enforcing the new program and its policy;
- Annual penetration testing and bi-annual vulnerability assessments of an entity's information system;
- Maintenance of audit trails to detect and respond to Cyber-security events;
- Limitation and regular review of user access privileges;
- Encryption of Non-public information;
- Establishment of an incident response plan;
- Establishment of security policy for third party service provider.

This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's

cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

The first certification will be due in February 2018.

01_18. EU Commission Consultation on the impact of FinTech (Mar 2017)

The EU Commission (EC) launched a Consultation on technology and its impact on the European financial services sector as part of its consumer financial services action plan. The consultation is structured along four policy objectives:

- Fostering access to financial services for consumers and businesses;
- Bringing down operational costs and increasing efficiency for the industry;
- Making the single market more competitive by lowering barriers to entry; and
- Balancing greater data sharing and transparency with data security and protection needs.

The last of the four areas notes: "... important questions about personal data processing, data management policies, data standardization, data sharing, security and ability to access and supervise data from (licensed) providers of financial services should move to the forefront of the policy agenda for FinTech. Mismanagement in these important areas can cause loss of trust and disruption in the market that would require policy intervention."

The consultation aims to gather information on the impact of innovative technology on the financial sector to aid the EC in developing its policy approach and to help assess whether the regulatory and supervisory framework promotes technological innovation.

Comments were accepted until 15 June 2017.

01_19. BaFin Consultation on bank regulatory requirements for IT systems (Mar 2017)

The German Federal Financial Supervisory Authority (BaFin) published (in German language) a Draft Circular "Banking Supervision Requirements for IT" (BAIT).

The draft specifies BaFin's minimum requirements for risk management (MaRisk) with respect to the security of information technology. It highlights the IT security requirements imposed by BaFin and the Bundesbank on institutions.

Furthermore, the circular helps increase institutions' awareness of IT risks, including the risks from third-party providers.

Comments were due by 5 May 2017. (FSB-ST[i])

01_20. UK Open Banking Initiative (Mar 2017)

The UK Competition and Markets Authority (CMA) announced on-schedule release of standardised data about UK banking products, branches and ATMs by the end of March, by the nine banking institutions mandated by the CMA. The CMA will require the biggest UK retail banks, to open access to transaction data by January 13, 2018, coinciding with the EU Payment Systems Directive 2.

In early 2016, the Open Banking Working Group (OBWG) established by the UK Treasury, published a manual, the Open Banking Standard, setting out a detailed framework of how Open Banking Standard could be designed and delivered, with a time table for achieving this. The Open Banking Initiative website explains that its "delivery is split between March 2017 and January 2018, with March 2017 being focused on Open Data, making available information on ATMs, Branches, Personal Current Accounts, Business Current Accounts (for SMEs) & SME Unsecured Lending and Commercial Credit Cards. January 2018 is aligned to the upcoming European Regulation (Payment Services Directive 2), where authorized third parties can be given consent by the account holder to access their Bank accounts to extract statement information and to initiate payments, without having to use the Banks Online services. It is envisaged that this capability will then lead to far reaching innovative services being created by new entrants and technology companies."

The OBWG includes nine Banks mandated by the CMA (Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group, Santander), as well as Challenger Banks, Fintechs, Third Parties, Consumer Groups and other parties to define and develop the required Application Programmer Interfaces (APIs), security and messaging standards that underpin Open Banking.

01_21. CPMI report - DLT in payment clearing/settlement (Feb 2017)

The BIS Committee on Payments and Market Infrastructures (CPMI) published a Report on distributed ledger technology (DLT) in payment clearing and settlement. Distributed ledgers, also known as *blockchains*, are ledgers of electronic transactions maintained by a shared network of participants and not by a centralised entity.

The report provides an analytical framework for central banks and other authorities to review and analyse the use of this technology for payment, clearing, and settlement. The objective of the framework is to help understand the uses of DLT and, in doing so, identify both the opportunities and challenges associated with this technology.

The framework presents the technology's potential to provide operational efficiencies and to make financial markets more robust and resilient. Enhanced operational resilience and reliability are of particular interest to the authorities given the importance of protecting against cyberthreats. It also contains a set of questions that should be useful when looking at DLT arrangements.

It highlights that work is still needed to ensure that the legal underpinnings of DLT arrangements are sound, governance structures are robust, technology solutions meet

industry needs, and that appropriate data controls are in place and satisfy regulatory requirements.

04_25. NACD The role of directors regarding cyber-risk oversight (Jan 2017)

The National Association of Corporate Directors (NACD) released an updated edition of its "Director's Handbook on Cyber-Risk Oversight." Recognizing that board directors have a key role to play to ensure proper oversight of cyber risks for their organizations, the publication aims to improve the effectiveness of cyber oversight practices.

"NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps boards should consider as they seek to enhance their oversight of cyber risks. This handbook is organized according to these five key principles:

- PRINCIPLE 1 Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
- PRINCIPLE 2 Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- PRINCIPLE 3 Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
- PRINCIPLE 4 Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
- PRINCIPLE 5 Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

The Handbook also includes several appendices that both chief information security officers (CISOs) and directors will find useful: Questions for the Board to Ask Management About Cybersecurity; Questions Directors Can Ask to Assess the Board's "Cyber Literacy"; Assessing the Board's Cybersecurity Culture; Board-Level Cybersecurity Metrics; Sample Cyber-Risk Dashboards; and Cybersecurity Considerations During M&A Phases. The appendices also contain information about Cybersecurity Resources and the relationship between boards and CISOs.

01_22. US NIST draft updated Cybersecurity Framework (Jan 2017)

The US National Institute of Standards and Technology (NIST) issued in January 2017 a draft update to the Framework for Improving Critical Infrastructure Cybersecurity—also known as the Cybersecurity Framework. Providing new details on managing cyber-supply chain risks, clarifying key terms, and introducing measurement methods for cyber-security. The updated framework aims to further develop NIST's voluntary guidance to organizations on reducing cybersecurity risks. (See final.)

The Cyber-Security Framework was published in February 2014 following a collaborative process involving industry, academia and government agencies, as directed by a

presidential executive order. The original goal was to develop a voluntary framework to help organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid, but the framework has been widely adopted by many types of organizations across the country and around the world.

The 2017 draft, Version 1.1 incorporates feedback since the release of framework version 1.0, and integrates comments from the December 2015 Request for Information as well as comments from attendees at the Cyber-security Framework Workshop 2016.

03_25. US FSSCC Cyber Insurance Purchaser's Guide (2016)

The Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security published a Purchaser's Guide to Cyber Insurance Products, "intended to provide resources and advice to organizations—particularly small and medium-sized enterprises—that are considering the purchase of cyber insurance. It provides an overview of the cyber insurance market and identifies key questions that a prospective policyholder should ask itself, its broker or agent, and its insurer when considering the purchase of cyber insurance."

03_26. EC Introduction to the European IACS components Cybersecurity Certification Framework (ICCF) (2016)

The European Commission published a report on Introduction to the European industrial automation and control systems (IACS) components Cybersecurity Certification Framework (ICCF): Feasibility study and initial recommendations for the European Commission and professional users.

"Abstract: The principal goal of this report is to propose an initial set of common European requirements and broad guidelines that will help fostering IACS cybersecurity certification in Europe in a manner fully compatible with practices adopted beyond. It describes the IACS component Cybersecurity Certification Framework (ICCF) and its components and makes suggestions for its governance, adoption and implementation. This report is not intended to be a standard, nor aims at the establishment of new ones, as this effort's focus is to perform and publish a feasibility study that could foster the certification of IACS components in Europe."

02_28. Turkey National Cyber Security Strategy and Action Plan (2016, 2013)

Turkey published its National Cyber Security Strategy for the period 2016-2019 in 2016. Two main objectives of the strategy are to strengthen the understanding of cyber security's role as an integral part of national security for all stakeholders, and to acquire the competency that will allow taking administrative and technological precautions for maintaining the absolute security of all systems and stakeholders in national cyber space.

Targets and sub actions are determined in the strategy, while ensuring and supervising their implementation. This is an updated version of the National Cyber Security Strategy and Action Plan for 2013-14, published in 2013. The strategy for 2013-2014 defines cybersecurity risks and principles for maintenance of cybersecurity to be updated in a coordinated way at the national level, taking into account the requests from the public and private sector, and considering also the developing technology, changing conditions and needs. (FSB-ST[i])

02_29. UK National Cyber Security Strategy 2016-2021 (2016)

Building on the achievements, objectives and judgements of the first five-year National Cyber Security Strategy issued in 2011, the UK government issued a new National Cyber Security Strategy document, with the following goals:

"DEFEND: We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

DETER: The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

DEVELOP: We have an innovative, growing cyber security industry, underpinned by world leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges." (FSB-ST[i])

01_23. UK CBEST Intelligence-Led Vulnerability Testing 2.0 (2016)

The Bank of England's Sector Cyber-Team (SCT) published version 2.0 of its CBEST "framework for intelligence-led penetration testing of systemically critical organizations" for the CBEST engagement participants and service providers.

The CBEST framework was first launched in June 2014 by UK Financial Authorities, headed by the Bank of England at the recommendation of the Financial Policy Committee (FPC), which is "charged with taking action to remove or reduce systemic risks with a view to protecting and enhancing the resilience of the UK financial system."

CBEST is a voluntary cyber vulnerability assessment program made available to core firms/FMIs of the UK financial system. The assessment operates within a framework and includes a set of Key Performance Indicators (KPIs) for 1) threat intelligence and 2) intrusion detection and incident response. Each include a section used by the BoE's Sector

Cyber Team assessing "the provider's ability to deliver CBEST services in accordance with the framework agreement", as well as a section conducted by the approved provider which is an assessment of "the client firm's capability surrounding use of either cyber threat intelligence, intrusion detection, or incident response." The completed KPIs, kept by the SCT, help inform the cybersecurity assessment for the tested firm and an industry understanding of the financial sector cybersecurity capability for the regulators as well as the UK Financial Policy Committee (FPC).

CBEST tests are "built around the key potential attackers for a particular firm and the attack types they would deploy," making use of up-to-date threat intelligence direct from UK Government agencies and accredited commercial providers.

CBEST program has also brought forth new accreditation standards for threat intelligence providers and penetration testing providers, working with the Council for Registered Ethical Security Testers (CREST).

Its resource components include the following:

1. Implementation Guide, which explains the key phases, activities, deliverables and interactions involved in a CBEST assessment;

2. Services Assessment Guide, which provides background information, in the form of a set of assessment criteria, that CBEST participants can use as they assess prospective threat intelligence and penetration testing service providers approved by the Council for Registered Ethical Security Testers (CREST); and

3. Understanding Cyber Threat Intelligence Operations, which defines best practice standards for the production and consumption of threat intelligence... intended to provide the CBEST programme with a foundation for defining and executing intelligence-led cyber threat vulnerability tests in conjunction with accredited providers of threat intelligence products and services. After establishing some important terminology, this document presents an overview of the process underpinning a best practice threat intelligence capability and the organisation, roles and skills required for running it. It then discusses maturity models relating to the production and consumption of threat intelligence.

02_30. PRC National Cyberspace Security Strategy (Dec 2016)

The National Cyberspace Security Strategy (unofficial English version) of the People's Republic of China is formulated to elaborate China's major standpoints concerning cyberspace development and security, guide China's cybersecurity work and safeguard the country's interests in the sovereignty, security and development of cyberspace. The objective of the strategy is to promote peace, security, openness, cooperation and order in cyberspace.

