Financial Sector's Cybersecurity: A Regulatory Digest*

October 2017

This Digest is intended to be a "live", periodically updated compilation of recent cybersecurity laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector, therefore is 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 time of addition to the Digest.* It has been compiled and it is being maintained by Aquiles A. Almansi (Lead Financial Sector Specialist, GFM03), Yejin Carol Lee (Senior Financial Sector Specialist, GFM01a), and Johanna Lincoln (FinSAC Consultant).

CONTENTS

TABLES

TABLE 1. List of Included Documents Applicable to Single Jurisdictions

(Alphabetical Order of Country followed by Date)

INSTITUTION	DATE	NAME
Australia Treasury	Sep 2017	Draft Treasury Laws Amendment (Banking Executive Accountability and Related Measures) Bill 2017
Australian Securities & Investment Commission	Mar 2015	ASIC Report on Cyber Resilience
China	Jun 2017	People Republic of China Cyber-Security Law
Germany BaFin	Mar 2017	BaFin consultation on Circular on bank regulatory requirements for IT systems
HK SFC	Dec 2016	HK SFC Circular on augmenting accountability of senior management
HKMA	Dec 2016	HKMA Circular on the Cyber-security Fortification Initiative
HK SFC	Oct 2016	HK SFC Review of cyber-security of online and mobile trading systems
Reserve Bank of India	Sep 2016	India Non-Banking Financial Company - Account Aggregators
Bank of Ireland	Sep 2016	Central Bank of Ireland Cross Industry Guidance on IT and Cyber-security Risks
Bank of Israel	Mar 2015	Central Bank of Israel Directive on Cyber-defense Management
Korea	Jan 2007	Korea Electronic Financial Transactions Act and Enforcement Decree
Korean FSC/FSS	Jan 2007	Korea Regulation on Supervision of Electronic Financial Transactions
SC Malaysia	Oct 2016	Malaysia Securities Commission Guidelines to enhance cyber-resilience of the Capital Market
Association of Banks in Singapore	June 2017	Singapore Association of Banks' Guidelines on control objectives and procedures for outsourced service providers
MA Singapore	July 2016	MAS Guidelines on Outsourcing
MA Singapore	Oct 2015	MAS Circular on Technology risk and cyber-security training for Board

INSTITUTION	DATE	NAME
MA Singapore	Aug 2015	MAS Circular on Early Detection of Cyber Intrusions
MA Singapore	Mar 2014	MAS Notice on Technology Risk Management
UK FCA	Jul 2017	UK FCA Consultation on extending Individual Accountability regime (SMCR)
UK CMA	Mar 2017	UK Open Banking Initiative
UK Government	Dec 2016	UK Government Cyber-security Regulation and Incentives Review
Bank of England	2016	UK CBEST Intelligence-led cyber security assessment 2.0
UK FCA & PRA	Jul 2015	UK FCA Senior Managers and Certification Regime (final rules)
US NIST	Aug 2017	US NIST Cybersecurity Workforce Framework
US SEC	Aug 2017	US SEC Cybersecurity Examination Initiative Risk Alert
US FFIEC	May 2017	FFIEC Cybersecurity Assessment Tool
NYDFS	Mar 2017	New York cyber-security requirements for financial services companies
US NIST	Jan 2017	US NIST draft updated Framework for Improving Critical Infrastructure Cyber-security
US FinCEN	Oct 2016	US FinCEN Advisory on FIs obligations on cyber-related events and crimes
US Federal Banking Agencies	Oct 2016	US Federal Banking Agencies ANPR for enhanced cyber-security standards
US FFIEC	Jun 2011	FFIEC - Supplement to Authentication in an Internet Banking Environment

