FSB FINANCIAL STABILITY BOARD

Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices

13 October 2017

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board
Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Executive Summary

Cyber attacks are a threat to the entire financial system. The changing nature of, and growth in, cyber risk to financial institutions is driven by several factors, including evolving technology; interconnections among financial institutions and between financial institutions and other external parties; determined efforts by cyber criminals to find new methods to attack and compromise information and communications technology (IT) systems; and the attractiveness of financial institutions as targets for cyber criminals seeking illicit financial gains. Authorities across the globe have taken regulatory and supervisory steps designed to facilitate both the mitigation of cyber risk by financial institutions, and their effective response to, and recovery from, cyber attacks.

This is a report of an FSB stocktake of existing publicly available regulations and supervisory practices with respect to cybersecurity in the financial sector, as well as of existing international guidance. The G20 Finance Ministers and Central Bank Governors (Ministers and Governors) requested the FSB stocktake and report at a March 2017 meeting in Baden-Baden.[1] The report is based on responses of FSB member jurisdictions and international bodies to a survey undertaken by the FSB in the spring of 2017. All 25 FSB member jurisdictions responded to the survey.[2] In addition, nine international body members and the G7 Cyber Expert Group submitted survey responses.[3]

The report includes information concerning jurisdictions' self-reported existing publicly released regulations, guidance and supervisory practices; future plans; and views regarding effective regulatory and supervisory practices.[4] The report also contains information regarding international bodies' self-reported guidance, other publications and future plans. It also includes three Annexes, namely, Additional Tables containing survey responses (Annex A), a Glossary of existing international guidance and standards (Annex B) and narrative summaries of each individual jurisdiction's response to the FSB survey (Annex C).

The conclusions from the stocktake include the following.

FSB member jurisdictions have been active in addressing cybersecurity for the financial sector. All 25 member jurisdictions report that they have publicly released regulations or guidance that address cybersecurity for at least a part of the financial sector, and a majority have also publicly released supervisory practices. All or nearly all jurisdictions have addressed

---

1 See http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

2 The FSB member jurisdictions are Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

3 This includes the Basel Committee on Banking Supervision, Committee on the Global Financial System, Committee on Payments and Market Infrastructures, International Association of Insurance Supervisors, International Accounting Standards Board, International Monetary Fund, International Organization of Securities Commissions, Organisation for Economic Co-Operation and Development and the World Bank.

4 For purposes of the FSB survey, generally "regulations and guidance" were defined as materials that impose requirements on, or provide guidance for, regulated entities; and "supervisory practices" were defined as practices that supervisory authorities or regulators use in their oversight or examination of regulated entities.

banks and financial market infrastructures (FMIs), and a majority have addressed trading venues, insurance companies, broker-dealers and asset managers.

FSB member jurisdictions report a significantly higher number of publicly released regulatory schemes than publicly released supervisory practices schemes. It is important to note, however, that some supervisory practices may not have been publicly released, and therefore were out of scope of the stocktake.

International bodies also have been active in addressing cybersecurity for the financial sector. The 10 international bodies that responded to the FSB survey reported published guidance covering electronic banking; FMIs; firms and supervisory and regulatory authorities throughout the financial sector; critical information infrastructures, including financial sector actors that are critical information infrastructures; and all economic and social activities, across all sectors, from businesses, governments and individuals.

All FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cybersecurity regulatory and supervisory schemes for the financial sector. This suggests that jurisdictions have found the existing guidance and standards to be useful and that there is some degree of international convergence in cybersecurity regulation and supervision of the financial sector.

The number of schemes of regulations and guidance addressing cybersecurity for the financial sector varied widely across jurisdictions. All member jurisdictions reported at least one regulatory scheme, with some reporting as many as 10. It is difficult to draw particular conclusions from the number of schemes reported. For example, there was no direct correlation between the number of schemes reported by a jurisdiction and the financial subsectors covered.

Jurisdictions reported that their regulatory schemes more commonly took a targeted approach to cybersecurity and/or IT risk (66% of reported schemes) and less commonly addressed operational risk generally (34% of reported schemes). By financial subsector, the percentage of reported regulatory schemes targeted to cybersecurity and/or IT risk ranged from a high of 83% for trading venues to a low of 60% for asset managers. For FMIs and banks, the percentages of reported targeted regulatory schemes were 77% and 71%, respectively.

Regulatory schemes categorised by jurisdictions as addressing operational risk often were characterised as principles-based, risk-based or proportional and specified the objectives to be met by regulated institutions. Nonetheless, many operational risk schemes enumerated a number of elements to be addressed by regulated institutions, commonly including **governance; risk assessment and risk management; policies, procedures and controls; prevention, detection and reduction of vulnerability; protection of information; security tests; backup sites and disaster recovery; business continuity planning; notice to regulators; independent review; and third-party risks.**

There were 56 schemes of regulations and guidance reported as targeted to cybersecurity and/or IT risk, which covered a variety of content elements. Some of the elements covered by those schemes, listed in descending order by the number of schemes in which they were included, are risk assessment (55); regulatory reporting (50); role of the board (49); third-party interconnections (49); system access controls (48); incident recovery (46); testing (44); training (43); creation of role responsible for cybersecurity, such as chief information security officer

(38); information sharing (31); expertise of the board or senior management (22); and cyber risk insurance (15).

There were 35 schemes of reported supervisory practices, which covered a variety of content elements. Some of the elements covered by those schemes, listed in descending order by the number of schemes in which they were included, are review of policies and procedures (32); review of programmes for monitoring, testing and auditing (31); review of data security controls (31); review of governance arrangements (30); review of risk assessment process (30); review of past incidents and organisation's response and recovery (27); testing by supervisor and/or submission of test results to supervisor (21); communications by supervisor (21); review of sectoral impact of past incidents (21); information sharing by financial institutions (18); expertise of supervisory team (17); supervisory review of third parties (16); and joint public-private testing (14).

There are a number of similarities across international guidance, with many of the same topics addressed, even though there are considerable differences in the scope of entities covered and date of issuance of the guidance. Common topics addressed include governance; risk analysis and assessment; information security; security controls and incident prevention; expertise and training; monitoring, testing and/or auditing; incident response and recovery; communications and information sharing; oversight of interconnections; and continuous learning.

Jurisdictions remain active in the area of cybersecurity. Seventy-two per cent of jurisdictions reported publicly released plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year. These plans include engaging FMIs in a self-assessment exercise, developing a cybersecurity strategy and guidance for the financial sector and issuing new cybersecurity regulation.

Jurisdictions provided a wide range of responses when asked to cite practices that they deem effective in addressing cybersecurity through regulations, guidance and/or supervisory practices. Some items commonly cited were: specific, existing international guidance and standards; principle-based, risk-based or proportional supervision; the important role of the board and senior management; and communications, coordination and information sharing. Other items cited include independence of risk management, policies and procedures concerning information systems management, identification and updating of cybersecurity requirements, strong control of outsourcing risks, assessment of cross-border and cross-sector threats and systemic risk, and a number of specific supervisory tools.

Box 1: What are Cybersecurity and Cyber Resilience?

Here are some definitions reported by FSB members.

Cybersecurity:

Argentina. "A cycle composed by 5 related and integrated information security processes: awareness, access control, integrity and register, control and monitoring, incident management".

China. "Using of technology and management to ensure the usability, confidentiality, intactness and non-repudiation of information during collection, transit, exchange and storage. Cybersecurity includes internet security, system security and content security, which covers all levels of security, i.e. physical circumstances, internet, mainframe system, desktop system, data, application, storage, disaster back-up, security management and personnel".

Hong Kong. "The ability to protect or defend against cyber attacks, which refer to attacks that target an institution's IT systems and networks with an aim to disrupt, disable, destroy or maliciously control an IT system/network, to destroy the integrity of the institution's data, or to steal information from it".

India. "Measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber attack and to continue operation during, and recover from, a cyber attack".

Italy. "The set of controls and organizational measures and means (human, technical, etc.) used to protect information systems assets and communication networks against all non-physical attacks, irrespectively of the attack being initiated through a physical or logical security breach".

Saudi Arabia. "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats".

Cyber resilience:

CPMI-IOSCO. "An FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber attack".

Australia. "The ability to prepare for, respond to and recover from a cyber attack. Cybersecurity is the praxis of protecting digital assets from connected threats. Resilience is more than just preventing or responding to an attack – it also takes into account the ability to operate during, and to adapt and recover, from such an event".

1. Regulations, guidance and supervisory practices in FSB member jurisdictions

1.1 Introduction

This Section describes publicly released regulations, guidance and supervisory practices in FSB member jurisdictions that address cybersecurity for the financial sector. FSB member jurisdictions have been active in this area and have plans to continue in the future. The FSB survey was limited in scope to publicly released materials issued by government authorities. Non-public information, such as supervisory practices that are used but not publicly released, is not covered by this report. In addition, the survey did not cover any guidance, supervisory practices or similar materials that may have been issued by self-regulatory organisations or in some jurisdictions by local authorities (such as states). As a result, particularly in the area of supervisory practices, the report may give an incomplete picture of practices actually in use within jurisdictions. The information on regulatory schemes and supervisory practices set out in this Section should also be considered in the context of the different regulatory and business environments of each individual jurisdiction.