The four principles of the strategy are:

- Respecting and protecting sovereignty in cyberspace
- Peaceful use of cyberspace
- Governing cyberspace according to the law
- Comprehensively manage cybersecurity and development

Details of nine strategic tasks are also included in the strategy. (FSB-ST[i])

01_24. UK Gov Cyber-Security Regulation and Incentives Review (Dec 2016)

In December 2016, the UK Government published the Cyber-Security Regulation and Incentives Review. During the year, as part of the Government's 1.9 billion pounds strategy to protect the UK in cyber-space, the Department for Digital, Culture, Media & Sport (DCMS) conducted a review to consider whether there is a need for additional regulation or incentives to boost cyber-risk management across the wider economy. The review was conducted in close consultation with a wide range of businesses, industry partners and stakeholders, and gathered evidence from a broad range of sources.

"The review shows that there is a strong justification for regulation to secure personal data, as there is a clear public interest in protecting citizens from crime and other harm... Government will therefore seek to improve cyber-risk management in the wider economy through its implementation of the forthcoming General Data Protection Regulation (GDPR). The breach reporting requirements and fines that can be issued under GDPR will represent a significant call to action. These will be supplemented by a number of measures to more clearly link data protection with cyber-security, including through closer working between the Information Commissioner's Office and the new National Cyber-Security Centre."

02_31. HKMA Enhanced Competency Framework on Cybersecurity (Dec 2016)

Hong Kong Monetary Authority (HKMA) and the banking industry released a Guide to Enhanced Competency Framework (ECF) on Cybersecurity for the banking sector. "This framework enables cybersecurity talent development and facilitates the building of professional competencies and capabilities of those staff engaged in cybersecurity duties." The Guide aims to provide details of the scope of application, qualification structure, recognised certificates and continuing professional development requirements to equip relevant staff with the right skills, knowledge and behaviour.... The HKMA will assess the progress of implementation of the ECF on Cybersecurity by [authorized institutions] and [their] effort in enhancing staff competence in this area during its on-going supervisory process. (FSB-ST[i])

01_25. SFC Circular on augmenting accountability of senior mgmt (Dec 2016)

The Hong Kong Securities and Futures Commission (SFC) issued a Circular on enhancing the accountability regime for senior management of licensed companies. The circular specifies definition of *senior management* and their regulatory obligations and potential legal liabilities. It specifies eight core functions of a licensed company for which it must appoint at least one fit and proper person to be the manager in charge (MIC), and provides guidance on selection of the MIC(s). It also brings in the roles and responsibilities of the Board of Directors.

01_26. HKMA circular on Cybersecurity Fortification Initiative (Dec 2016)

The Hong Kong Monetary Authority (HKMA) issued in December 2016 a Circular to authorized institutions to inform them of the implementation details of the Cybersecurity Fortification Initiative (CFI). The CFI consists of three pillars:

- Pillar 1: Cyber-Resilience Assessment Framework (C-RAF):

  The C-RAF is a tool to help authorized institutions evaluate their cyber resilience. The assessment comprises three stages:

  - Inherent Risk Assessment – This facilitates an AI to assess its level of inherent cyber-security risk and categorize it into "low", "medium" or "high" in accordance with the outcome of the assessment;

  - Maturity Assessment – This assists an AI in determining whether the actual level of its cyber-resilience is commensurate with that of its inherent risk. Where material gaps are identified, the AI is expected to formulate a plan to enhance its maturity level; and

  - Intelligence-led Cyber-Attack Simulation Testing (iCAST) – This is a test of the AI's cyber-resilience by simulating real-life cyber-attacks from adversaries, making use of relevant cyber-intelligence. AIs with an inherent risk level assessed to be "medium" or "high" are expected to conduct the iCAST within a reasonable time.

  The HKMA will adopt a phased approach to the implementation of the C-RAF as follows:

  - the first phase will cover around 30 authorized institutions including all major retail banks, selected global banks and a few smaller authorized institutions – the HKMA will inform these authorized institutions individually;

  - the expected timeline for completing the C-RAF assessment under the first phase is end-September 2017 for inherent risk assessment and maturity assessment, and end-June 2018 for iCAST (if applicable); and

- depending on industry feedback and the experience gathered from the first phase, the second phase will cover all the remaining authorized institutions. They will be expected to complete the inherent risk assessment and the maturity assessment by the end of 2018. The HKMA will consider the assessment results of the second phase in determining a timeframe for the remaining authorized institutions to complete the iCAST. Although authorized institutions covered in the second phase are given a longer timeframe for implementation, they should familiarize themselves with the C-RAF and take steps to strengthen their cyber-resilience at an early stage where necessary.

- Pillar 2: Professional Development Programme (PDP):

  The PDP, rolled out in December 2016, seeks to provide a local certification scheme and training program for cybersecurity professionals. At the request of the industry, the HKMA has adopted a list of professional qualifications, recommended by an expert panel, which are equivalent to the certification provided under the PDP. A person holding a PDP certification or an equivalent professional qualification may perform the assessments and tests in relation to the different roles defined under the C-RAF as set out in the Annex of the circular.

- Pillar 3: Cyber-Intelligence Sharing Platform (CISP):

  The HKMA noted that all banks are expected to join the Cyber Intelligence Sharing Platform. Banks were advised to start to make the necessary preparations including system changes at an early stage.

  The CISP is ready for access by banks with effect from December 2016.

01_27. G-7 Fundamental Elements of Cybersecurity for Financial Sector (Oct 2016)

The G7 published its fundamental elements of cybersecurity for the financial sector to "serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture. The elements also provide steps in a dynamic process through which the entity can systematically re-evaluate its cyber-security strategy and framework as the operational and threat environment evolves. Public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts."

The eight elements noted are:

1. *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.;

2. *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;

3. *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;

4. *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;

5. *Response*: Timely (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 service providers, and customers as appropriate); and (d) coordinate joint response activities as needed;

6. *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;

7. *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;

8. *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.

01_28. US FinCEN Advisory on FIs obligations on cyber-related events (Oct 2016)

On 25 October 2016, the US Treasury Financial Crimes Enforcement Network (Fin-CEN) issued an Advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

- Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);
- Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;
- Collaborating between BSA/Anti-Money Laundering (AML) units and inhouse cyber-security units to identify suspicious activity; and
- Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

01_29. US FBAs ANPR for enhanced cybersecurity standards (Oct 2016)

On 19 October 2016, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (the Federal Banking Agencies) issued an Advanced Notice of Proposed Rulemaking to establish enhanced cyber-security standards.

The proposed rules would apply to large institutions subject to the agencies' jurisdiction, including:

- US bank holding companies with total consolidated assets of USD 50 billion or more;
- banks with total consolidated assets of USD 50 billion or more;
- the US operations of foreign banking organizations with total US assets of USD 50 billion or more, and
- nonbank financial companies supervised by the Federal Reserve per the Dodd Frank Act. (section 165).

While the ANPR is based on some existing regulatory guidance, it also adds some new and more stringent requirements to covered entities. For example, it requires a very short two-hour timeframe to recover critical systems from cyber-events. Improvements are proposed in the following areas:

- Incident responses and cyber-resilience;
- Cyber-risk governance;
- Cyber-risk management;
- Internal and external dependency management.

Comments received are accessible here.

01_30. SFC Review of cybersecurity of online & mobile trading systems (Oct 2016)

The Hong Kong Securities and Futures Commission (SFC) launched a Review of cyber-security, compliance and resilience of brokers' internet/mobile trading systems. This initiative follows several reports from securities brokers that the security of some customers' online and mobile trading accounts has been compromised and unauthorized securities trading transactions have been conducted through these accounts.

Cybersecurity management is a priority for the SFC's supervision of licensed corporations. Licensed corporations should critically review and enhance their controls to combat cyber-attacks. This would involve:

- Strengthening threat, intelligence and vulnerability management to pro-actively identify and remediate cyber-security vulnerabilities;
- Implementing reliable preventive, detective and monitoring measures to protect sensitive information and trading systems;
- Being vigilant in monitoring unusual or questionable logins/transactions in client accounts;
- Implementing effective user authentication and access controls to deter potential hacking attempts; and
- Establishing an effective contingency plan which covers, among others, possible cyber-attack scenarios where trade and position data are impacted.

Examples of good practices observed in the market place include (i) implementing client data encryption; (ii) putting in place controls to detect internet protocol (IP) ranges used by clients and abnormal buy/sell transactions; (iii) implementing two factor authentications in conjunction with strong password requirements for client's logon; and (iv) sending timely trade confirmation to clients via SMS. A combination of these measures enables brokers spot suspicious activities and mitigate against hacking risks. Where the security of accounts is compromised, early detection enables brokers to send alert to clients to stop further unauthorized trading.

The SFC review has three components:

- surveying a mix of small to medium sized brokers to assess relevant cybersecurity features of brokers' internet and mobile trading systems;
- onsite inspections of selected brokers for an in-depth review of their information technology and other related management controls and an assessment of their design and effectiveness in preventing and detecting cyber-attacks; and
- benchmarking the SFC's regulatory requirements and market practice in Hong Kong against other major financial services regulators and other relevant market practices overseas and locally. The findings of the cyber-security review are designed to assist the SFC's policy formulation to improve overall resilience of the markets.

01_31. MY SC Guidelines to Enhance Cyber resilience of Capital Mkt (Oct 2016)

Malaysia's Securities Commission (SC) published on October 2016 new Guidelines on Management of Cyber-risk to enhance cyber-resilience of the capital market by requiring capital market entities to establish and implement effective governance measures to counter cyber-risk and protect investors.

The Guidelines, among other requirements, clearly stipulate the roles and responsibilities of the board and senior management in building cyber-resilience of a capital market entity. The entity is required to identify a responsible person to be accountable for the effective management of cyber-risk. The involvement of the board and senior management is deemed important to ensure that the capital market entity puts adequate focus on cyber-risk issues, determines risk tolerance and priorities, and allocates sufficient resources to cyber-risk.

The Guidelines require regulated entities to have in place a risk management framework to minimize cyber-threats, implement adequate measures to identify potential vulnerabilities in their operating environment and ensure timely response and recovery in the event of a cyber-breach.

Regulated entities are also required to report cyber-incidents to the SC to enhance industry's awareness on, and preparedness in dealing with, cyber-risk. The reporting is to provide a platform for SC to collaborate with market entities and stakeholders to enhance cyber-resilience on an ongoing basis.

These Guidelines are to be implemented in phases for entities based on, among others, size, nature of activities, and market share.

03_27. US CFTC System Safeguards Testing Requirements (Sep 2016)

The US Commodity Futures Trading Commission (CFTC) released Final Rule on System Safeguards Testing Requirements.

"Summary: The Commodity Futures Trading Commission (''Commission'' or ''CFTC'') is adopting final rules amending its current system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories, by enhancing and clarifying current provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing.

The final rules clarify the Commission's current system safeguards rules for all designated contract markets, swap execution facilities, and swap data repositories by specifying and defining the types of cybersecurity testing essential to fulfilling system safeguards testing obligations. These testing types are vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment.

The final rules also clarify current rule provisions respecting: The categories of risk analysis and oversight that statutorily-required programs of system safeguards-related risk analysis and oversight must address; system safeguards-related books and records

obligations; the scope of system safeguards testing; internal reporting and review of testing results; and remediation of vulnerabilities and deficiencies. In addition, the final rules adopt new provisions set forth in the Commission's Notice of Proposed Rulemaking, applicable to covered designated contract markets (as defined) and all swap data repositories, establishing minimum frequency requirements for conducting certain types of cybersecurity testing, and requiring performance of certain tests by independent contractors."