TABLE 2. List of Included Documents Applicable to the European Union

INSTITUTION	DATE	NAME
ECB	2017	ECB (SSM) Cyber Incident Reporting Framework (2017)
EU Parliament	May 2017	EU Parliament Report on influence of technology on future of financial sector
ESAs (EBA, EIOPA, ESMA)	Apr 2017	ESAs Report on main risks for the EU Financial System
EC	Mar 2017	EU Commission Consultation on the impact of FinTech
ENISA	Aug 2016	ENISA Strategies for Incident Response and Cyber Crisis Cooperation
EC	Jul 2016	EU Directive on Security of Network and Information Systems
EBA	Jun 2016	EBA ICT risk guidelines
EC	Apr 2016	EU General Data Protection Regulation
EC	Jan 2016	EU Payment Services Directive 2
EBA	Dec 2014	EBA Guidelines on Security of Internet Payments
ENISA	Dec 2009	ENISA National Exercise Good Practice Guide
ENISA	Dec 2009	ENISA Good Practice Guide on Incident Reporting

TABLE 3. List of Included Documents Applicable to Multi-Jurisdictions

INSTITUTION	DATE	NAME
Financial Stability Institute	Aug 2017	FSI Insights on policy implementation No 2: Regulatory approaches to enhance banks' cyber-security frameworks
IMF	Aug 2017	IMF Working Paper - Cyber Risk, Market Failures, and Financial Stability
SWIFT	July/May/Apr 2017	SWIFT Customer Security Program
G7	May 2017	G7 CEG developing fundamental elements for effective assessment of cyber-security
AICPA	Apr 2017	AICPA SOC for Cybersecurity
CPMI	Feb 2017	CPMI Report on distributed ledger technology in payment clearing and settlement
G7	Oct 2016	G7 fundamental elements of cyber-security in the financial sector
CPMI-IOSCO	Jun 2016	CPMI-IOSCO Guidance on cyber-security
IOSCO	Apr 2016	Report on IOSCO's Cyber Risk Coordination Efforts
ISO/IEC	Feb 2016	ISO/IEC Standards on IT, Security Techniques, Information Security Management Systems
World Bank Group	Sep 2011	World Bank Financial Infrastructure Series - General Principles for Credit Reporting
BCBS	Jun 2011	BCBS Principles for the Sound Management of Operational Risk
AICPA	Apr 2010	AICPA SOC suite of Service Organization Standards and Implementation Guidance

DIGEST DOCUMENTS (in reverse chronological order)

56. ECB (SSM) Cyber Incident Reporting Framework (2017)

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 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…" The pilot exercise has resulted in improvements to the framework including incident definitions, the reporting template, and the reporting instructions.

55. AU - Banking Exec 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.

54. 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.

53. 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.

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

"FSI Insights are written by members of the Financial Stability Institute of the Bank for International Settlements, often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of policy issues and implementation challenges faced by financial sector authorities. The views expressed in the FSI Insights are those of the authors and do not necessarily reflect the views of their respective institutions."

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", finally closing with "some policy considerations".

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

"Working Paper - Cyber Risk, Market Failures, and Financial Stability *Abstract:* Cyber-attacks on financial institutions and financial market infrastructures are becoming more common and more sophisticated. Risk awareness has been increasing, firms actively manage cyber risk and invest in cybersecurity, and to some extent transfer and pool their risks through cyber liability insurance policies. 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."

50. 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.

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

The 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."

(See UK FCA/PRA Senior Managers and Certification Regime (final rules) (Jul 2015)

48. 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."

(See "MAS Guidelines on Outsourcing (Jul 2016)" below)

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

The Cyber-security Law of the People's Republic of China (PRC) took effect on 1 June 2017. (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.

46. G7 - 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*.

45. 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.

44. 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 (see 2015 FAQs). The CAT remains "a voluntary tool that institution management may use to determine the institution's inherent risk and cybersecurity preparedness."

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

The Council 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.

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

Fast technological change is expected to have a significant impact on the existing business models of financial institutions over time. Many financial intermediaries have to deal with ageing core IT systems, hence the need for extensive IT investments, which further aggravate profitability. In addition, cyber-risk threatens data integrity and business continuity in an interconnected financial system.

Against this background, the demand for cyber-insurance is expected to grow while cyber-coverage products are still relatively new in the market, with limited underwriting experiences. Unlike other types of insurance, there is a severe lack of historical data that can be used for pricing purposes.