All 25 member jurisdictions report that they have publicly released regulations or guidance that address cybersecurity for at least a part of the financial sector, and a majority have also publicly released supervisory practices. All or nearly all jurisdictions have addressed banks and FMIs, and a majority have addressed trading venues, insurance companies, broker-dealers and asset managers. In the FSB survey, members reported significantly more publicly released materials with respect to regulations and guidance than supervisory practices. Lower reported publication activity in the area of supervisory practices, however, does not necessarily equate to an actual lower level of supervisory activity. Supervisory practices that have not been publicly released were out of scope of the stocktake and are therefore not reflected in this report. A majority of jurisdictions reported near-term plans for continuing activity in the areas of regulation and supervision of cybersecurity for the financial sector.

Figure 1, below, provides aggregate data regarding publicly available cybersecurity regulations, guidance and supervisory practices reported by member jurisdictions for financial subsectors. Table 1 provides summary information regarding existing activity and future plans for each jurisdiction.

Figure 1: Number of Jurisdictions Reporting Regulatory or Supervisory Schemes, by Sector

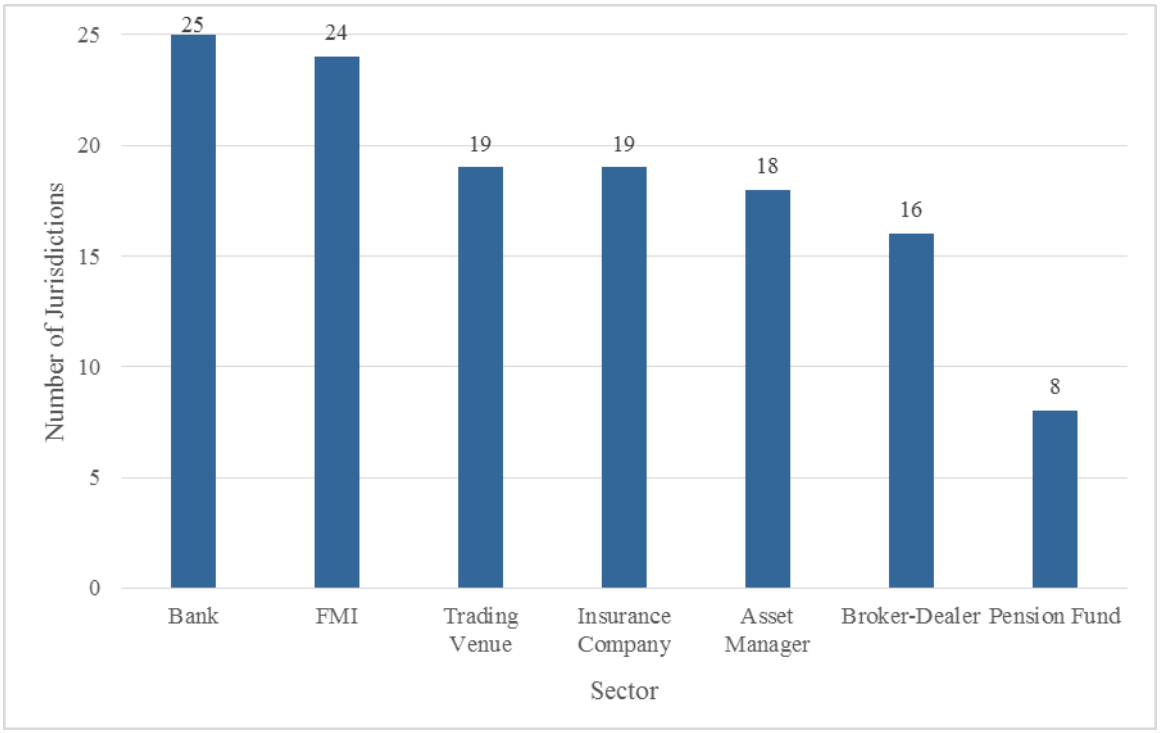


Table 1: Summary Reported Publicly Available Information by Jurisdiction

Jurisdiction	National Strategy	Regulations/Guidance							Supervisory Practices							Future Plans
		FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.	FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.	
Argentina		■		■							■					✓
Australia	✓	■	■	■	■	■	■	■	■							✓
Brazil	✓	■	■	■	■	■	■							■		✓
Canada	✓	■	■	■	■	■	■									
China	✓	■	■	■	■	■	■			■	■		■	■		✓
European Union	✓	■	■	■	■	■					■					✓
France	✓	■	■	■	■	■	■	■	■		■	■				✓
Germany	✓	■	■	■	■	■	■	■								✓
Hong Kong	✓	■		■	■	■	■		■		■		■	■		✓
India	✓	■	■	■	■						■					✓
Indonesia		■		■		■	■		■		■		■			
Italy	✓	■	■	■	■		■		■	■						✓
Japan	✓	■	■	■	■	■	■		■	■	■	■	■			
Korea		■	■	■	■		■		■	■	■	■		■		
Mexico		■	■	■	■	■	■	■	■	■	■	■	■	■		✓
Netherlands	✓	■									■	■		■	■	✓
Russia	✓	■	■	■							■					✓
Saudi Arabia		■		■	■											✓
Singapore	✓	■	■	■	■	■	■		■	■	■	■	■	■		✓
South Africa	✓			■												✓
Spain	✓	■	■	■												✓
Switzerland	✓	■	■	■	■	■	■									
Turkey	✓	■	■	■		■	■	■	■	■	■		■	■	■	
United Kingdom	✓	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
United States	✓	■	■	■	■	■	■	■	■	■	■	■	■	■	■	✓
Total	**20**	**24**	**19**	**24**	**18**	**16**	**17**	**7**	**12**	**9**	**16**	**8**	**9**	**10**	**4**	**18**

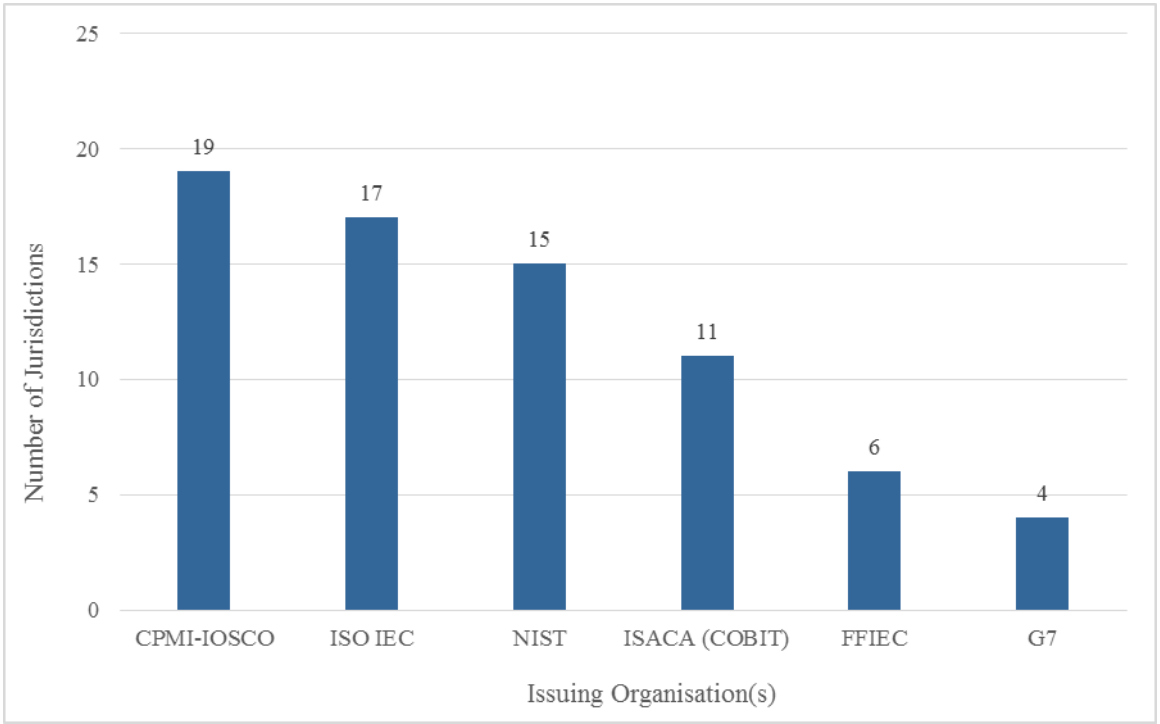
■ Jurisdictions with coverage

Blank cell indicates no coverage

In developing their cybersecurity regulatory and supervisory schemes for the financial sector, all FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies. Some examples are the *Guidance on cyber resilience for financial market infrastructures* published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO Guidance), the US National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), and the International Organization for Standardization 27000 series, which provides information security control standards. This suggests that jurisdictions have found the existing guidance and standards to be useful in developing their own schemes and that there is some degree of international convergence in cybersecurity regulation and supervision of the financial sector.

Figure 2, below, provides aggregate data on jurisdictions' self-reported use of existing guidance and standards. The data reflects jurisdiction responses to questions about whether regulations, guidance and supervisory practices **incorporate** existing national or international guidance or standards. The data does not capture every instance where a jurisdiction has in place regulations, guidance or supervisory practices that are similar to, or generally aligned with, such existing guidance or standards. Table 6, contained in Annex A, contains a breakdown of this information by jurisdiction. Annex B provides a brief description of the referenced national and international guidance and standards.