03_28. US FFIEC IT Examination Handbook: Information Security Booklet (Sep 2016)

The US Federal Financial Institutions Examination Council (FFIEC) released an Information Security Booklet as part of its Information Technology Examination Handbook (IT Handbook) series.

"This "Information Security" booklet is an integral part of the Federal Financial Institutions Examination Council (FFIEC)1 Information Technology Examination Handbook (IT Handbook) and should be read in conjunction with the other booklets in the IT Handbook. This booklet provides guidance to examiners and addresses factors necessary to assess the level of security risks to a financial institution's2 information systems.3 It also helps examiners evaluate the adequacy of the information security program's integration into overall risk management."

02_32. APRA Information Paper: 2015/16 Cyber Security Survey Results (Sep 2016)

The Australian Prudential Regulation Authority's (APRA) Information Paper informs on the results of its 2015/16 Cyber Security Survey:

"As part of its activities to understand and assess industry preparedness for, and resilience to, cyber attacks, APRA undertook a survey between October 2015 and March 2016 to gather information on cyber security incidents and their management within APRA-regulated sectors. Respondents to the survey included 37 regulated entities and four significant service providers, covering all APRA-regulated industries, with the exception of private health insurance…

The survey results, in conjunction with other supervisory information, confirm that APRA regulated entities, not only the largest of these entities, need to operate on the assumption that cyber attacks will occur and that such attacks will remain a constant challenge..." (FSB-ST[i])

02_33. CSA Staff Notice on Cyber Security (Sep 2016)

The Canadian Securities Administrators (CSA – covering FMIs, trading venues, asset managers, broker-dealers, and reporting issuers) issued a Staff Notice 11-332: Cyber

Security, updating a previous Staff Notice: "Since the 2013 Notice, the cyber security landscape has evolved considerably, as cyber attacks have become more frequent, complex and costly for organizations. Accordingly, the CSA is publishing this Notice on cyber security in order to:

- further highlight the importance of cyber risks for Market Participants;
- inform stakeholders about recent and upcoming CSA initiatives;
- reference existing standards and work published, including work published by the Investment Industry Regulatory Organization of Canada (IIROC), the Mutual Fund Dealers Association of Canada (MFDA) and international regulatory authorities and standard-setting bodies;
- communicate general expectations for Market Participants with respect to their cyber security frameworks; and
- examine ways to coordinate communication and information sharing between regulators and Market Participants." (FSB-ST[i])

01_32. IE CB Cross Industry Guidance on IT and Cybersecurity Risks (Sept 2016)

The Central Bank of Ireland issued in September 2016 a Guidance on IT and cybersecurity governance and risk management for financial services firms.

The document sets out the Central Bank's observations from supervisory work in this area and outlines guidance reflecting "the current thinking as to good practices that regulated firms should use to inform the development of effective IT and cybersecurity governance and risk management frameworks."

Boards and Senior Management of regulated firms are expected to fully recognize their responsibilities for these issues and to put them among their top priorities. The guidance lists Central Bank expectations on key issues such as alignment of IT and business strategy, outsourcing risk, change management, cyber-security, incident response, disaster recovery and business continuity.

01_33. India Non-Banking Financial Company - Account Aggregators (Sep 2016)

The Reserve Bank of India produced final Directions providing a framework for the registration and operation of "Account Aggregators" in India, requiring these operators to register and be regulated by the RBI. It defines "Account Aggregators" as non-banking financial companies that will collect and provide information on a customer's financial assets, in a consolidated, organized and retrievable manner to the customer or any other person as per the instructions of the customer. The Directions prohibit Account Aggregators from conducting any other business than that of aggregator, handling transactions for customers, for example. It clearly sets out Data Security requirements, including prohibiting request or storing of customer credentials.

01_34. ENISA Strategies for Incident Response & Cyber Crisis Coop. (Aug 2016)

This document from the European Union Agency for Network and Information Security (ENISA) is an input for the Network and Information Security (NIS) Platform for the discussion on incident response and cyber crisis coordination (by "WG2" – see below). It briefly introduces what incident response is, who the main actors are, what baseline capabilities these entities should possess in order to effectively combat cyberattacks, and what challenges there may be that impede efficiency in incident response. The notion of Computer Security Incident Response Teams (CSIRTs) as key players in incident response is introduced. Descriptions of incident response mechanisms will be elaborated, taking into account national-level cybersecurity strategies, cyber crisis coordination and management covering both escalation and communication between CSIRTs and government bodies.

As part of the implementation of the cybersecurity Strategy of the EU, the NIS Platform was created in 2013 to help European stakeholders carry out appropriate risk management, establish good cybersecurity policies and processes and further adopt standards and solutions that will improve the ability to create safer market conditions for the EU.

The expert work of the components of the NIS Platform was divided into Working Groups (WGs), all dealing with their special field of expertise in cybersecurity:

- WG1 on risk management, including information assurance, risks metrics and awareness raising;
- WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
- WG3 on secure ICT research and innovation.

Ongoing work by the WGs is a series of chapters to be adopted by the NIS Platform. The chapters foreseen by the three WGs are:

1. Organizational structures and requirements;
2. Verification and auditing of requirements;
3. Voluntary information sharing;
4. Incident response;
5. Mandatory incident notification;
6. Data protection;
7. (Optional) Incentives for the uptake of good cybersecurity practices;
8. (Optional) Recommendations on research challenges and opportunities.

01_35. MAS Guidelines on Outsourcing (Jul 2016)

The Monetary Authority of Singapore (MAS) states "[t]hese Guidelines provide guidance on sound practices on risk management of outsourcing arrangements... An institution should ensure that outsourced services (whether provided by a service provider or its sub-contractor) continue to be managed as if the services were still managed by the institution."

After describing an institution's expected engagement with MAS on outsourcing, including notification to MAS of adverse developments, the Guideline goes through the following areas of risk management practices which institutions are obliged to implement: Responsibility of the Board and Senior Management; Evaluation of Risks; Assessment of Service Providers; Outsourcing Agreement; Confidentiality and Security; Business Continuity Management; Monitoring and Control of Outsourcing Arrangements; Audit and Inspection; Outsourcing Outside Singapore; Outsourcing with a Group; and Outsourcing of Internal Audit to External Auditors.

The Guideline ends with a separate section on Cloud Computing/Service (CS), that "MAS considers CS operated by service providers as a form of outsourcing… The types of risks in CS that confront institutions are not distinct from that of other forms of outsourcing arrangements. Institutions should perform the necessary due diligence and apply sound governance and risk management practices articulated in this set of guidelines when subscribing to CS…."

Its Annexes include a list of non-exhaustive examples of outsourcing arrangements to which the guidelines apply and don't apply, a guidance in assessing the materiality of an outsourcing arrangement, and a template for a register of outsource entities of an institution to be maintained for submission to MAS, at least annually or upon request.

The Guideline's audit and inspection section specifies that "An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives." This specifically includes, not only that the outsourcing agreements should include clauses that "allow the institution to conduct audits on the service provider and its subcontractors, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its sub-contractors,", but that which also "allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution to: (i) access and inspect the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors; and (ii) access any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement."

01_36. EU Directive on Security of Network and Information Systems (Jul 2016)

This EU Directive on security of network and information systems sets out security obligations for operators of essential services, including those in the banking and financial sectors, and for digital service providers, such as online marketplaces, search engines and cloud services.

Member States will be required to designate a national authority for dealing with cyber-threats and to develop a national cyber-strategy among others.

I. General Provisions: "... describes the goals of the Directive, and its legislative environment. It also gives formal definitions to terms that appear in the text."

II. National Frameworks on the security of Network and Information Systems: "... lists the different entities and legislative frameworks that each Member State will have to set up in order to comply with the Directive. Each MS needs to adopt a national NIS strategy; designate one or more national competent authorities, as well as a single point of contact for cross-border cooperation; and set up at least one Computer Security Incident Response Team (CSIRT). These teams need to cover certain sectors and services."

III. Cooperation: "... defines two groups meant to improve NIS-related cooperation between MS. The first is the Cooperation Network, composed of representatives of MS, the Commission, and ENISA. This group is meant to focus on strategic issues. The second group is the CSIRT Network, composed of representatives of MS' CSIRT and CERT-EU, with the Commission as observer and ENISA as Secretary and active support."

IV. Security of the Network and Information Systems of Operators of Essential Services: "... defines security requirements for and duties of operators of essential services. These services are described in Annex 2 of the Directive."

V. Security of the Network and Information Systems of Digital Service Providers: "... defines security requirements for and duties of digital service providers. These providers are described in Annex 3 of the Directive"

VI. Standardization and Voluntary Notification: "...encourages the use of EU or international standards" and discusses handling of voluntary notifications.

VII. Final Provisions: "... covers all other aspects, like the details the timeline for transposition of the Directive, or penalties"

The Directive entered into force on 8 August 2016 and needs to be transposed by 9 May 2018.

02_34. IDRBT Cyber Security Checklist (Jul 2016)

Institute for Development and Research in Banking Technology (IDRBT - established by the Reserve Bank of India) published a Cyber Security Checklist.

Developed after an annual retreat of heads of public sector banks and officials of RBI, the checklist was completed by a IDRBT group with members from banks, industry and academia, to "help banks in identifying any gaps in cybersecurity systems", "help board level subcommittees on risk management and information security on monitoring the cyber defence preparedness of banks", and "likely to help banks preparing the cyber security framework as required by the RBI Circular dated 2 Jun 2016."

The Checklist is organized into sections: 1) Enterprise Control; 2) IT Infrastructure Security; 3) Endpoint Security: Hardening (Desktops; Mobiles; Tablets); 4) Security Monitoring; and 5) Outsourcing Security (Optional). (FSB-ST[i])

02_35. RBI Circular to Establish Cyber Security Framework in Banks (Jun 2016)

The Reserve Bank of India (RBI) published a Circular outlining an urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis.

In it, RBI requires "Banks should immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their board" to be confirmed in three months' time to RBI's Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision.

Further, it states that Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy of a bank.

It mandates that a SOC (Security Operations Centre) be set up at the earliest, if not done already, so it "ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats." An indicative configuration of a SOC "to monitor and manage cyber risks in real time" is given in Annex 2.

It requires that the IT architecture be reviewed by the IT Sub Committee of the Board and upgraded as necessary, and provides an indicative "minimum baseline cyber security and resilience framework to be implemented by the banks" in Annex 1.

"A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. Considering the fact that cyber-risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate and hence needs to be revisited keeping in view the nuances of the cyber-risk... CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment."

It urges banks to comprehensively address network and database security, ensure protection of customer information, review organisational arrangements with a view to security, and to develop Cyber security preparedness indicators used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.

"It is reiterated that banks need to report all unusual cybersecurity incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank. Banks are also encouraged to actively participate in the activities of their CISOs' Forum coordinated by IDRBT and promptly report the incidents to Indian Banks – Center for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

It provides a cyber-incident reporting template (Annex 3) and announces that "it has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents. Banks are required to report promptly the incidents".

Further, an immediate assessment of gaps in preparedness to be reported to RBI.

Banks are required to take suitable steps in building awareness about the potential impact of cyber-attacks among customers, employees, partners and vendors, and also to urgently bring the Board of Directors and Top Management in banks up to speed on cyber-security related aspects. (FSB-ST[i])

01_37. CPMI-IOSCO Guidance on cybersecurity (Jun 2016)

The Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) have published a Guidance on cyber-security which highlights the following points:

- Sound cyber-governance is key. Board and senior management attention is critical to a successful cyber-resilience strategy;
- The ability to resume operations quickly and safely after a successful cyberattack is paramount;
- Financial Market Infrastructures (FMI) should make use of good-quality threat intelligence and rigorous testing;
- FMIs should aim to instil a culture of cyber-risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber-resilience at every level within the organization; and
- Cyber-resilience cannot be achieved by an FMI alone; it is a collective endeavor of the whole ecosystem.