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.

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.

42. 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."

41. 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.

40. 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.

39. BaFin Consultation on bank regulatory reqs 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.

38. 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.

37. 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.

36. 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.

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 held at the NIST campus in Gaithersburg, Maryland.

35. 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 2016, 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."

34. HK SFC Circular on augmenting accountability of senior mgmt (Dec 2016)

HK 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-incharge (MIC), and provides guidance on selection of the MIC(s). It also brings in the roles and responsibilities of the Board of Directors.

33. 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.

32. G7 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.

31. 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.

30. 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 DoddFrank 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.

29. HK SFC Review of cybersec. 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.

28. 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.

27. 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 is deemed unique in that the 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.

26. 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."

A major message is that the 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.

25. 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 Aggregator" 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.

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

This European Union Agency for Network and Information Security (ENISA) document 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.

23. MAS Guidelines on Outsourcing (Jul 2016)

"These 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 are shared, 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."

22. 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.

21. EBA ICT risk guidelines (Jun 2016; May 2017 finalized)

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.

20. 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 instill a culture of cyber-risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber-resilience at every level within the organization;
- Cyber-resilience cannot be achieved by an FMI alone; it is a collective endeavor of the whole ecosystem.

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

This 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 (Autorit´e des march´e s 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.

18. 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.

17. 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

16. 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.

15. MAS Circular - Tech Risk and Cybersec 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.

14. 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.

13. UK FCA/PRA Senior Managers and Certification Regime (Jul 2015)

The UK FCA 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."

12. Central Bank of Israel Directive on Cyber-Defense Management (Mar 2015)

In 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 cyberdefense. 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

11. ASIC's Report on Cyber Resilience (Mar 2015)

This report by the Australian Securities & Investment Commission (ASIC) 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.

10. EBA Guidelines on Security of Internet Payments (Dec 2014)

EBA's Guidelines on Security of Internet Payments was published, with an implementation date of 1 August 2015, with the substance as consulted, i.e. a conversion of the original SecuRe Pay recommendations. 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.

9. 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.

8. 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."

7. BCBS Principles for the Sound Management of Operational Risk (Jun 2011)

These 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.

6. 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.

5. AICPA suite of SOC & Implementation Guidance (Apr 2010)

System and Organization Controls (SOC) is a suite of service offerings (independent audit reports) 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, but 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

4. ENISA National Exercises Good Practice Guide (Dec 2009)

The European Union Agency for Network and Information Security (ENISA) guide was prepared "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."

3. 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, 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.

2. KR Electronic Financial Transactions Act and Enforcement Decree (Jan 2007)

South Korea's Electronic Financial Transactions Act was enacted and enforced in January 2007. The Act (last amended May 2013) and Enforcement Decree (last amended March 2014) was 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.

1. KR Reg. on Supervision of Electronic Financial Transactions (Jan 2007)

South Korea's Regulation on Supervision of Electronic Financial Transactions, frequently amended latest being 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".

APPENDIX: INDEX by CONCEPTS

Following table lists the documents (by numbers as referenced in the Table of Contents) in which the listed concepts appear.