Figure 2: Aggregate Data on Jurisdiction Use of Existing Guidance and Standards



Box 2: National Cybersecurity Strategies

As reflected in Table 1, above, 20 FSB member jurisdictions reported that, in addition to regulatory or supervisory schemes for the financial sector, the jurisdictions had released national cybersecurity strategies, policies or frameworks for the jurisdiction that apply more broadly.

Many of these jurisdictions reported strategies that fell into a small number of thematic areas. Predominant themes include: defence; education; growth and innovation; partnerships and collaboration; and working with international partners.

Defence. A significant proportion of the reported strategies address national defence against the cyber threat. Often, jurisdictions specified action to secure government systems and critical national infrastructures.

Education. Many jurisdictions reported strategies that cover education. Often, this was specifically reported in relation to increasing citizens' awareness of cyber issues.

Growth and Innovation. Several jurisdictions covered growth and innovation, research and development, and science and technology. One jurisdiction set out the aspiration to have a pipeline of talent to meet the national need across both the public and private sectors and expertise to meet and overcome future threats and challenges.

Partnerships and Collaboration. The importance of effective partnerships and collaboration was highlighted by a number of jurisdictions. A frequently reported focus in this area was on public-private partnerships. One jurisdiction presents partnerships as the means to secure vital cyber systems outside the federal government. Another jurisdiction outlines action to create a platform for information sharing on the basis of mutual trust.

Working with International Partners. Many jurisdictions outlined action relating to working with international partners. One jurisdiction reported a specific strategy focused on international cooperation. One jurisdiction noted the importance of international action to enhance collective security. Another jurisdiction specifically reported action to strengthen international law enforcement.

1.2 Reported regulations, guidance and supervisory practices

The 25 FSB member jurisdictions reported 85 schemes of publicly released regulations and guidance (also referred to in this report as "regulatory schemes") and 35 schemes of publicly released supervisory practices. For purposes of the FSB survey, generally "regulations and guidance" were defined as materials that impose requirements on, or provide guidance for, regulated entities; and "supervisory practices" were defined as practices that supervisory authorities or regulators use in their oversight or examination of regulated entities. Annex C contains brief narrative descriptions for each jurisdiction of the reported schemes of regulations, guidance and supervisory practices.

All jurisdictions reported at least one scheme of publicly released regulations and guidance, while six jurisdictions reported no publicly released schemes of supervisory practices. The numbers of schemes of regulations and guidance per jurisdiction ranged from as little as one to as many as 10. Jurisdictions were asked to use their best judgment in determining what to report as separate schemes and what to report as a single scheme. For that reason, it is difficult to draw particular conclusions from the number of schemes reported. For example, there was no direct correlation between the number of schemes reported by a jurisdiction and the financial subsectors covered.

All jurisdictions reported having either regulations and guidance or supervisory practices that address cybersecurity for banks, and 24 jurisdictions reported addressing FMIs. The lowest reported coverage was with respect to pension funds, with respect to which eight jurisdictions reported regulations and guidance or supervisory practices.

Tables 2 and 3, below, provide combined data, by jurisdiction, for regulations and guidance and supervisory practices. Table 2 shows the subsectors covered by either regulations and guidance schemes, supervisory practices schemes or both in each jurisdiction, together with the number of schemes. Table 3 presents the subsectors reported as not covered in member jurisdictions.

Table 2: Regulatory and Supervisory Schemes, by Jurisdiction

Jurisdiction	Number of Schemes		Sector						
	Regulations / Guidance	Supervisory Practices	FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.
Argentina	1	1	■		■				
Australia	3	1	■	■	■	■	■	■	■
Brazil	4	1	■	■	■	■	■	■	
Canada	3	0	■	■	■	■	■	■	
China	6	2	■	■	■	■	■	■	
European Union	10	2	■	■	■	■	■		
France	2	1	■	■	■	■	■	■	■
Germany	7	0	■	■	■	■	■	■	■
Hong Kong	3	2	■		■	■	■	■	
India	3	1	■	■	■	■			
Indonesia	4	2	■		■		■	■	
Italy	7	2	■	■	■	■		■	
Japan	1	1	■	■	■	■	■	■	
Korea	1	1	■	■	■	■		■	
Mexico	5	3	■	■	■	■	■	■	■
Netherlands	1	1	■		■	■		■	■
Russia	1	1	■	■	■				
Saudi Arabia	1	0	■		■	■			
Singapore	1	1	■	■	■	■	■	■	
South Africa	1	0			■				
Spain	1	0	■	■	■				
Switzerland	3	0	■	■	■	■	■	■	
Turkey	3	4	■	■	■		■	■	■
United Kingdom	3	3	■	■	■	■	■	■	■
United States	10	5	■	■	■	■	■	■	■
Total	**85**	**35**	**24**	**19**	**25**	**19**	**16**	**18**	**8**

■ Jurisdictions with coverage

Blank cell indicates no coverage

Table 3: Subsectors Not Covered, by Jurisdiction

Jurisdiction	Sector						
	FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.
Argentina		■		■	■	■	■
Australia							
Brazil							■
Canada							■
China							■
European Union						■	■
France							
Germany							
Hong Kong		■					■
India					■	■	■
Indonesia		■		■			■
Italy					■		■
Japan							■
Korea					■		■
Mexico							
Netherlands		■			■		
Russia				■	■	■	■
Saudi Arabia		■			■	■	■
Singapore							■
South Africa	■	■		■	■	■	■
Spain				■	■	■	■
Switzerland							■
Turkey				■			
United Kingdom							
United States							
Total	1	6	0	6	9	7	17

■ Jurisdictions with no coverage

Blank cell indicates coverage

1.2.1 Regulations and guidance generally

As noted above, FSB member jurisdictions reported 85 schemes of regulations and guidance. Nearly all of these schemes (79) have been published in final form, with six published only in draft form. Of the 79 final regulatory schemes that are in place, jurisdictions reported that draft amendments or other elaborations have been published for nine. Basic information for each of the 85 regulatory and guidance schemes is summarised in Table 4, below, with aggregate information about final and draft status in Figure 3, below.

Table 4: Summary of Individual Regulatory Schemes

Note: "Other" includes types of entities not captured by the preceding categories, e.g. other credit providers, payment service providers and credit rating agencies.

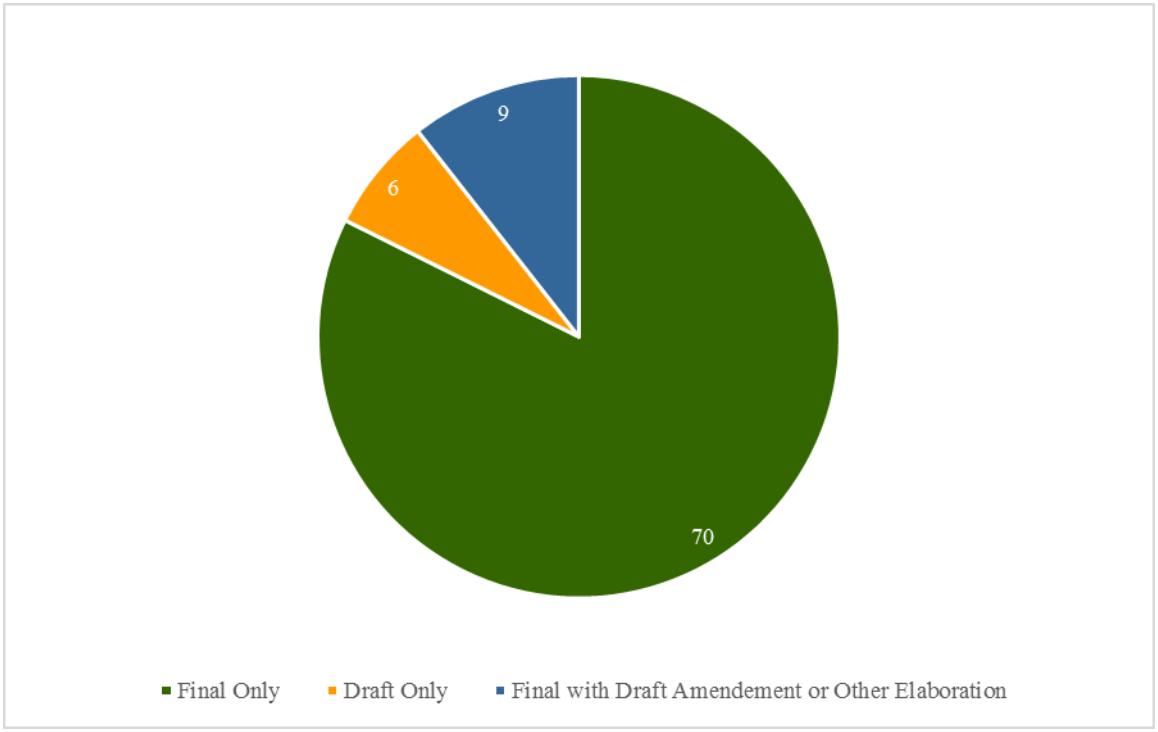
Jurisdiction/Scheme	Targeted to Cyber	General Op. Risk	Final	Draft	Sector							
					FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.	Other
Argentina	✓		✓		■		■					
Australia 1	✓		✓				■	■			■	■
Australia 2	✓		✓		■	■	■	■	■	■	■	■
Australia 3		✓	✓		■							
Brazil 1		✓	✓				■		■			■
Brazil 2		✓	✓		■	■				■		■
Brazil 3		✓	✓					■				■
Brazil 4		✓	✓		■							
Canada 1	✓		✓		■	■			■	■		■
Canada 2	✓		✓		■	■						
Canada 3	✓		✓				■	■				■
China 1	✓		✓		■	■	■	■				
China 2	✓		✓		■		■					
China 3	✓		✓				■					
China 4	✓		✓			■			■	■		■
China 5	✓		✓				■					
China 6	✓			✓				■				
European Union 1		✓	✓									■
European Union 2	✓		✓									■
European Union 3	✓		✓		■							
European Union 4		✓	✓		■							
European Union 5	✓		✓		■							
European Union 6		✓	✓					■				
European Union 7	✓		✓									■
European Union 8	✓		✓		■							
European Union 9	✓		✓		■	■			■			■
European Union 10	✓			✓			■					■
France 1		✓	✓		■	■	■	■	■	■	■	■
France 2	✓		✓				■	■				■
Germany 1	✓		✓		■	■	■	■			■	■
Germany 2		✓	✓				■					
Germany 3		✓	✓				■					
Germany 4	✓			✓			■					
Germany 5		✓	✓				■					■
Germany 6		✓	✓					■			■	
Germany 7		✓	✓						■	■		
Hong Kong 1	✓		✓		■		■					■
Hong Kong 2		✓	✓					■				
Hong Kong 3		✓	✓						■	■		
India 1	✓		✓					■				
India 2	✓		✓				■					
India 3	✓		✓		■	■						
Indonesia 1		✓	✓				■					
Indonesia 2		✓	✓		■				■	■		
Indonesia 3		✓	✓		■		■					■
Indonesia 4	✓		✓									■
Italy 1	✓		✓		■							■
Italy 2	✓		✓		■							■