04_26. G7 Ise-Shima Summit Leaders Declaration, establishment of Ise-Shima Cyber Group (ISCG) & G7 Principles and Actions on Cyber (May 2016)

G7 Leaders released a Declaration at the Ise-Shima Summit of 25-26 May, 2016. In the area of cyber, the Declaration included the following affirmations and decisions:

> We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity... We will take decisive and robust measures in close cooperation against malicious use of cyberspace, both by states and non-state actors, including terrorists. We reaffirm that international law is applicable in cyberspace.
>
> We commit to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in

cyberspace, the promotion of voluntary norms of responsible state behavior during peacetime, and the development and the implementation of practical cyber confidence building measures between states. In this context, we welcome the report of the UN Group of Governmental Experts in 2015 and call upon all states to be guided by the assessments and recommendations of the report.

We also reaffirm that no country should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

We commit to facilitate the free flow of information to ensure openness, transparency and freedom of the Internet, and a fair and equal access to the cyberspace for all actors of digital economy while respecting privacy and data protection, as well as cyber security.

We commit to the protection and promotion of human rights online. We commit to promote a multi-stakeholder approach to Internet governance which includes full and active participation by governments, the private sector, civil society, the technical community, and international organizations, among others…

We endorse the G7 Principles and Actions on Cyber … to promote and protect an open, interoperable, reliable and secure cyberspace.

We decide to establish a new G7 working group on cyber (Ise-Shima Cyber Group (ISCG)) to enhance our policy coordination and practical cooperation to promote security and stability in cyberspace.

02_36. HKMA Circular Security controls related to Internet banking services (May 2016)

Hong Kong Monetary Authority (HKMA), making reference to reports by banks regarding security breaches in April, published a circular detailing additional ways authorised institutions providing Internet banking services should "enhance their fraud monitoring mechanisms so as to keep up with new and emerging threats and fraudulent schemes." (FSB-ST[i])

04_27. G7 ICT Ministers Charter for the Digitally Connected World & Joint Declaration and Annex (Apr 2016)

Information and Communications Technology (ICT) Ministers from the G7 countries adopted the "Charter for the Digitally Connected World" at the Meeting in Takamatsu Kagawa, Japan on 30 April 2016. The charter provides 1) Common Goals for realizing sustainable and inclusive development, 2) reaffirms their intention to cooperate on addressing the global challenges and reaffirms Fundamental Principles of i) Promoting

and Protecting Human Rights; ii) Promoting and protecting the free flow of information; iii) Supporting a multi-stakeholder approach; and iv) Strengthening digital connectivity and inclusiveness for all, and 3) lays out G7 ICT Strategy, consisting of i) Promoting access to ICT; ii) Strengthening international collaboration for promoting the free flow of information, privacy protection and cybersecurity; iii) Fostering innovation; iv) Using ICT to address global challenges and opportunities; and v) Strengthening comprehensive international cooperation and collaboration.

The ICT Ministers also released a Joint Declaration (Action Plan on implementing the Charter), which included promoting cybersecurity:

> "19. We reaffirm our support for policies that improve cybersecurity as essential for the development of a trustworthy digitally connected world. As part of our efforts to address cybersecurity risks, threats and vulnerabilities, including those to ICT and ICT-enabled critical infrastructures, we endeavor to strengthen international collaboration, capacity building and public-private partnerships. We also support risk management based approaches to cybersecurity including research on methods to analyze threats and continue to work with all stakeholders on such efforts also through constructive discussions in international fora.
>
> 20. To promote cybersecurity awareness, all stakeholders in the digitally connected world must take active responsibility. To this end, we recognize the importance of developing human capital to reduce threats to cybersecurity. That could be done through training, education and increased awareness to enable citizens, enterprises including critical infrastructure operators and governments to meet their objectives in an efficient manner."

The separate Annex called "G7 Opportunities for Collaboration" listed information on opportunities for collaboration for greater international cooperation in four areas: 1. Promoting access to ICT; 2. Promoting and protecting the free flow of information; 3. Fostering Innovation; and 4. Using ICT to address global challenges and opportunities.

Notable Cybersecurity related project initiatives included the following:

- Japan welcomes collaboration on the CyberGreen Project, which is a global collaborative initiative which aims to develop and utilize risk-based common metrics for assessing cyber risks to eliminate bots and vulnerable network servers and make the cyberspace clean and resilient to cyberattack.
- Japan welcomes collaboration on the Network Incident Analysis Center for Tactical Emergency Response (NICTER), as a method to observe and analyze threats in the cyberspace to comprehend global trends of malicious activities and to share analysis results in a real-time manner.
- Japan welcomes collaboration among Information Sharing and Analysis Centers (ISACs) and related bodies for the purpose of sharing best practices on Critical Information Infrastructure Protection.
- The U.S. welcomes collaboration to support initiatives to enhance open source security, such as the Linux Foundation's Core Infrastructure Initiative (CII) - CII is

a new initiative that performs security audits and remediates vulnerabilities in key open source software projects.

- Canada welcomes international collaboration in the domain of spam and malware intelligence. Greater information sharing between international partners and their respective spam reporting centers will lead to more timely and effective intelligence, improving our collective enforcement of spam, malware, phishing and other online threats, creating a safer and more secure cyberspace.

03_29. US FFIEC IT Examination Handbook: Retail Payment Systems Booklet (Apr 2016)

The US Federal Financial Institutions Examination Council (FFIEC) released an Retail Payment Systems Booklet as part of its Information Technology Examination Handbook (IT Handbook) series. It includes an appendix (E) on "Mobile Financial Services"

"The FFIEC IT Examination Handbook (IT Handbook), "Retail Payment Systems Booklet" (booklet), provides guidance to examiners, financial institutions, and technology service providers (TSPs) [1] on identifying and controlling risks associated with retail payment systems and related banking activities."

01_38. Report on IOSCO's Cyber Risk Coordination Efforts (Apr 2016)

International Organization of Securities Commissions (ISOSCO)'s report, covers the main regulatory issues and challenges related to cyber security for relevant segments of securities markets. For IOSCO member organizations, the report provides an overview of some of the different regulatory approaches related to cybersecurity that IOSCO members have implemented thus far, to serve as reference of potential tools available to regulators as they consider appropriate policy responses. For market participants, the report outlines various plans and measures participants have put in place to enhance cyber security in terms of identification, protection, detection, response and recovery.

The report results from a board-level coordination effort led by the Quebec AMF (Autoritédes marchés financiers) with assistance of the China Securities Regulatory Commission and the Monetary Authority of Singapore, bringing together the contribution of relevant IOSCO Policy committees and related stakeholders.

02_37. Australia's Cyber Security Strategy (Apr 2016)

Australian Cyber Security Strategy lays out initiatives under five themes for action by the Government to improve cyber security, up to the year 2020: 1) A national cyber partnership; 2) Strong cyber defenses; 3) Global responsibility and influence; 4) Growth and innovation; and 5) A cyber smart nation.

The initiatives are intended to be reviewed and updated annually, while the Strategy document itself will be updated every four years. (FSB-ST[i])

01_39. EU General Data Protection Regulation (Apr 2016)

The EU General Data Protection Regulation, GDPR, was set into place in April 2016 and will come into force in May 2018. The new EU Regulation repeals the Data Protection Directive of 1995 and replaces local laws for data protection, bringing a single standard among all EU member states.

Some important highlights of the regulation include the following issues of scope: 1) responsibility of data protection, including demonstration of compliance (accountability principle), now extends to data processor and not just the data controller (i.e. a supervisor can supervise processors directly as well); 2) scope of the law follows the data – GDPR is applicable to entities outside the EU if they are servicing EU member states; 3) includes not just direct personal data but any derived data that can be either by itself or in combination with other data be identified back to an individual.

Other important matters are:

- Data portability and "Right to be Forgotten" – individual's right to their own data and to have it be transported or deleted if certain conditions are met.
- Elevation of importance of data protection through imposing principles of "data protection by design" and "data protection by default."
- Required maintenance of a record of all processing activities
- Data breach notification to the supervisory authority within 72 hours (and to the individuals in cases of high risk) unless it can "demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons."
- Security measures, such as encryption and pseudonymisation, to be taken based on risks for the individuals' data compromise.
- Responsibility of carrying out Data Protection Impact Assessments to "evaluate, in particular, the origin, nature, particularity and severity" of risk of data compromise, to then take commensurate steps to mitigate, or report to the supervisory authority prior to processing.
- Explicit details on administrative fines (except in Denmark and Estonia where legal system prohibits) setting maximum figures based on categories.

02_38. ASIC - Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd (Mar 2016)

This report by the Australian Securities & Investment Commission (ASIC) presents the findings of the cyber resilience assessments of ASX Group and Chi-X Australia Pty Ltd.

It also provides some examples of emerging good practices implemented by a wider sample of organisations operating in the Australian financial sector. (FSB-ST[i])

03_30. US DHS Cyber Resilience Review (CRR) Method Description and Self-Assessment User Guide and Assessment Package (Feb 2016)

The purpose of the US Department of Homeland Security's Cyber Resilience Review (CRR) Method Description and Self-Assessment User Guide is "to enable organizations to conduct a self-assessment using the Cyber Resilience Review (CRR). The CRR Self-Assessment provides a measure of an organization's cyber resilience capabilities. This user's guide

- presents an overview of the CRR structure and content
- provides information on how to prepare for a self-assessment
- provides information on how to conduct the self-assessment, which includes recording responses and scoring functions
- assists the organization in evaluating its cyber resilience capabilities
- provides guidance for follow-on activities"

The Cyber Resilience Review (CRR) website provides further resources, background, and the full package which is the entire CRR self-assessment, including the fillable assessment form and report generator:

"The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices."

"The Department of Homeland Security's (DHS) Office of Cybersecurity & Communications (CS&C) conducts complimentary and voluntary assessments to evaluate operational resilience and cybersecurity capabilities within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The Cyber Security Evaluation Program (CSEP) administers the Cyber Resilience Review (CRR) while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers the Cyber Security Evaluation Tool® (CSET) for industrial control systems. While related, the CRR and CSET are two distinct assessments with different areas of focus. Organizations should carefully review the information below and determine which assessment best fits their operating environment.

While the CRR and CSET predate the establishment of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the inherent principles and recommended practices within the CRR and CSET align closely with the central tenets of the CSF."

01_40. ISO/IEC - IT, Security Techniques, InfoSec Management Systems (Feb 2016)

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) maintain an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards. Using the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information. The ISMS family consists of the following International Standards:

- ISO/IEC 27000, Information security management systems - Overview and vocabulary
- ISO/IEC 27001, Information security management systems - Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management - Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 -Requirements
- ISO/IEC 27010, Information security management for inter-sector and interorganizational communications
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014, Governance of information security

- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management - Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

01_41. EU Payment Services Directive 2 (Jan 2016)

The Directive (PSD2) revises the PSD, adopted in 2007, "provides legal foundation for further development of a better integrated internal market for electronic payments within the EU". It takes into account new market entrants offering services, specifically "account information services" (which allow a payment service user to have an overview of their financial situation at any time) and "payment initiation services" (which allow consumers to pay via credit transfer from accounts without intermediaries).