Concept	Digest document numbers (as listed in Table of Contents) in which the concept appears*
authorised person	11 13 18 49
best practices	3 4 7 8 10 11 17 18 19 20 22 23 24 26 27.1 27.3 30 32 35 36 36 38 40 42 45 46 49 51 52 54
business area	13 17 21 26 38 40 49
business continuity	3 4 7 8 10 11 12 13 16 17 19 20 21 22 23 24 25 26 27.1 27.3 28 30 35 36 39 41 43 44 48 49 51 52 53 54
busines operations	1 2 7 11 12 15 17 19 21 23 24 26 27.3 28 34 41 42 48 52 54
central bank	7 8 10 11 16 19 20 22 26 37 38 40 43 45 46 50 51 52
communications network	2 3 4 11 16 18 22 24 26 51 54
competent authority	4 10 16 18 19 21 22 23 24 38 40 43 45 49
conduct authority	13 19 20 27.1 38 49
control function	13 21 23 27.3 34 44 49
critical infrastructure	3 4 11 17 19 20 22 24 26 28 30 35 36 44 51 52 54
cross border	7 8 11 13 16 17 18 19 20 21 22 24 38 40 43 45 46 49 51 52
cyber attack	3 4 10 11 14 19 20 21 24 26 27.1 27.3 28 30 31 33 35 37 38 40 44 45 46 51 52 54
cyber defense	12 27.3 44 51 54
cyber event	19 20 30 31 41 44 51 52 54
cyber incident	12 19 20 24 28 30 31 32 44 46 51 53 54
cyber resilience	11 12 14 15 19 20 24 26 27.3 28 30 33 43 44 46 51 52
cyber risk	11 12 15 19 20 21 24 26 27.3 28 29 30 32 33 35 36 41 42 43 44 45 46 50 51 52 53 54

Concept	Digest document numbers (as listed in Table of Contents) in which the concept appears*
cyber security	11 19 24 35 51 52
cyber threat	6 11 12 19 20 21 24 27.1 27.2 27.3 28 29 30 31 32 35 36 37 40 43 44 45 46 48 50 51 52 54
cybersecurity framework	11 19 20 30 36 42 44 51 54
data protection	3 8 10 13 16 17 18 19 20 21 22 24 27.2 27.3 35 37 38 40 45 49 52 54
digital services	22 35 38 45
financial business	1 2 17 26 49
financial companies	1 2 25 30 43 51
financial conduct	13 19 20 27.1 38 49
financial institution	6 7 8 9 10 11 14 15 16 17 19 20 21 23 27.2 27.3 28 30 31 37 38 40 43 44 45 46 48 49 51 52
financial market	7 8 11 13 16 18 19 20 21 22 23 26 27.1 30 37 43 45 49 51 52
financial sector	7 8 11 12 19 20 22 25 26 27.1 27.3 30 32 37 38 40 43 44 45 46 49 51 52
financial services	1 2 6 7 8 11 13 16 17 19 20 21 23 25 27.1 27.2 27.3 28 29 37 38 40 41 43 44 45 46 48 49 51 52
financial stability	7 8 11 19 20 26 27.1 30 32 40 43 45 46 51 52
financial system	7 8 10 11 13 16 19 20 21 23 26 30 31 32 37 40 41 43 45 46 49 51 52
financial transactions	1 2 11 17 20 30 31 37 38 40 41 51
general principles	8 13 18 19 21 22 34 35 38 49 52 55
good practices	3 4 10 11 16 24 26 29 35 38 46 54
governing bodies	8 13 17 19 22 24 38 41 46 49 52 54
incident report	3 4 10 12 16 22 24 28 31 38 45 48 52 54
incident response	3 4 11 12 18 19 20 21 22 24 26 27.1 27.3 28 30 32 35 36 37 41 44 48 50 51 52 53 54
information security	1 2 3 4 6 8 11 12 16 17 18 19 20 22 24 26 27.1 27.2 27.3 28 29 30 31 33 35 36 37 38 39 41 42 43 44 45 47 48 50 51 52 53 54
information sharing	3 4 8 10 11 12 17 19 20 22 24 25 26 27.3 31 32 36 37 38 40 41 44 45 46 47 50 51 52 54