Jurisdiction/Scheme	Targeted to Cyber	General Op. Risk	Final	Draft	Sector							
					FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.	Other
Italy 3	✓		✓				■					
Italy 4	✓		✓									■
Italy 5		✓	✓							■		
Italy 6	✓		✓			■						■
Italy 7		✓	✓					■				
Japan	✓		✓		■	■	■	■	■	■		
Korea	✓		✓		■	■	■	■		■		
Mexico 1	✓		✓		■	■	■		■	■		■
Mexico 2	✓			✓			■	■	■	■	■	
Mexico 3	✓		✓				■					
Mexico 4	✓		✓									■
Mexico 5		✓	✓					■				■
Netherlands	✓		✓		■							
Russia	✓		✓		■	■	■					
Saudi Arabia	✓		✓		■		■	■				■
Singapore	✓		✓		■	■	■	■	■	■		■
South Africa	✓		✓				■					
Spain		✓	✓		■	■	■					
Switzerland 1	✓		✓		■	■	■		■			■
Switzerland 2		✓	✓							■		■
Switzerland 3		✓	✓					■				■
Turkey 1	✓		✓				■					
Turkey 2	✓		✓		■							
Turkey 3	✓			✓	■	■			■	■	■	
United Kingdom 1	✓		✓		■							
United Kingdom 2		✓	✓				■					■
United Kingdom 3		✓	✓			■	■	■	■	■	■	■
United States 1	✓		✓		■	■						■
United States 2		✓	✓				■		■			
United States 3	✓		✓		■							■
United States 4	✓		✓				■					■
United States 5	✓			✓				■				■
United States 6		✓	✓		■							
United States 7	✓		✓							■		■
United States 8	✓		✓		■	■			■			■
United States 9	✓		✓						■	■		■
United States 10	✓		✓		■	■			■	■	■	■
Total	**56**	**29**	**79**	**6**	**39**	**23**	**38**	**23**	**20**	**20**	**9**	**42**

■ Jurisdictions with coverage

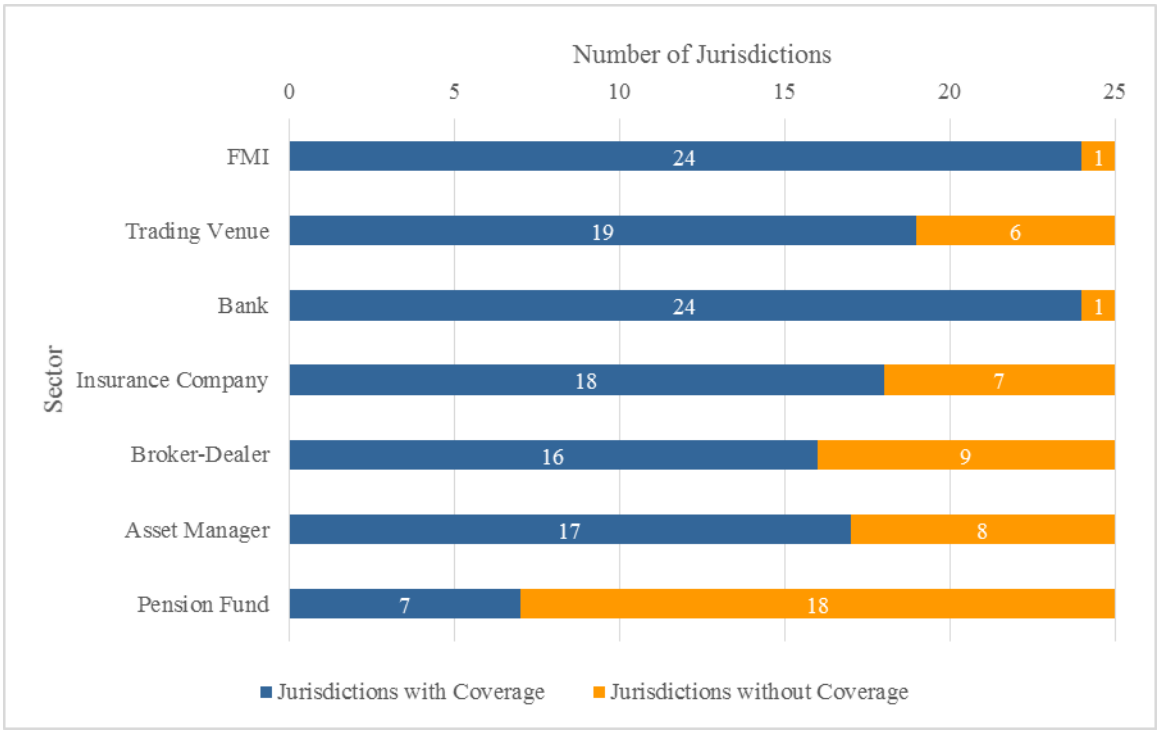
Blank cell indicates no coverage

Figure 3: Number of Regulatory Schemes in Final or Draft Form



Nearly all jurisdictions reported schemes of regulations and guidance for banks and FMIs, with a majority of jurisdictions covering insurance companies, trading venues, asset managers and broker-dealers. Seven jurisdictions reported regulatory and guidance schemes for pension funds. This data is reflected in Figure 4, below.

Figure 4: Number of Jurisdictions with Regulatory Schemes, by Sector



The survey requested that jurisdictions characterise their regulatory and guidance schemes as either: (i) addressing operational risk generally; or (ii) targeted to cybersecurity and/or IT risk. Overall, 29 schemes (34%) were reported as addressing operational risk generally, and 56 schemes (66%) were reported as targeted to cybersecurity and/or IT risk. By sector, trading venues (83%) and FMIs (77%) had the highest reported percentages of regulatory and guidance schemes targeted to cybersecurity and/or IT risk, while broker-dealers (65%), insurance companies (61%) and asset managers (60%) had the lowest reported percentages of regulatory and guidance schemes targeted to cybersecurity and/or IT risk. This information is reported in Figures 5 and 6, below.