This is made possible as banks will be required to open up customer data via a standard set of Application Programming Interfaces (APIs). It enhances consumer rights, including removal of surcharges for use of credit or debit card, reduced liability for non-authorized payments, and unconditional refund right for euro direct debits. It enhances to role of the EBA to develop a public central register of authorized payment institutions undated by national authorities, to resolve disputes from national authorities, develop regulatory technical standards on strong customer authentication and secure communication channels for all payment service providers, and to develop cooperation and information exchange between the supervisory authorities.

Countries are to incorporate it into national laws by Jan 13, 2018.

02_39. South Africa National Cybersecurity Policy Framework (Dec 2015)

The South African Ministry of State Security published a National Cybersecurity Policy Framework document, establishing the following:

"a) The development and implementation of a Government led, coherent and integrated cybersecurity approach to address cybersecurity threats;

b) Establishing a dedicated policy, strategy and decision making body to be known as the JCPS to identify and prioritise areas of intervention and focused attention regarding Cybersecurity related threats. The Cybersecurity Response Committee will be chaired by the State Security Agency (SSA) and will be a situated at the SSA

c) The capability to effectively coordinate departmental resources in the achievement of common Cybersecurity safety and security objectives (including the planning, response coordination and monitoring and evaluation);

d) Fighting cybercrime effectively through the promotion of coordinated approaches and planning and the creation of required staffing and infrastructure;

e) Coordination of the promotion of Cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to Cybersecurity threats, through interaction with and in conjunction with the Hub (to be established within the Department of Telecommunications and Postal Services);

f) Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;

g) Ensuring of the protection of national critical information infrastructure;

h) The promotion of a Cybersecurity culture and compliance with minimum security standards;

i) The establishment of public-private partnerships for national and action plans in line with the NCPF; and

j) Ensuring a comprehensive legal framework governing cyberspace."

(FSB-ST[i])

03_31. US FFIEC IT Examination Handbook: Management Booklet (Nov 2015)

The US Federal Financial Institutions Examination Council (FFIEC) released an Management Booklet as part of its Information Technology Examination Handbook (IT Handbook) series.

"The "Management" booklet is one of 11 booklets that make up the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook* (*IT Handbook*). The "Management" booklet rescinds and replaces the June 2004 version. This booklet provides guidance to examiners and outlines the principles of overall governance and, more specifically, IT governance. Additionally, this booklet explains how risk management is a component of governance and how IT risk management (ITRM) is a component of risk management. This booklet describes the interaction of these components. The examination procedures in this booklet assist examiners in evaluating the following:
• IT governance as part of overall governance in financial institutions.
• Processes for ITRM as part of risk management in financial institutions."

02_40. France National Digital Security Strategy (Oct 2015)

The French government published a revised National Digital Security Strategy which set out five objectives: 1) Fundamental interests, defence and security of State information systems and critical infrastructures, major cybersecurity crisis; 2) Digital trust, privacy, personal data, cyber-malevolence; 3) Awareness raising, initial training, continuing education; 4) Environment of digital technology businesses, industrial policy, export and internationalization; and 5) Europe, digital strategic autonomy, cyberspace stability. (FSB-ST[i])

01_42. MAS Circular - Tech Risk and Cybersecurity Training for Board (Oct 2015)

The Monetary Authority of Singapore's Circular No. SRD TR 03/2015 on Technology Risk and Cyber Security Training for Board establishes that the board of directors and the senior management of a financial institution are responsible for the oversight of technology risks and cyber security. The Board needs to endorse the organization's IT strategy and risk tolerance, and ensure that management focus, expertise and resources are brought to bear. The board also needs to ensure an appropriate accountability structure and organizational risk culture is in place to support effective implementation of the organization's cyber resilience program. MAS expects the Board to be regularly apprised on salient technology and cyber risk developments, and the financial institution should have a comprehensive technology risk and cybersecurity training program for the Board.

02_41. HKMA Supervisory Policy Manual, Risk Management of E-banking (Sep 2015)

Hong Kong Monetary Authority (HKMA) released a guidance note for authorized institutions, a Supervisory Policy Manual titled "Risk Management for E-banking, defined as "financial services (which could be transactional, enquiry or payment services) provided to personal or business customers and delivered over the Internet, wireless networks, automatic teller machines (ATMs), fixed telephone networks or other electronic terminals or devices." Specifically referenced are (i) Internet banking; (ii) contactless mobile payments; (iii) financial services delivered through self-service terminals; and (iv) phone banking.

It provides guidance in following sections: Major risks inherent in e-banking; Risk governance of e-banking; Customer security; System and network security for Internet banking; Controls related to services offered via Internet banking or the Internet; Security controls in respect of specific e-banking channels; Fraud and incident management; and System availability and business continuity management. (FSB-ST[i])

02_42. Japan's National Center of Incident Readiness and Strategy for Cybersecurity (Sep 2015)

The Japanese government published a Cybersecurity Strategy document under the care of the National Center of Incident Readiness and Strategy for Cybersecurity formulated pursuant to the Basic Act that prescribes the Government's responsibility to establish the Cybersecurity Strategy. The strategy outlines the basic directions of Japan's cybersecurity policies for the coming three years approximately "…to ensure a free, fair, and secure cyberspace; and subsequently contribute to improving socio-economic vitality and sustainable development, building a society where people can live safe and secure lives, and ensuring peace and stability of the international community and national security."

The National Center of Incident Readiness and Strategy for Cybersecurity conducts a cross-sectoral cybersecurity exercise for 13 critical infrastructures, including the financial sector. (FSB-ST[i])

03_32. US NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug 2015)

US National Futures Association (NFA) published an interpretive notice on Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs. The rule is effective March 1, 2016 and requires adoption and enforcement of a written information systems security program. "This Notice provides guidance regarding information systems security practices that Member firms should adopt and tailor to their particular business activities and risks."

Background: "NFA is the industrywide, self-regulatory organization for the U.S. derivatives industry. Designated by the CFTC as a registered futures association, NFA strives every day to safeguard the integrity of the derivatives markets, protect investors and ensure Members meet their regulatory responsibilities."

01_43. MAS Circular on Early Detection of Cyber Intrusions (Aug 2015)

The Monetary Authority of Singapore's Circular No. SRD TR 01/2015 requires that financial institutions not only secure their perimeters from a potential breach, but also have robust capabilities to promptly detect any cyber intrusions so as to enable swift containment and recovery. It considers important that financial institutions maintain a keen sense of situational awareness by continuously enhancing their technical and internal control processes to monitor and detect intrusions in their networks, systems, servers, network devices and endpoints.

02_43. SEBI Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories (Jul 2015)

Securities and Exchange Board of India (SEBI) published a framework regarding cyber security and cyber resilience that Market Infrastructure Institutions would be required to comply with in six months' time. The document specifies that "Cyber security framework include measures, tools and processes that are intended to prevent cyber attacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber attack and to continue operation during, and recover from, a cyber attack." The Framework content is organized in the following sections: 1) Governance; 2) Identify; 3) Protection; 4) Monitoring and Detection; 5) Response and Recovery; 6) Sharing of Information; 7) Training; and 8) Periodic Audit. (FSB-ST[i])

02_44. JFSA Policy Approaches to Strengthen Cyber Security in the Financial Sector (Jul 2015)

The Japanese Financial Services Agency (JFSA) published policy approaches that address cybersecurity for the financial sector in July 2015. The JFSA has been conducting the supervision and inspection regarding cyber security management as a part of system risk control. Given that the threat of cyber attacks is a significant risk for the stability of the financial system, it is necessary to enhance the resilience of the financial system by strengthening the cyber security of not only each financial institution but the financial industry as a whole.

The JFSA will address the five policies below to contribute to strengthening cyber security in the financial sector from the financial regulator's perspective:

1. Constructive dialogue with financial institutions and grasp of their current condition regarding cyber security
2. Improvement of the information sharing framework among financial institutions
3. Continuous implementation of industry-wide cyber security exercises
4. Cybersecurity human resource development in financial sector
5. Arrangement of cyber security initiatives in the JFSA

In addition, the JFS A conducted industry-wide exercises for the first time in October 2016. A year later, the JFSA conducted a more inclusive industry-wide exercise (Delta Wall II) to upgrade capability of small and medium-sized financial institutions and to encourage large financial institutions to utilize more sophisticated evaluation methods to further improve their capability to address cyber security risks. (FSB-ST[i])

02_45. APRA Information Paper: Outsourcing involving Shared Computing Services (including Cloud) (Jul 2015)

Australian Prudential Regulation Authority (APRA) released an Information Paper focusing on 'shared computing services' (arrangements involving the sharing of IT assets with other parties (whether labelled cloud or otherwise)) with the following introduction:

"…Prudential Standard CPS 231 Outsourcing (CPS 231) and Prudential Standard SPS 231 Outsourcing (SPS 231) include requirements relating to the risk management of outsourcing arrangements. In November 2010, APRA wrote to all regulated entities highlighting key prudential concerns that should be addressed when outsourcing includes the use of cloud computing services. More recently, APRA has observed an increase in the volume, materiality and complexity of outsourcing arrangements involving shared computing services (including cloud) submitted to APRA under the consultation and notification requirements of CPS 231 and SPS 231. APRA's review of these arrangements has identified some areas of weakness, reflecting risk management and mitigation techniques that are yet to fully mature in this area. Further guidance may therefore be beneficial.

This Information Paper outlines prudential considerations and key principles that could be considered when contemplating the use of shared computing services. This Information Paper is relevant for a broad audience including senior management, risk management, technical specialists and Internal Audit. Finally, APRA has a number of existing prudential standards and practice guides that are pertinent to shared computing services. This Information Paper applies the concepts included in those standards and guides…" (FSB-ST[i])

01_44. UK FCA/PRA Senior Managers and Certification Regime (Jul 2015)

The UK Financial Conduct Authority (FCA)/ Prudential Regulation Authority (PRA) published final rules for a new regulatory framework "Senior Managers and Certification Regime (SMR)", which replaced the Approved Persons Regime (APR) for banks, building societies, credit unions and dual-regulated (FCA and PRA regulated) investment firms, effective March 2016:

"While the Senior Managers Regime will ensure that senior managers can be held accountable for any misconduct that falls within their areas of responsibilities, the new Certification Regime and Conduct Rules aim to hold individuals working at all levels in banking to appropriate standards of conduct ...

- The Senior Managers Regime focuses on individuals who hold key roles and responsibilities in relevant firms. Preparations for the new regime will involve allocating and mapping out responsibilities and preparing Statements of Responsibilities for individuals carrying out Senior Management Functions (SMFs). While individuals who fall under this regime will continue to be

preapproved by regulators, firms will also be legally required to ensure that they have procedures in place to assess their fitness and propriety before applying for approval and at least annually afterwards.

- The Certification Regime applies to other staff who could pose a risk of significant harm to the firm or any of its customers (for example, staff who give investment advice or submit to benchmarks). These staff will not be preapproved by regulators and firms' preparations will need to include putting in place procedures for assessing for themselves the fitness and propriety of staff, for which they will be accountable to the regulators. These preparations will be important not only when recruiting for roles that come under the Certification Regime but when reassessing each year the fitness and propriety of staff who are subject to the regime.

- The Conduct Rules set out a basic standard for behavior that all those covered by the new regimes will be expected meet. Firms' preparations will need to include ensuring that staff who will be subject to the new rules are aware of the conduct rules and how they apply to them. Individuals subject to either the SMR or the Certification Regime will be subject to Conduct Rules from the commencement of the new regime on 7th March 2016, while firms will have a year after commencement to prepare for the wider application of the Conduct Rules to other staff."