Concept	Digest document numbers (as listed in Table of Contents) in which the concept appears*																								
information system	3	4	7	8	11	12	17	18	19	20	22	23	24	25	26	27.2	27.3	28	30	33	35	36	40	41	44
	45	48	54																						
information technology	1	2	3	4	7	8	9	10	11	12	13	15	16	17	18	19	20	21	23	25	26	27.3	28	29	30
	32	33	34	36	39	41	42	44	48	49	51	52	54	55											
internal audit	7	12	13	17	21	23	27.3	28	30	35	39	42	44	49	50	55									
international standard	4	8	10	17	22	38	45	46	51	54															
internet payment	10	16	26	38																					
management function	7	10	12	13	21	27.3	30	44	49	51	54														
management process	3	5	7	10	11	12	13	16	17	19	20	21	23	24	26	27.1	34	36	38	39	43	44	48	49	51
	54																								
management response	2	7	13	17	20	26	36	44	47	49	52														
management system	3	7	11	12	13	17	19	21	26	27.3	36	39	44	45	47	48	49	51	52	53	54				
managing cyber	11	12	19	20	24	28	30	35	36	42	44	51	52	54											
market infrastructure	8	11	17	19	20	22	26	27.1	30	37	40	43	45	51	52										
market participants	8	10	11	19	21	30	37	40	43	45	49	51													
money laundering	8	10	11	13	16	18	27.3	31	34	37	40	45	46	49	55										
network security	3	4	11	17	19	23	39	41	47	48	54														
operational risk	7	8	11	12	16	19	20	21	22	23	26	27.3	28	30	36	37	39	40	43	51	52	54			
outsourcing arrangement	7	11	13	16	23	25	26	28	29	48	49														
payment initiation	10	16	17	38	40	45																			
payment institution	10	16	38																						
payment instrument	2	10	16	38																					
payment services	10	11	13	16	21	27.3	38	40	44	45	49														
payment transactions	2	10	16	21	37	38																			
penetration test	12	19	20	21	26	27.1	27.2	27.3	28	30	35	38	39	41	44	46	48	52	53	54					
person data	8	10	11	13	16	18	19	21	22	35	38	40	45												
practice guidance	3	4	24	26	38																				
regulated activity	13	19	23	34	38	43	49																		

Concept	Digest document numbers (as listed in Table of Contents) in which the concept appears*
reporting service	8 21 42 49
reporting system	3 7 8 12 17 21 47 51 54
response function	3 13 27.3 49 54
risk assessment	4 6 7 8 10 11 12 13 14 16 17 19 20 21 22 23 24 26 27.1 27.2 27.3 29 30 33 36
	38 39 41 42 43 44 45 47 48 51 52 53 54
risk management	5 6 7 8 9 10 11 12 13 16 17 19 20 21 22 23 24 25 26 27.1 27.2 27.3 28 30 31
	32 34 35 36 37 39 42 43 44 45 48 49 50 51 52 53 54 55
risk profile	7 11 12 13 16 19 20 21 23 26 28 30 32 37 38 40 41 44 49 51 52 54
security incident	3 4 9 10 11 12 16 17 17 18 19 21 22 24 26 27.1 27.3 38 39 44 47 48 51 52 54
security management	4 11 17 19 21 24 26 27.2 29 33 36 38 39 42 47 48 52 54
security risk	10 16 17 18 19 21 26 35 36 37 38 44 45 47 48 51 52 54
senior management	4 7 10 11 12 13 15 16 19 20 21 23 26 27.2 30 34 35 41 42 44 48 49 51 52 53
	54
service provider	2 3 4 7 8 10 11 12 13 16 17 18 19 20 21 22 23 24 25 26 27.1 27.2 27.3 28 30
	32 35 36 37 38 39 40 41 42 44 45 47 48 49 50 51 52 53
supervisory authority	7 8 10 16 18 20 21 22 26 30 40 43 45 51 52
third countries	13 16 18 22 43 45 49
third parties	2 3 4 7 8 10 11 12 13 16 17 18 19 20 21 22 23 24 25 26 27.2 27.3 28 30 32
	35 36 37 38 39 41 42 43 44 45 46 48 49 50 51 52 53 54
threat intelligence	11 19 20 24 26 27.1 27.2 27.3 29 30 36 44 50 51 52

*Some Digest items have multiple pieces, which are as follows:

DIGEST TOC ref#	TOC TITLE
27.1	UK CBEST Intelligence-Led Vulnerability Testing 2.0 (2016) - Implementation Guide
27.2	Procuring Penetration Testing Services
27.3	Threat Intelligence Framework