Figure 5: Percentage of Targeted and Operational Risk Regulatory Schemes, by Sector

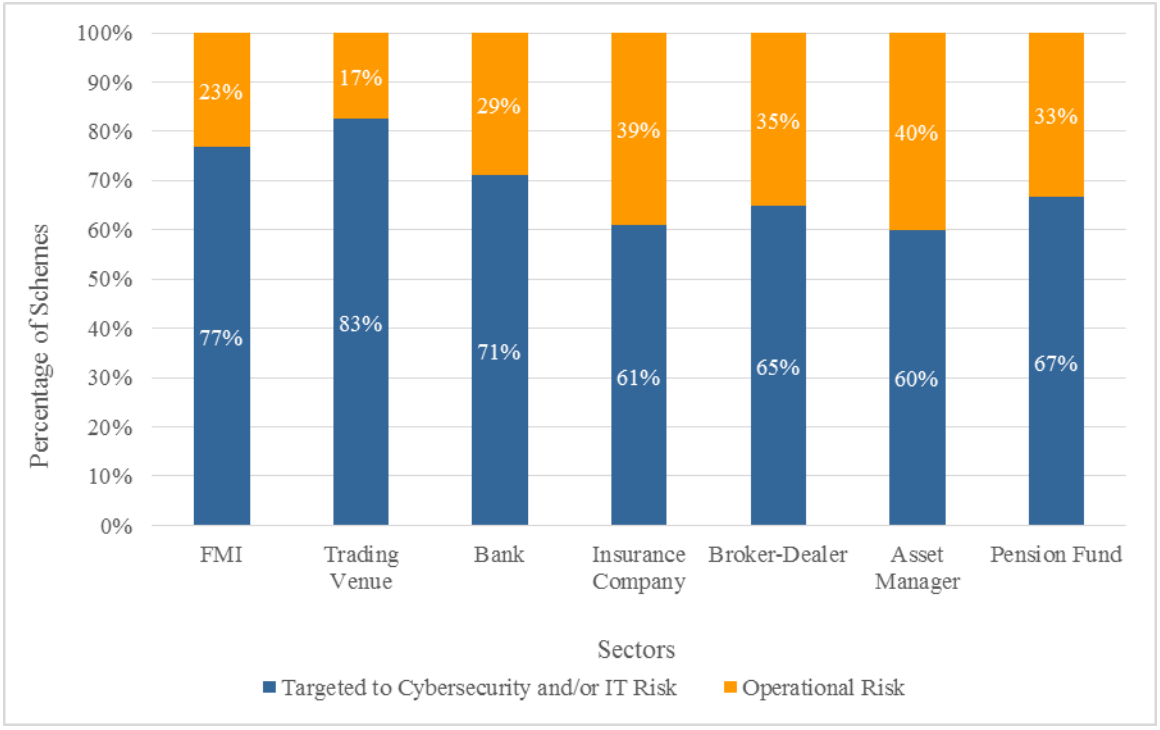
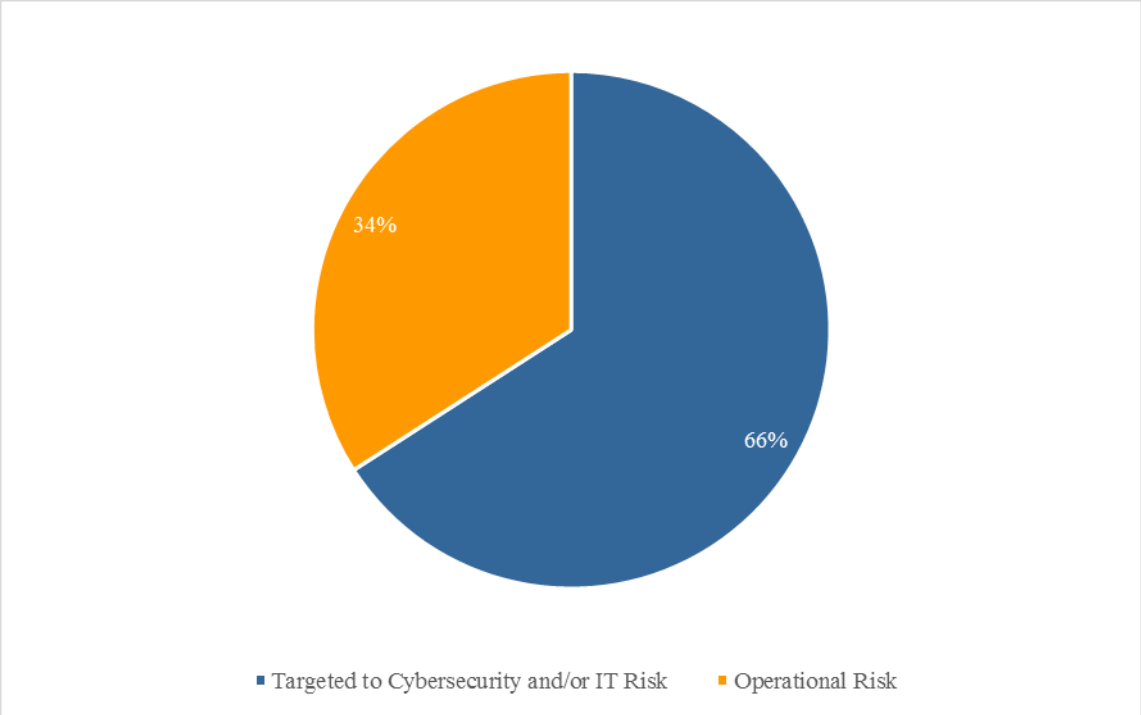
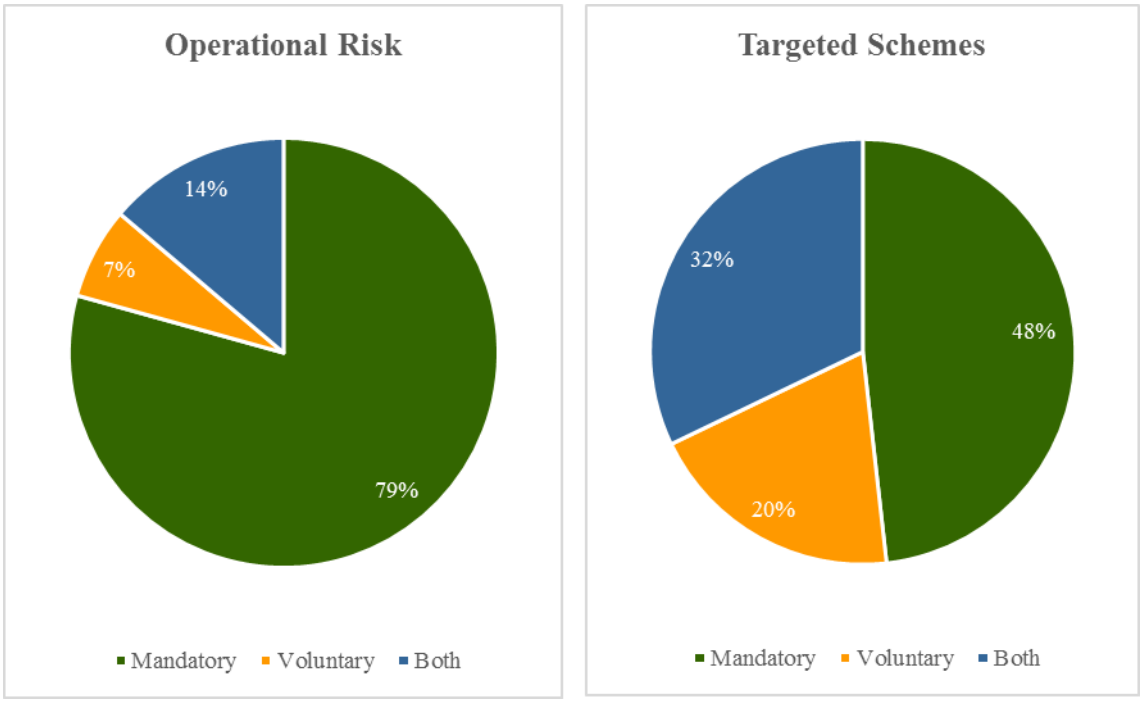


Figure 6: Aggregate Percentage of Targeted and Operational Risk Schemes



The survey also asked jurisdictions whether their schemes of regulations/guidance impose mandatory requirements, provide voluntary guidance or both. Almost all operational risk schemes were mandatory only (23 of 29, 79%) or combined mandatory requirements and voluntary guidance (4 of 29, 14%), with only two (7%) operational risk schemes reported as voluntary guidance only. The mandatory/voluntary character of schemes targeted to cybersecurity and/or IT risk was more mixed. Twenty-seven of 56 (48%) were reported as mandatory only, 18 of 56 (32%) were reported to combine mandatory requirements and voluntary guidance, and 11 (20%) were reported as voluntary guidance only.

Figure 7: Percentage of Mandatory and Voluntary Schemes



1.2.2 Regulations and guidance that address operational risk

Regulatory schemes categorised by jurisdictions as addressing operational risk often were characterised as principles-based or proportional and specified the objectives to be met by regulated institutions. For example, one principles-based scheme specifies that control of information systems shall ensure that regular assessments of information systems security are carried out and corrective action is taken where appropriate; backup procedures are available to allow business operations to continue in the event of serious systems failure; and, in any event, the integrity and confidentiality of information is preserved. Another principles-based scheme provides institutions discretion while implementing adequate and effective controls, reflecting the principle of proportionality which takes account of institution-specific risks, the complexity of an institution's business model and the nature and scale of its business. Another jurisdiction reported that its scheme requires that institutions conduct continuous review and maintenance of IT systems and processes to ensure proper operational upkeep. Another scheme reported to be principles-based is focused on the efficiency and effectiveness of the institution's information systems, namely, that the systems are adequate to the risks; that data be available, reliable and stored with adequate granularity; and that information security be assured. Another principles-based scheme provides that financial sector institutions should take reasonable steps to ensure continuity and regularity in the performance of their regulated activities and have effective processes and internal control mechanisms in respect to information processing systems.

Nonetheless, many operational risk schemes enumerated a number of elements to be addressed by regulated institutions. **Governance**, including the role of the board and senior management, was mentioned in a number of instances. For example, one scheme provides that governance arrangements should ensure that the risk management and internal control functions have

sufficient authority, independence, resources and access to the board, including a separate and independent internal audit function. Another scheme provides that an institution shall implement a system of reporting to senior management that provides operational risk reports to relevant functions within the institution. Another scheme provides for active supervision by the board. Yet another scheme calls for robust governance arrangements, including a clear organisational structure with well defined, transparent and consistent lines of responsibility, as well as a business strategy supported by a well-articulated and measurable statement of risk appetite that is clearly owned, approved and actively used by the board to monitor and control risks and to inform key business decisions.