02_46. SFC Circular to all Licensed Corporations on Internet Trading (Jun 2015)

Hong Kong Securities and Futures Commission (SFC) launched a self-assessment checklist (MS Excel based) on its website for Licensed Companies (LCs) with internet trading. The Circular explains:

"The Checklist provides guidance for [Licensed Companies (LCs)] to conduct regular self-assessment of their internet trading systems, network infrastructure, related policies, procedures and practices in order to identify areas that require improvement and, where needed, enhance the same so to ensure compliance with the relevant electronic trading requirements.

Given the potential impact to investors and to market integrity, LCs providing internet trading services to clients are expected to closely monitor the integrity, reliability, security and capacity of the internet trading systems and maintain sufficient resources to cope with any increase in business volume transacted through their internet trading systems. LCs are also expected to complete the Checklist as part of their regular review of their internet trading systems and rectify deficiencies (if any) as soon as practicable." (FSB-ST[i])

02_47. SEC Investment Management Guidance Update on Cybersecurity Guidance (Apr 2015)

The U.S. Securities and Exchange Commission (SEC) issued a guidance note on cybersecurity: "Registered investment companies ("funds") and registered investment advisers ("advisers") may wish to consider in addressing cybersecurity risk, including the following, to the extent they are relevant:

Conduct a periodic assessment of: (1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses; (2) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems; (3) security controls and processes currently in place; (4) the impact should the information or technology systems become compromised; and (5) the effectiveness of the governance structure for the management of cybersecurity risk. An effective assessment would assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk.

Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include: (1) controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening; (2) data encryption; (3) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events; (4) data backup and retrieval; and (5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy.

Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures. Firms may also wish to educate investors and clients about how to reduce their exposure to cyber security threats concerning their accounts." (FSB-ST[i])

01_45. Central Bank of Israel Directive on Cyber-Defense Management (Mar 2015)

The Central Bank of Israel issued a Directive on Cyber-Defense Management. This Directive contains regulatory provisions of the Banking Supervision Department's requirements and expectations regarding the management of cyber defense. The Directive prescribes a structured but flexible framework for cyber-risk management, while allowing the banking corporation to exercise discretion in its implementation. This form of regulatory approach is intended to enable the banking corporation to adapt its defense system in a dynamic manner to the changing cyber-threat landscape. Therefore, the Directive defines principles for cyber-defense, rather than specifying a strict "list of controls". The expectation is that the banking corporation shall adopt these principles while

establishing a cyber-defense array in accordance with the scope and the nature of its business activity, and its risk profile.

01_46. ASIC's Report on Cyber Resilience (Mar 2015)

The Australian Securities & Investment Commission's (ASIC) report "Cyber resilience: health check" is intended to help regulated entities improve their cyber resilience by increasing awareness of cyber risks, encouraging collaboration between industry and government, and identifying opportunities to improve cyber resilience. It also aims to identify how cyber risks should be addressed as part of current legal and compliance obligations relevant to ASIC's jurisdiction.

03_33. US FFIEC IT Examination Handbook: Business Continuity Planning Booklet (Feb 2015)

The US Federal Financial Institutions Examination Council (FFIEC) released an Business Continuity Planning Booklet as part of its Information Technology Examination Handbook (IT Handbook) series. It includes an appendix (J) on Outsourcing "Strengthening the Resilience of Outsourced Technology Services"

"This booklet is one in a series of booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook. This booklet provides guidance to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. This booklet was also designed to provide helpful guidance to financial institutions regarding the implementation of their business continuity planning processes."

03_34. US FINRA Report on Cybersecurity Practices (Feb 2015)

The Financial Industry Regulatory Authority (FINRA) published a Report on Cybersecurity Practices in the broker-dealer industry to highlight effective practices that firms should consider to strengthen their cybersecurity programs. The report "draws in part from the results of FINRA's recent targeted examination ("sweep") of a cross-section of firms. The sweep, conducted in 2014, focused on the types of threats firms face, areas of vulnerabilities in their systems and firms' approaches to managing these threats."

Background: "The Financial Industry Regulatory Authority (FINRA), is the largest independent regulator for all securities firms doing business in the United States. FINRA is dedicated to investor protection and market integrity through effective and efficient regulation and complementary compliance and technology-based services. FINRA touches virtually every aspect of the securities business – from registering and educating all industry participants to examining securities firms, writing rules, enforcing those rules

and the federal securities laws, and informing and educating the investing public. In addition, FINRA provides surveillance and other regulatory services for equities and options markets, as well as trade reporting and other industry utilities. FINRA also administers the largest dispute resolution forum for investors and firms."

03_35. US CSBS Cybersecurity 101: A Resource Guide for Bank Executives (Dec 2014)

The Conference of State Bank Supervisors (CSBS) has a Cybersecurity 101: A Resource Guide for Bank Executives. "CSBS has published a non-technical, easy-to-read resource guide on cybersecurity that bank CEOs and senior executives may use to help mitigate cybersecurity threats at their banks. The guide puts into one place industry recognized standards for cybersecurity and best practices currently used within the financial services industry. The information provided within this guide is tailored to furnish CEOs with the necessary tools to better understand the threats your institution faces and how to prepare for them. It also provides questions to ask staff to ensure they are proactive in identifying and addressing cybersecurity risks."

Background: "CSBS supports state regulators in advancing the system of state financial supervision by ensuring safety, soundness and consumer protection; promoting economic growth; and fostering innovative, responsive supervision. CSBS was organized in 1902 as the National Association of Supervisors of State Banks. In 1971, the name of the organization was changed to the Conference of State Bank Supervisors…"

01_47. EBA Guidelines on Security of Internet Payments (Dec 2014)

The European Banking Authority (EBA)'s Guidelines on Security of Internet Payments was published, with implementation date 1 August 2015. The implementation of any potentially more stringent requirements necessary under the Payment Systems Directive 2 was intended to occur at a later stage, by the date set in the PSD 2.

The Guidelines encompass the following:

1. *General control and security environment*: Governance; Risk Assessment; Incident Monitoring and Reporting; Risk Control and Mitigation; and Traceability.
2. *Specific control and security measures for internet payments*: Initial customer identification, information; Strong customer authentication; Enrolment for, and provision of, authentication tools and/or software delivered to the customer; Log-in attempts, session time out, validity of authentication; Transaction monitoring; and Protection of sensitive payment data.
3. *Customer awareness, education, and communication* including Notifications, setting of limits; and Customer access to information on the status of payment initiation and execution.

02_48. Japan's Basic Act on Cybersecurity (Nov 2014)

Japan adopted the Basic Act on Cybersecurity in November 2014. The purpose of this Act is to promote cybersecurity, given the intensification of threats on a worldwide scale, and the need to ensure the free flow of. In addition to requiring the national and local governments to take measures to boost cybersecurity, the law obligates businesses related to infrastructure and cyber-businesses to take voluntary measures to enhance cybersecurity and cooperate with the government on implementation of relevant measures. The government provides support for cybersecurity measures for infrastructure businesses.

The Cybersecurity Strategic Headquarters are established under the Cabinet. "The promotion of the Cybersecurity policy must be required to be carried out in consideration of the basic principles of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society." (FSB-ST[i])

03_36. CBR Central Bank of Russia Standard for Maintenance of Information Security of the Russian Banking System Organisations (Jun 2014)

Central Bank of Russia published its General Provisions & Assessment Method for its Standard STO BR IBBS-1.0-2014 on Maintenance of Information Security of the Russian Banking System Organisations.

"To check the level of information security (IS) both in the Bank of Russia and the organisations of the banking system (BS) of the Russian Federation (RF), the Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions' defines the requirements for regular IS audit and IS self-assessment.

This standard establishes the methods for determining the degree of compliance with the requirements of the Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions', as well as the final level of IS conformity to the requirements of the Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of Organisations of the Russian Banking System Organisations. General Provisions' during the IS audit and IS self-assessment…

"The provisions of this standard shall apply on a voluntary basis, unless the application of specific provisions is made binding by Russian legislation or other regulations, including Bank of Russia regulations. The application of this standard may be made binding by agreements concluded by RF BS organisations or the decision of a RF BS organisation to accede to the standard. In such cases, requirements of this standard containing 'must' provisions are obligatory, while recommendations are to be applied as decided by the RF BS organisation."

02_49. CODISE publishes new Guide (May 2014)

Italy's CODISE (the acronym of the Italian "continuità di servizio" (business continuity), created in 2003, is responsible for crisis management coordination in the Italian financial marketplace. It is chaired by the Banca d'Italia and includes representatives of Italian Securities Commission (CONSOB) and the systemically important financial institutions.

CODISE's objectives, its roles, responsibilities and activities are described in the newly published guide. "It serves to purpose to facilitate the exchange of information, the adoption of the necessary measures to deal with events that may put at risk the system business continuity, the smooth functioning of financial infrastructures and the public confidence in money. Interventions are defined according to the type of event, its extent and its potential impacts on the financial system.

CODISE plans and executes simulations to check the adequacy of its procedures, while allowing participants to test their internal procedures for business continuity management.

It is also a forum for analysis and discussion among its participants on the evolution of business continuity threats, risk prevention and control measures including cyber security." (FSB-ST[i])

02_50. CBR Russian banking system standard on information security maintenance (Apr 2014)

Bank of Russia published a standard on information security maintenance for Russian banking system organisations. "The main aims of the standardisation of information security maintenance in Russian banking system organisations include:

- To develop and strengthen the Russian banking system;
- To increase confidence in the Russian banking system;
- To maintain the stability of Russian banking system organisations and thereby the stability of the Russian banking system as a whole;
- To achieve adequacy of protective measures to actual information security threats;
- To prevent and/or reduce damage from information security incidents.

The main objectives of standardisation for information security provision for Russian banking system organisations include:

- To establish uniform requirements for information security maintenance in Russian banking system organisations;
- To improve the effectiveness of information security maintenance and support measures in Russian banking system organisations." (FSB-ST[i])

01_48. MAS Notice on Technology Risk Management (Mar 2014)

Notice CMG-N02 of the Monetary Authority of Singapore (MAS) requires regulated financial institutions to: a) make all reasonable effort to maintain high availability for critical systems; b) establish a recovery time objective of not more than 4 hours for each critical system; c) notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident; d) submit within 14 days a root cause and impact analysis report to the Authority; and e) implement IT controls to protect customer information from unauthorized access or disclosure.

This Notice applies to all: (a) approved exchanges; (b) licensed trade repositories; (c) approved clearing houses; (c) recognized clearing houses which are incorporated in Singapore; (d) holders of a capital markets services license; (e) recognized market operators which are incorporated in Singapore; and (f) persons who are approved under section 289 of the Act to act as a trustee of a collective investment scheme which is authorized under section 286 of the Securities and Futures Act and constituted as a unit trust.

02_51. Spain National Cyber Security Strategy (Dec 2013)

Spain published a National Cyber Security Strategy that establishes the guiding principles of cybersecurity, namely:

- National leadership and the coordination of efforts;
- Shared responsibility;
- Proportionality, rationality and efficiency; and
- International cooperation.

The overall objective of the strategy is to ensure that "Spain makes secure use of information and telecommunication systems, strengthening cyber attack prevention, defence, detection, analysis, investigation, recovery and response capabilities." To achieve this, the strategy lays down specific objectives, action lines and establishes the organizational structure under the direction of the Prime Minister. (FSB-ST[i])

02_52. Netherlands National Cyber Security Strategy (Oct 2013)

Building on the first Strategy (2011), which appointed the Cyber Security Council (which provides requested and unrequested advice to the government, and also has as task ensuring the performance of the National Cyber Security Strategy (NCSS)), the Dutch Ministry of Security and Justice published its NCSS2.