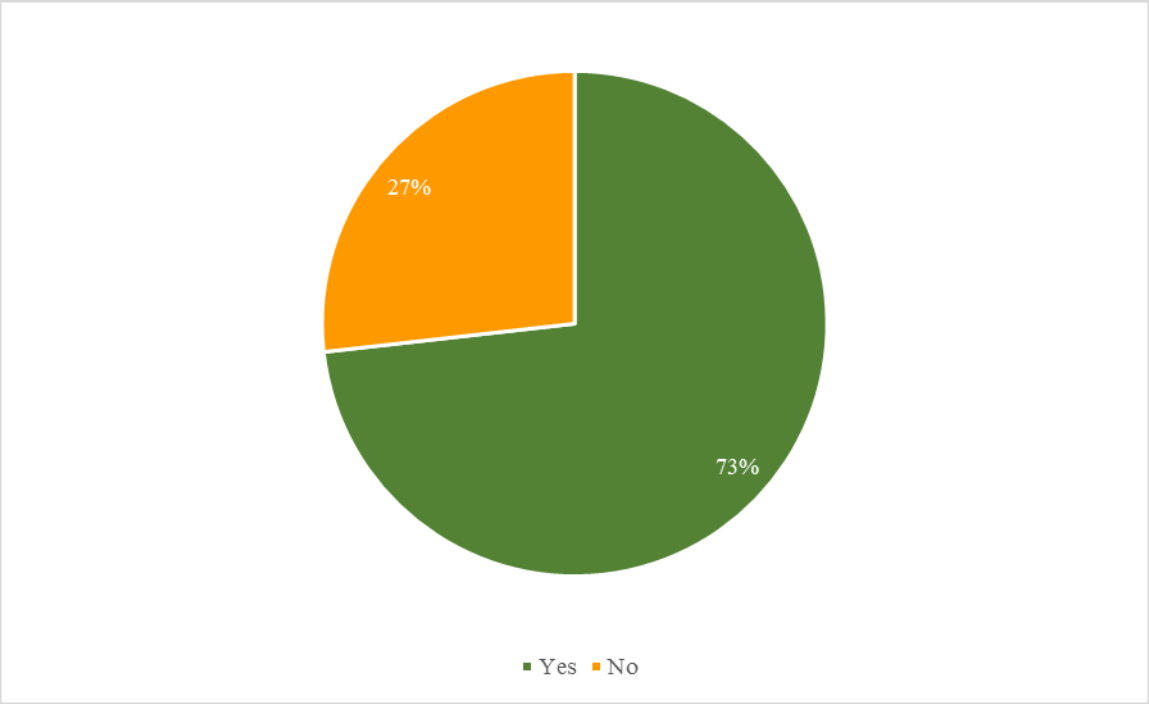
Risk Assessment and Risk Management are frequently mentioned elements of operational risk schemes. One scheme calls for a risk management framework that adequately addresses operational risk events and, more specifically, flaws in systems, processes or infrastructures related to IT. Another scheme requires adequate and effective risk management, including suitable IT resources and adequate contingency plans for IT systems. Another scheme requires risk assessment of critical infrastructures covering both physical and cybersecurity risks. One scheme requires that both operational risks and loss events related to operational risk, including risks and events related to IT and cyber risk, be identified and analysed. Another scheme sets out that firms should have robust frameworks for risk management and financial and operational control, commensurate with the nature, scale and complexity of their business, and consistent with their safety and soundness.

Other elements commonly covered in operational risk schemes include establishment of **policies, procedures and controls** to address operational risk; **prevention, detection and reduction of vulnerability** to digital attacks; **protection of information**, including confidential information; **security tests** for information systems; **backup sites and disaster recovery**, sometimes with specified recovery time objectives; **business continuity planning**; **notice to regulators** of operational risk events; **independent review** of operating procedures and systems; and **third-party risks**.

1.2.3 Regulations and guidance targeted to cybersecurity and/or IT risk

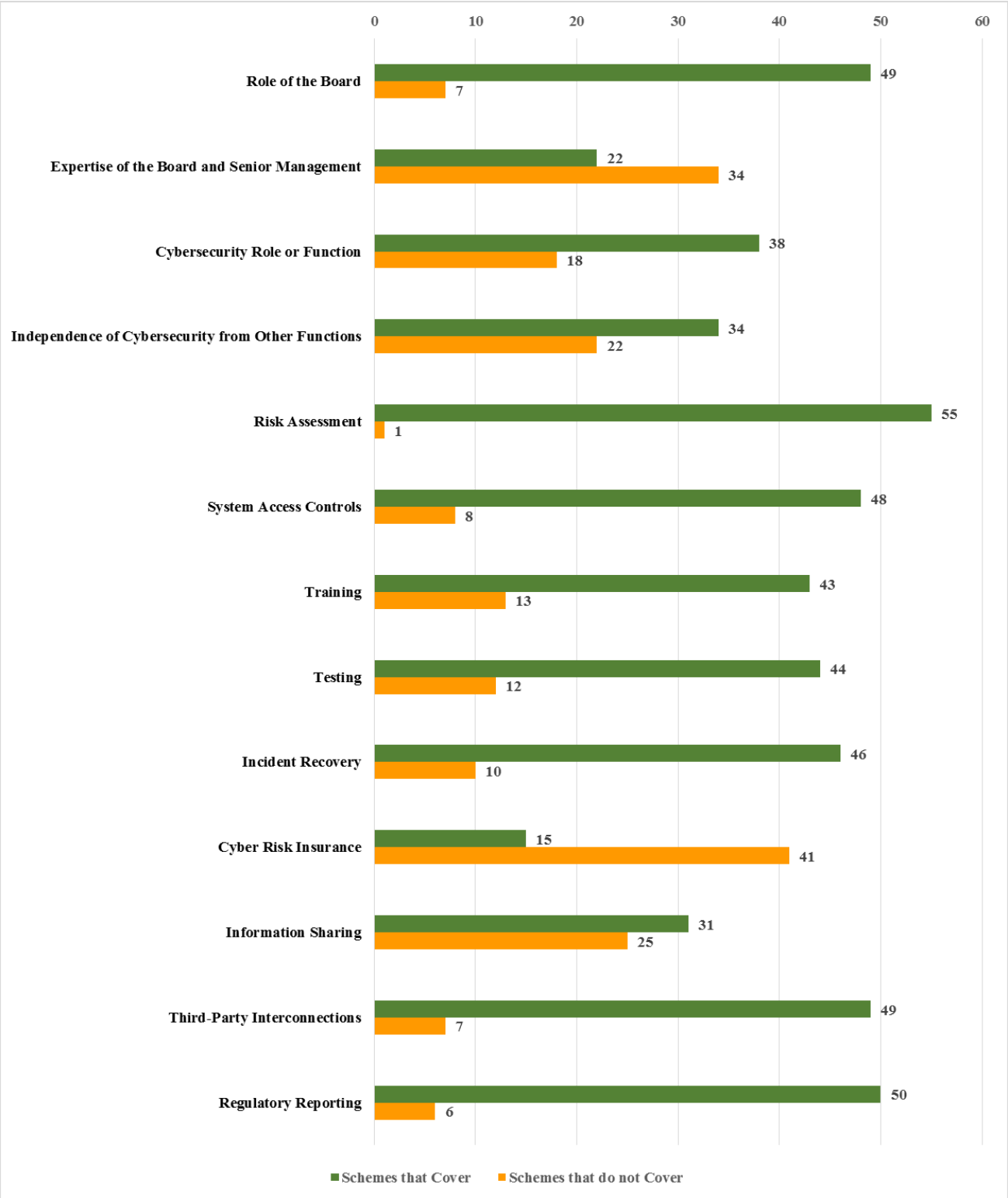
For the 56 regulatory and guidance schemes that were identified as targeted to cybersecurity and/or IT risk, jurisdictions were asked to identify whether the schemes incorporated any existing national or international guidance or standards of public authorities or private bodies. Forty-one (73%) of the targeted schemes were reported to incorporate such existing guidance or standards. This is reflected in Figure 8, below.

Figure 8: Percentage of Regulatory Schemes that Incorporate Existing Guidance



For the 56 regulatory and guidance schemes that were identified as targeted to cybersecurity and/or IT risk, jurisdictions were asked whether or not the schemes addressed a number of specific content elements. Table 7, contained in Annex A, indicates the number of yes and no responses received for each content element. Figure 9, below, provides the information for a subset of those elements.

Figure 9: Number of Targeted Regulatory Schemes that Cover Certain Topics



The following discussion elaborates on the information provided in Figure 9.

Role and Expertise of Board and Senior Management. A significant majority of schemes (49 of 56) address the cybersecurity role of the board of directors or other body responsible for general oversight of the financial institution. Some matters covered include approval of framework for cybersecurity policy and strategy; board accountability for delegated functions; information required to be furnished to the board; risk management role; and assignment of sufficient human, technological and financial resources. By contrast, less than half of the schemes (22 of 56) address the expertise of the board or senior management. Those that address board expertise cover, among other things, board ability to ask risk and audit committees relevant questions and engagement of experts by the board, as well as board training about cyber risk.

Cybersecurity Role. Thirty-eight of 56 schemes address the creation of a role or function responsible for cybersecurity, such as a chief information security officer (CISO). This role is often mandated. Thirty-four of the schemes address the independence of the cybersecurity function from other business functions.

Risk Assessment. This element is nearly universal, with 55 of 56 schemes reported to address risk assessment. Some topics covered include identification of reasonable and foreseeable cyber threats, likelihood and impact; continuous monitoring and the use of data analytics; annual independent system review by qualified party; hardware and software vulnerability scans and penetration testing; periodic evaluation and audit of cybersecurity of technological infrastructure; and threat intelligence.

System Access Controls. Of the 56 schemes, 48 address system access controls. Topics covered include limiting access to personnel with appropriate security clearance; automatic detection and blocking of unauthorised network access; ability to identify, restrict numbers of, and monitor persons with access rights to IT systems to ensure traceability; and storage and monitoring of access logs.

Training. Training is addressed by 43 of the 56 regulatory and guidance schemes. Matters covered include the audience for training and education, including customers and technical and non-technical staff; staff testing; and types of training, including awareness of cybersecurity and response to attack and scenarios of significant concern, such as phishing and social engineering, loss of data through e-mail or removable media or unintentional posting of confidential or proprietary information on social media.

Testing. Forty-four of the 56 schemes cover testing related to cybersecurity. This includes vulnerability hardware and software scans, penetration testing, testing prior to system launch, testing of business continuity policy and disaster recovery plan and security incident response plan testing.

Incident Recovery. Forty-six of 56 schemes address incident recovery. This includes recovery planning, such as scenario planning and communication plans; specified times for resumption of operations; resumption of services; assurance of system integrity following cybersecurity incident; recovery of lost or corrupted data; and backup sites.

Cyber Risk Insurance. This is one of the least frequently addressed areas, covered by only 15 of 56 regulatory and guidance schemes. Schemes that address cyber risk insurance typically

suggest that such insurance be considered to provide financial mitigation and reduce the impact of disruptions.

Information Sharing. Jurisdictions reported that 31 of the schemes address information sharing internal and/or external to an organisation. Some approaches include notification to authorities of cybersecurity and threat information, with authorities determining whether to notify industry; required information sharing among peer institutions; incident management process to include informing internal stakeholders; platform for information sharing among institutions; and participation in financial sector information sharing organisations.

Third-Party Interconnections. This issue was addressed by 49 of 56 regulatory and guidance schemes. Topics covered include managing risk exposures arising from third-party vendors; outsourcing management, including outsourcing policies and identification, management and monitoring of risks; risk assessment prior to external procurement of IT services; review of third parties' cyber resilience plans and on-site assessment of third parties; risk analysis of interconnections with third parties; required terms of outsourcing agreements; and due diligence in selecting and monitoring third-party service providers.

Regulatory Reporting. This topic was covered by 50 regulatory and guidance schemes. Topics covered include incident reporting, including nature of incident, measures taken following the incident and initiatives to avoid recurrence; authorities' use of reported information; timeframe for reporting incidents; and annual reporting of security violations and vulnerabilities, measures taken and results of measures.

1.2.4 Supervisory practices

As noted above, FSB member jurisdictions reported 35 schemes of supervisory practice. Basic information for each of these schemes is summarised in Table 5, below.

Table 5: Summary of Individual Supervisory Practices Schemes

Note: "Other" includes types of entities not captured by the preceding categories, e.g. other credit providers, payment service providers and credit rating agencies.

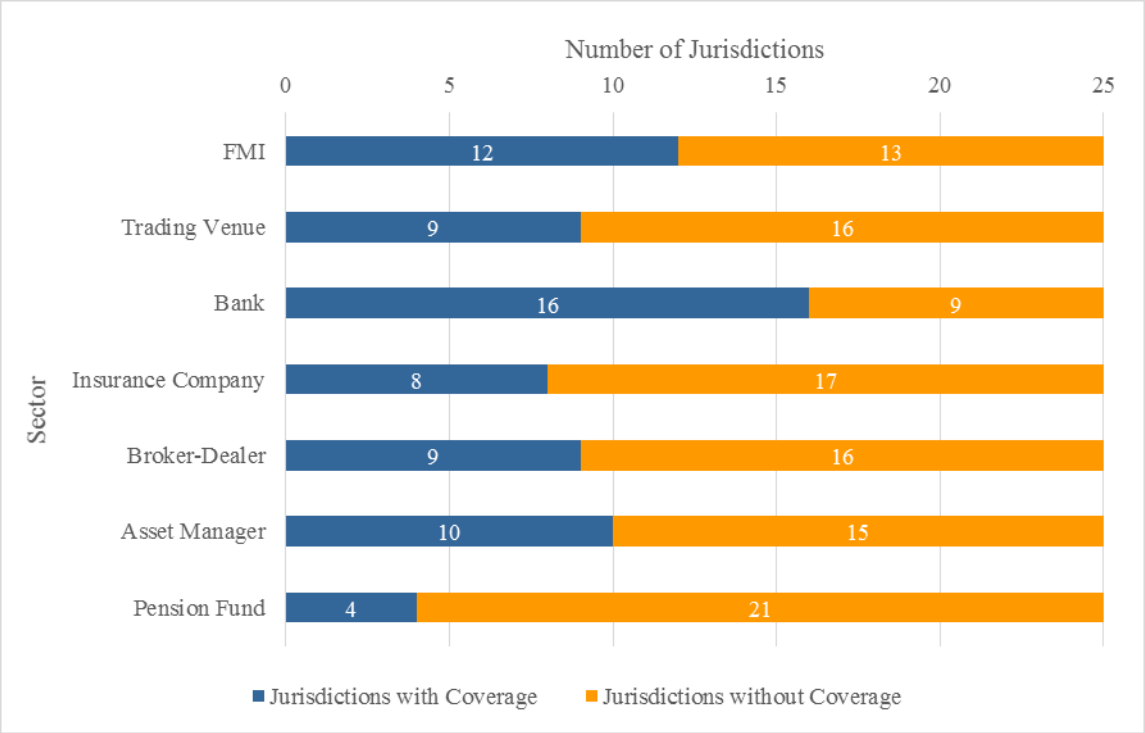
	Sector							
Jurisdiction/Scheme	FMI	Trad. Ven.	Bank	Ins. Co.	B-D	Asset Mgr.	Pens. Fd.	Other
Argentina			■					
Australia	■							
Brazil						■		■
China 1		■			■	■		■
China 2			■					
European Union 1								■
European Union 2			■					■
France	■		■	■				
Hong Kong 1	■		■					
Hong Kong 2					■	■		
India			■					
Indonesia 1	■				■			
Indonesia 2			■					
Italy 1	■							■
Italy 2		■						■
Japan	■	■	■	■	■			
Korea	■	■	■	■		■		
Mexico 1	■	■	■		■	■		■
Mexico 2	■		■					
Mexico 3				■				
Netherlands			■	■		■	■	■
Russia			■					
Singapore	■	■	■	■	■	■		■
Turkey 1	■							
Turkey 2			■					
Turkey 3								■
Turkey 4	■	■			■	■	■	
United Kingdom 1	■							
United Kingdom 2			■					■
United Kingdom 3		■	■	■	■	■	■	■
United States 1	■							■
United States 2			■					■
United States 3				■				
United States 4	■	■			■	■	■	■
United States 5	■	■						
Total	16	10	18	8	9	10	4	15

■ Jurisdictions with coverage

Blank cell indicates no coverage

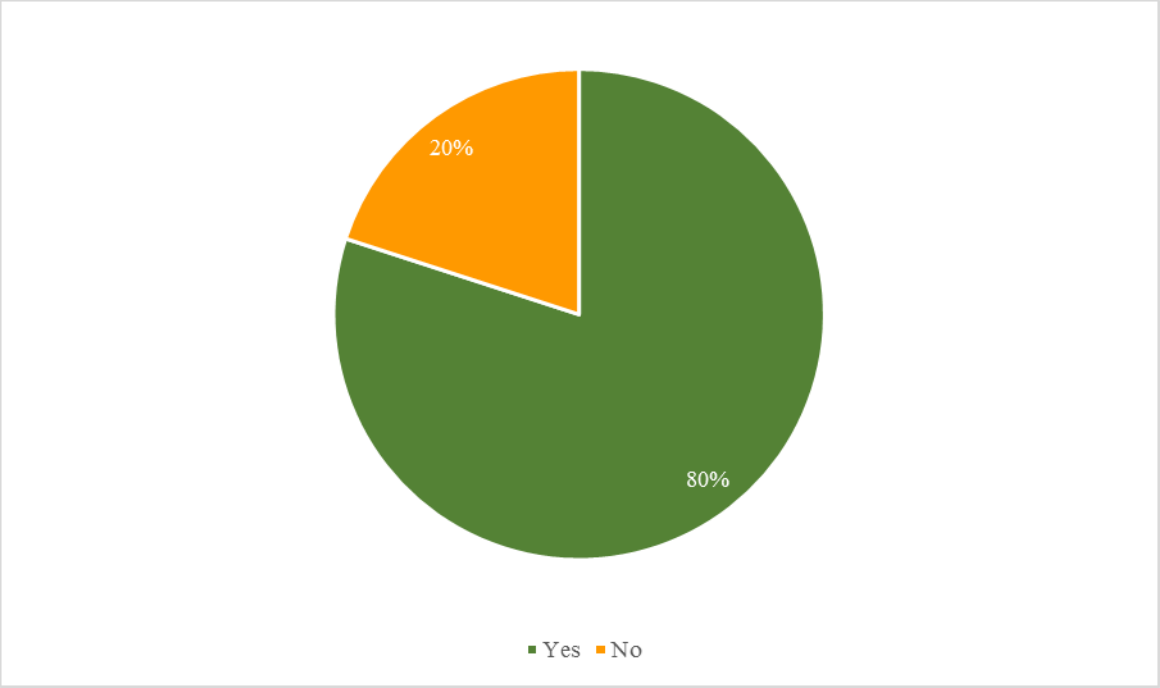
A majority of jurisdictions reported supervisory practice schemes for banks (16 of 25). Just under half reported supervisory practice schemes for FMIs (12 of 25). Ten jurisdictions reported supervisory practice schemes for asset managers, while approximately one-third reported supervisory practice schemes for trading venues, broker-dealers and insurance companies (8 or 9 of 25 for each of these categories). Four reported supervisory practice schemes for pension funds. This data is reflected in Figure 10, below.