The NCSS2 outlines the government's commitments, over the period into 2016, to the following five strategic objectives, that the Netherlands: 1) is resilient to cyber attacks and protects its vital interests in the digital domain; 2) tackles cyber crime; 3) invests in secure

ICT products and services that protect privacy; 4) builds coalitions for freedom, security and peace in the digital domain; and 5) has sufficient cyber security knowledge and skills and invests in ICT innovation."

The strategy includes strengthening of its National Cyber Security Centre (NCSC), instituting "a stronger structure for confidential information-sharing and analysis. Furthermore, the NCSC assumes the role of expert authority, providing advice to private and public parties involved, both when asked and at its own initiative. Finally, based on its own detection capability and its triage role in crises, the NCSC develops into Security Operations Centre (SOC) in addition to its role as a Computer Emergency Response Team (CERT)." (FSB-ST[i])

02_53. OSFI Cyber Security Self-Assessment Guidance (Oct 2013)

Canada's Office of the Superintendent of Financial Institutions (OSFI – covering banks, insurance companies, federally regulated trust and loan companies, and federally regulated cooperative credit associations) published "the annexed cyber security self-assessment guidance to assist federally regulated financial institutions (FRFIs) in their self-assessment activities. FRFIs are encouraged to use this template or similar assessment tools to assess their current level of preparedness, and to develop and maintain effective cyber security practices.

OSFI does not currently plan to establish specific guidance for the control and management of cyber risk. Notwithstanding, and in line with its enhanced focus on cyber security as highlighted in its Plan and Priorities for 2013-2016, OSFI may request institutions to complete the template or otherwise emphasize cyber security practices during future supervisory assessments…

This self-assessment template sets out desirable properties and characteristics of cyber security practices that could be considered by a FRFI when assessing the adequacy of its cyber security framework and when planning enhancements to its framework."

The assessment asks the institutions to rate their level of implementation 'maturity' in six areas: 1. Organization and Resources; 2. Cyber Risk and Control Assessment; 3. Situational Awareness; 4. Threat and Vulnerability Risk Management; 5. Cyber Security Incident Management; and 6. Cyber Security Governance. (FSB-ST[i])

02_54. ASIC REGULATORY GUIDE 172: Australian market licences: Australian operators (Sep 2013)

This guide by the Australian Securities & Investment Commission (ASIC) includes an addendum on market licensee systems and controls from November 2012. "The guide outlines [ASIC's] role in and approach to financial market regulation under the

Corporations Act 2001. It deals with financial markets operating in Australia, with particular focus on Australian operators…" (FSB-ST[i])

ASIC also has a report titled "Cyber Resilience: Health Check" of March 2015. AISC has under its jurisdiction FMIs, trading venues, banks, insurance companies, broker-dealers, asset managers, and pension funds.

02_55. ACPR guidance: risks associated with cloud computing (Jul 2013)

The French Autorité de Contrôle Prudentiel et de Résolution (ACPR - Prudential Supervisory Authority) published an analyses and syntheses paper on the risks associated with cloud computing. Gathering information from banks and insurance companies through a survey by the Secrétariat général de l'Autorité de contrôle prudentiel (SGACP – General Secretariat of the Prudential Supervisory Authority), the analyses largely pointed to a need to define cloud computing, that it posed a greater risk than conventional IT outsourcing, and that there were varied opinions on the economic aspects and use of cloud computing. Accordingly, ACPR noted: "These good practices form part of the broader framework defined for the supervision of outsourced services, including conventional outsourcing. The expectations of the ACP in terms of governance of decisions, risk analysis, contractual elements, monitoring and the internal control of cloud computing services are therefore similar to those currently in force in prudential supervision."

Specifically, ACPR noted following areas in which it is "encouraging the companies it supervises to take suitable risk management measures in respect of the following aspects:

- Legal: by enforcing a mandatory contractual framework for cloud computing services;
- Technical: by encrypting data during transport and storage (in the absence of anonymisation);
- Supervision of the service provider: by ensuring audit capability and the right for the ACP to conduct audits;
- Continuity of the service: by ensuring that the expectations of the client company can be formalised in service contracts;
- Reversibility of the service: by defining the conditions of reversibility when subscribing to the service;
- Integration and architecture of information systems: by adapting the organisation and governance of information systems to the use of cloud computing." (FSB-ST[i])

02_56. MAS Technology Risk Management Guideline (Jun 2013)

The Monetary Authority of Singapore (MAS) published a Guideline to "set out risk management principles and best practice standards to guide the FIs in the following: a.

Establishing a sound and robust technology risk management framework; b. Strengthening system security, reliability, resiliency, and recoverability; and c. Deploying strong authentication to protect customer data, transactions and systems." (FSB-ST[i])

The Guideline is organized into sections: 1) Oversight of technology risk by board of directors and senior management; 2) Technology risk management framework; 3) Management of IT outsourcing risks; 4) Acquisition and development of Information Systems; 5) IT service management; 6) Systems reliability, availability and recoverability; 7) Operational infrastructure security management; 8) Data centres protection and controls; 9) Access controls; 10) Online financial services; 11) Payment card security (ATMs, credit and debit cards); and 12) IT Audit.

02_57. APRA Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology (May 2013)

Australian Prudential Regulation Authority (APRA)'s jurisdiction encompasses banks, insurance companies, and pension funds. These prudential practice guides (PPGs) are not requirements but "provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss statutory requirements from legislation, regulations or APRA's prudential standards…"

This PPG aims to assist regulated institutions in the management of security risk in information and information technology (IT). It is designed to provide guidance to senior management, risk management and IT security specialists (management and operational).

The PPG targets areas where APRA continues to identify weaknesses as part of its ongoing supervisory activities. The PPG does not seek to provide an all-encompassing framework, or to replace or endorse existing industry standards and guidelines.

Subject to meeting APRA's prudential requirements, regulated institutions have the flexibility to manage security risk in IT in a manner best suited to achieving their business objectives. Not all of the practices outlined in this prudential practice guide will be relevant for every regulated institution and some aspects may vary depending upon the size, complexity and risk profile of the institution" (FSB-ST[i]).

04_28. PCI Data Security Standard Cloud Computing Guidelines (Feb 2013)

The PCI Security Standards Council published a new guidance version 2.0 of the PCI Data Security Standard (PCI DSS) on Cloud Computing.

"This document provides guidance on the use of cloud technologies and considerations for maintaining PCI DSS controls in cloud environments. This guidance builds on that provided in the PCI DSS Virtualization Guidelines and is intended for organizations

using, or thinking of using, providing, or assessing cloud technologies as part of a cardholder data environment (CDE). This document is structured as follows:

- Executive Summary – Includes a brief summary of some key points and provides context for the remainder of the document.
- Cloud Overview – Describes the deployment and service models discussed throughout this document.
- Cloud Provider/ Cloud Customer Relationships – Discusses how roles and responsibilities may differ across different cloud service and deployment models.
- PCI DSS Considerations – Provides guidance and examples to help determine responsibilities for individual PCI DSS requirements, and includes segmentation and scoping considerations.
- PCI DSS Compliance Challenges – Describes some of the challenges associated with validating PCI DSS compliance in a cloud environment.
- Additional Security Considerations – Explores a number of business and technical security considerations for the use of cloud technologies.
- Conclusion – Presents recommendations for starting discussions about cloud services

The following appendices are included to provide additional guidance:

- Appendix A: PCI DSS Responsibilities for different Service Models – Presents additional considerations to help determine PCI DSS responsibilities across different cloud service models.
- Appendix B: Sample Inventory – Presents a sample system inventory for cloud computing environments.
- Appendix C: PCI DSS Responsibility Matrix – Presents a sample matrix for documenting how PCI DSS responsibilities are assigned between cloud provider and client.
- Appendix D: PCI DSS Implementation Considerations – Suggests a starting set of questions that may help in determining how PCI DSS requirements can be met in a particular cloud environment…"

Background: "The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors, and vendors worldwide."

04_29. NIST Computer Security Incident Handling Guide SP 800-61 r.2 (Aug 2012)

"…This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications."

Supersedes SP 800-61 Rev. 1 (March 2008)

02_58. PBOC Implementation guide for classified protection of information system of financial industry (July 2012)

The People's Bank of China issued an "Implementation guide for classified protection of information system of financial industry" (part of unofficial English version) in July 2012. It is meant for use by the departments of financial institution (including its affiliates), e.g. system planning and development (service and technology), application development, system operation, security management, system use, internal supervision and audit. It also may serve as basis for supervision, inspection, and guidance for information security functions. (FSB-ST[i])

04_30. CBR Regulation No. 382-P – Fund transfers information protection (Jun 2012)

Central Bank of Russia released CBR Regulation No. 382-P "On the Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Monitor the Compliance with the Requirements to Protect Information Related to Funds Transfers" (Russian Only)

04_31. COBIT 5 (Apr 2012)

COBIT 5 (excerpt; presentation) was released by the IT Governance Institute (ITGI) of ISACA: "COBIT 5 is a comprehensive framework of globally accepted principles, practices, analytical tools and models that can help any enterprise effectively address critical business issues related to the governance and management of information and technology….

"COBIT 5 consolidates and integrates the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also draws significantly from the Business Model for Information Security (BMIS) and ITAF."

Indicating an evolution from a IT Governance Framework, COBIT 5 is "A Business Framework for the Governance and Management of Enterprise IT".

COBIT is primarily an educational resource for chief information officers (CIOs), senior management, IT management and control professionals.

03_37. US FFIEC IT Examination Handbook: Audit Booklet (Apr 2012)

The US Federal Financial Institutions Examination Council (FFIEC) released an Audit Booklet as part of its Information Technology Examination Handbook (IT Handbook) series.

"This "Audit Booklet" is one of several booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) and provides guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) audit function."

04_32. US NIST definition of Cloud Computing SP 800-145 (Sep 2011)

The National Institute of Standards and Technology (NIST) published this Guideline "Definition of Cloud Computing" for use by Federal agencies and intended audience of system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

"The NIST cloud computing definition is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services. It provides a simple and unambiguous taxonomy of three service models available to cloud consumers: cloud software as a service (SaaS), cloud platform as a service (PaaS), and cloud infrastructure as a service (IaaS). It also summarizes four deployment models describing how the computing infrastructure that delivers these services can be shared: private cloud, community cloud, public cloud, and hybrid cloud. Finally, the NIST definition also provides a unifying view of five essential characteristics that all cloud services exhibit: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service…"

04_33. NIST Cloud Computing Reference Architecture SP 500-292 (Sep 2011)

After the formation of its cloud computing definition, the National Institute of Standards and Technology (NIST) published this Paper "Cloud Computing Reference Architecture: Recommendations of the NIST" as a next step, "..to create an intermediate reference point from where one can frame the rest of the discussion about cloud computing and begin to identify sections in the reference architecture in which standards are either required, useful or optional…" The NIST has a technical lead role in the US Government's efforts related to the adoption and development of cloud computing standards.

"The NIST cloud computing reference architecture presented in this document is a logical extension to the NIST cloud computing definition. It is a generic high-level conceptual

model that is an effective tool for discussing the requirements, structures, and operations of cloud computing… It defines a set of actors, activities and functions that can be used in the process of developing cloud computing architectures, and relates to a companion cloud computing taxonomy.

The reference architecture contains a set of views and descriptions that are the basis for discussing the characteristics, uses and standards for cloud computing. This actor/role based model is intended to serve the expectations of the stakeholders by allowing them to understand the overall view of roles and responsibilities in order to assess and assign risk. The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

The design of the NIST cloud computing reference architecture serves the following objectives: to illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model; to provide a technical reference to USG agencies and other consumers to understand, discuss, categorize and compare cloud services; and to facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations…"

04_34. Chatham House - Cyber Security and the UK's Critical National Infrastructure (Sep 2011)

Chatham House's the Royal Institute of International Affairs published a research report "based on a series of high-level interviews through which the authors sought to gauge the various organizations' overall understanding of, and response to, the problem of cyber security…" focusing "wherever possible to assess the level of cyber security awareness at board level, and particularly among the most senior executives who had no specific IT expertise." The report takes specifically those organizations defined as critical national infrastructure (CNI) - communications, emergency services, energy, finance, food, government and public services, health, transport and water – by the Centre for the Protection of Critical National Infrastructure and the UK Cyber Security Strategy, and "asks whether the various agencies, bodies and individuals involved recognize the significance of the cyber stakeholder status that has been conferred upon them…. How do these organizations identify and measure their cyber dependencies, and how well and systematically do they manage the risks and mitigate the potential vulnerabilities associated with these dependencies?" The report includes observations and recommendations.

"Chatham House (Royal Institute of International Affairs) in London promotes the rigorous study of international questions and is independent of government and other vested interests."

01_49. World Bank - General Principles for Credit Reporting (Sep 2011)

World Bank Financial Infrastructure Series - General Principles for Credit Reporting Abstract: "This report describes the nature of credit reporting elements which are crucial for understanding credit reporting and to ensuring that credit reporting systems are safe, efficient and reliable. It intends to provide an international agreed framework in the form of international standards for credit reporting systems' policy and oversight. The Principles for credit reporting are deliberately expressed in a general way to ensure that they can be useful in all countries and that they will be durable. These principles are not intended for use as a blueprint for the design or operation of any specific system, but rather suggest the key characteristics that should be satisfied by different systems and the infrastructure used to support them to achieve a stated common purpose, namely expanded access and coverage, fair conditions, and safe and efficient service for borrowers and lenders. Section two provides a brief overview of the market for credit information sharing and credit reporting activities and then analyzes in some detail the key considerations underlying credit reporting. Section three outlines the general principles and related roles. Section four proposes a framework for the effective oversight of credit reporting systems."

01_50. BCBS Principles for the Sound Management of Operational Risk (Jun 2011)

Basel Committee on Banking Supervision (BCBS)'s Principles for the Sound Management of Operational Risk and the Role of Supervision updates and replaces the 2003 Sound Practices for the Management and Supervision of Operational Risk. This document incorporates the evolution of sound practice and details eleven principles of sound operational risk management covering (1) governance, (2) risk management environment and (3) the role of disclosure.

It covers fundamental principles of operational risk management: first, for the Board of Directors to establish a strong risk management culture, maintaining a framework for operational risk management fully integrated into the bank's overall risk management processes. Under Governance, it details the role of Board of Directors and Senior Management. Risk Management Environment section includes risk Identification and Assessment, regular Monitoring and Reporting, strong Control and Mitigation practices. The principles also speak to Business Resiliency and Continuity plans, as well as public disclosures to allow stakeholders' assessment of operational risk management.

Of relevance to cyber issues is Technology Risk and Outsourcing, specifically that Senior management needs to ensure that staff responsible for managing operational risk coordinate and communicate effectively with those responsible for outsourcing arrangements. The Control and Mitigation section includes the requirement to have an integrated approach to identifying, measuring, monitoring and managing technology risks. Further, it details that "the board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities" and delineates activities that outsourcing policies and risk management should encompass.

01_51. FFIEC - Authentication in Internet Banking Environment, suppl. (Jun 2011)

The US FFIEC released a Supplementary update to the Authentication in an Internet Banking Environment Guidance of 2005. "The Supplement reiterates and reinforces the expectations described in the 2005 Guidance that financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also identifies certain specific minimum elements that should be part of an institution's customer awareness and education program." "Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities."

New guidance took effect January 2012 for examiners to formally assess institutions against these enhanced expectations.

01_52. AICPA suite of SOC & Implementation Guidance (Apr 2010)

System and Organization Controls (SOC) is a suite of service offerings (independent audit reports) that Certified Public Accountants may provide in connection with system level controls of a service organization or entity-level controls of other organizations. They are independent attestations of an organization's operating environment, similar to the ISO certifications, a well-recognized audit regime that covers both financial and security aspects.

The SOC report series include:

- SOC 1: Reporting on Controls at a Service Organization;
- SOC 2: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy;
- SOC 3: Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy

02_59. CBRC Guidelines on the Risk Management of Commercial Banks' Information Technology (2009)

The China Banking Regulatory Commission (CBRC) released regulatory Guidelines on the Risk Management of Commercial banks' Information Technology, which apply to all the commercial banks legally incorporated within the territory of the People's Republic of China, and "may apply to other banking institutions including policy banks, rural cooperative banks, urban credit cooperatives, rural credit cooperatives, village banks, loan companies, financial asset management companies, trust and investment companies,

finance firms, financial leasing companies, automobile financial companies and money brokers". The Guideline covers IT governance, IT risk management, information security, application system development, test and maintenance, IT operation, business continuity management, outsourcing, internal audit, external audit, and supplementary provisions. (FSB-ST[i23])

01_53. ENISA National Exercises Good Practice Guide (Dec 2009)

The European Union Agency for Network and Information Security (ENISA) guide was released "to assist authorities in Member States to better understand the complexities of exercises and help them prepare local and national ones. This guide was prepared by interviewing experts on exercises throughout the EU and beyond with the aim to identify good practices that were already applied and proved to be effective."

"The guide examines these practices by first giving an introduction to the subject of exercises, then reviewing the life-cycle of an exercise (identifying, planning, conducting, and evaluating) systematically. Also, the roles of the involved stakeholders are presented. Throughout the guide, good practices are highlighted for easy identification."

01_54. ENISA Good Practice Guide on Incident Reporting (Dec 2009)

Given strong commitment by the EU institutions and the Member States to the resilience of public communications networks, the European Union Agency for Network and Information Security (ENISA) was asked to help Member States and EU institutions to identify good practices in incident reporting schemes. This document addresses many of the issues that Member States will face as they debate, take stock, establish, launch, develop and harmonize their incident reporting systems at national level. The report discusses schemes for reporting incidents that may harm or threaten the resilience and security of public eCommunication networks. It examines the whole lifecycle of a reporting scheme, from the first steps in designing the scheme, through engaging the constituency's cooperation, setting the reporting procedures, and then management and improvement of the scheme.

02_60. German Federal Office for Information Security Act (Aug 2009)

The Act established a Federal Office of Information Security to be overseen by the Federal Ministry of the Interior, to perform specific tasks to promote security of information technology and to be the central clearinghouse for cooperation among federal authorities in matters related to the security of information technology. (FSB-ST[i])

[23] "FSB-ST" denotes those items mentioned in the "FSB Stocktake on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices".

04_35. COBIT 4.1 (May 2007)

COBIT 4.1 (excerpt) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the enterprises' IT governance and control framework.

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution…

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

Designed and created by IT Governance Institute (ITGI) of the Information Systems Audit and Control Association (ISACA) in 1996, COBIT has evolved from an IT audit and control framework used by the assurance profession to a comprehensive IT governance framework. COBIT is primarily an educational resource for chief information officers (CIOs), senior management, IT management and control professionals. "COBIT 4.1 has become the integrator for IT best practices and the umbrella framework for IT governance, because it is harmonized with other standards and continuously kept up to date."

03_38. CBR Central Bank of Russia Standard for Information Security of Russian Banking Institutions Information Security Audit (May 2007)

Central Bank of Russia published its Standard STO BR IBBS-1.1-2007 Information Security of Russian Banking Institutions Information Security Audit.

"One of the prerequisites for achieving the goals of Russian banking institutions (RBIs) is maintaining a necessary and sufficient level of their information security (IS). An IS audit is the main type of inspection used to check the IS level in RBIs. Global experience in IS defines an IS audit as a key process in the continuous cycle of IS management in an organisation. The Bank of Russia is a proponent of regular IS audits conducted in RBIs. The main goals of the IS audit of RBIs are as follows: - Increasing confidence in RBIs; -

Assessing the compliance of IS in RBIs with IS audit criteria established in accordance with requirements of Bank of Russia Standard STO BR IBBS-1.0 "Information Security of Russian Banking Institutions. General Provisions""

"This standard applies to RBIs, as well as to organisations that conduct the IS audit of RBIs, and establishes the requirements for conducting the external IS audit of RBIs… The provisions of this standard shall apply on a voluntary basis, unless some specific provisions are made binding by applicable legislation, a Bank of Russia regulation or the terms of a contract."

01_55. KR Electronic Financial Transactions Act & Enforcement Decree (Jan 2007)

The South Korean Electronic Financial Transactions Act was enacted in January 2007. The Act (last amended May 2013) and Enforcement Decree (last amended March 2014) is for "ensuring the security and reliability of electronic financial transactions by clarifying their legal relations and to promoting financial conveniences for people and developing the national economy by creating a foundation for the sound development of electronic financial industry." It provides the legal grounds for the financial sector regulators to conduct supervision and examination of financial institutions and electronic financial business operators. According to the Act and other related regulations, Financial Institutions (FIs) should adopt comprehensive measures to better cope with cyber threats and manage related risks.

01_56. KR Reg. on Supervision of Electronic Financial Transactions (Jan 2007)

The South Korean Regulation on Supervision of Electronic Financial Transactions, last amended on June 30, 2016, prescribes to the Financial Services Commission, as the body delegated in the Electronic Financial Transactions Act, the matters under its authority that are "required for securing the safety of the information technology sector of an institution subject to examination by the Financial Supervisory Service under other Acts and subordinate statutes." It addresses "Rights and Obligations of Parties to Electronic Financial Transactions"; "Securing the Safety of Electronic Financial Transactions and Protecting Users"; "Licensing, Registration and Operation of Electronic Financial Affairs"; and "Supervision of Electronic Financial Affairs". It includes explanatory Tables on "Standards for Computing the Number of IT Personnel and Information Protection Personnel"; "Standards for IT Sector and Information Protection Budgets"; "Specific Limits on Use of Means of Electronic Payment"; "Prerequisites for Major Investors"; "Financial Companies Subject to Evaluation of IT Sector Operation"; and "Types of Assets with Low Investment Risk".

03_39. US FFIEC IT Examination Handbook: Operations Booklet (Jul 2004)

The US Federal Financial Institutions Examination Council (FFIEC) released an Operations Booklet as part of its Information Technology Examination Handbook (IT Handbook) series.

"This booklet is one in a series that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Handbook (IT Handbook). It provides guidance to examiners and financial institutions on risk management processes that promote sound and controlled operation of technology environments. Information is one of the most important assets of an institution, and information technology (IT) operations should process and store information in a timely, reliable, secure, and resilient manner. This booklet addresses IT operations in the context of tactical management and daily delivery of technology to capture, transmit, process, and store the information assets and support the business processes of the institution. The examination procedures contained in this booklet assist examiners in evaluating an institution's controls and risk management processes relative to the risks of technology systems and operations that reside in, or are connected to the institution."

03_40. US FFIEC IT Examination Handbook: Outsourcing Booklet (Jun 2004)

The US Federal Financial Institutions Examination Council (FFIEC) released an Outsourcing Booklet as part of its Information Technology Examination Handbook (IT Handbook) series.

"The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) "Outsourcing Technology Services Booklet" (booklet) provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships."

APPENDIX: INDEXES by CONCEPTS

Please see separate CyberDigest_Indexes_v5.xlsx file, tabs "Appendix-Concepts-to-Docs" and "Appendix-Docs-to-Concepts".