Figure 10: Number of Jurisdictions with Supervisory Practices Schemes, by Sector



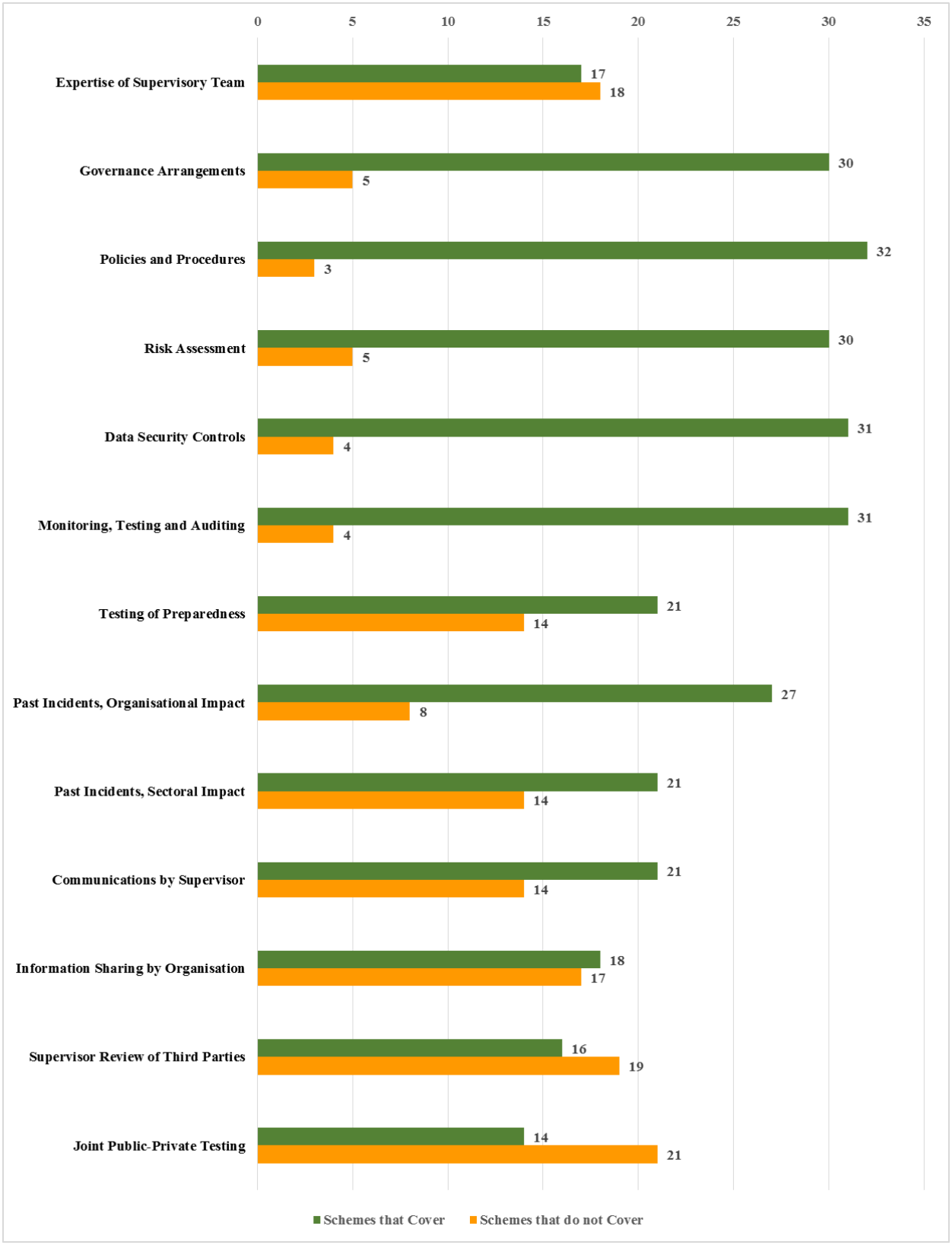
Jurisdictions were asked to identify whether the supervisory practices schemes incorporated any existing national or international guidance or standards of public authorities or private bodies. Twenty-eight of the supervisory practices schemes (80%) were reported to incorporate existing guidance or standards. This is reflected in Figure 11, below.

Figure 11: Percentage of Supervisory Practices Schemes that Incorporate Existing Guidance



Jurisdictions were asked whether or not the supervisory practices schemes addressed a number of specific content elements. Table 8, contained in Annex A, indicates the number of yes and no responses received for each content element. Figure 12, below, provides the information for a subset of the content elements.

Figure 12: Number of Supervisory Practices Schemes that Cover Certain Topics



The following discussion elaborates on the information provided in Figure 12.

Supervisory Team Expertise. Just less than half (17) of the 35 schemes address the expertise of the supervisory team. Those that do mention, among other things, in-depth knowledge of cybersecurity; relevant experience, professional qualifications, skills and ongoing training; engagement of outside experts; and IT background.

Governance Arrangements. Thirty of the schemes address review of an organisation's governance arrangements with respect to cybersecurity. This includes review of the existence of an independent role with information security responsibilities; clarity of the responsibilities and duties for IT-related decision-making; and composition, structure and involvement of the board on setting cybersecurity guidance and strategy.

Policies and Procedures. Nearly all of the schemes (32 of 35) address review of an organisation's policies and procedures related to cybersecurity. Matters cited in this area include assessment of whether an organisation has in place board-approved cybersecurity policies commensurate with its cyber risk and complexity, as well as policies to address cyber threat intelligence sharing and incident response and resilience and verification of procedures to protect confidentiality of information and policies for information security.

Risk Assessment Process. Thirty of the schemes address review of an organisation's risk assessment process. Topics covered include review of whether risk assessment processes are effective, whether an organisation establishes a routine risk identification and monitoring process and whether the results of IT risk assessment are properly used; periodic submission of an organisation's risk assessment to authorities; and verification that risk assessment is supported by adequate data collection concerning threats and vulnerabilities in relation to cyber risks.

Data Security Controls. Thirty-one of the schemes address review of an organisation's controls with respect to data security. This includes data backup and recovery policies, traceability of data, authentication and authorisation, and monitoring and logging.

Monitoring, Testing and Auditing. Thirty-one reported schemes address review of an organisation's programmes for monitoring, testing and auditing. This includes review of threat monitoring and audit trails, whether penetration tests and vulnerability scans are routinely applied and procedures for using tools that detect computer viruses and malicious code.

Testing by Supervisor/Submission of Test Results to Supervisor. Twenty-one of the 35 supervisory practice schemes address testing by the supervisor of an organisation's cybersecurity preparedness and/or submission to the supervisor of the results of such testing by the organisation. Some supervisors reported carrying out penetration tests on financial institutions or requesting institutions to submit assessment results for penetration testing, as well as industry-wide exercises.

Organisational and Sectoral Impact of Past Incidents. Twenty-seven reported schemes address review of past cybersecurity incidents and the organisation's response to, and recovery from, those incidents. Twenty-one schemes address review of incidents in order to evaluate the potential impact of incidents at one financial institution on other financial institutions or the financial sector. Some supervisors reported organisational mechanisms for organising a sector-wide response to disruptions that could endanger the stability of the financial sector, including

communications plans, and follow-up on an incident at one institution to check whether the same incident occurred elsewhere and/or how the overall sector is affected.

Communications by Supervisor. Twenty-one of 35 schemes addressed plans for communications by the supervisor with other domestic or international authorities or other parties. Means of addressing this issue include specifying criteria for information to be shared, establishing contacts with other domestic and international authorities and law enforcement, information-sharing memoranda of understanding and jurisdiction-wide incident response frameworks.

Information Sharing by Financial Institutions. Eighteen of 35 supervisory practices schemes address review of a financial institution's information sharing regarding cybersecurity. This includes review of whether institutions report to authorities in a timely manner, whether institutions have policies and procedures for cyber threat intelligence sharing, and encouraging financial institutions to join information-sharing organisations.

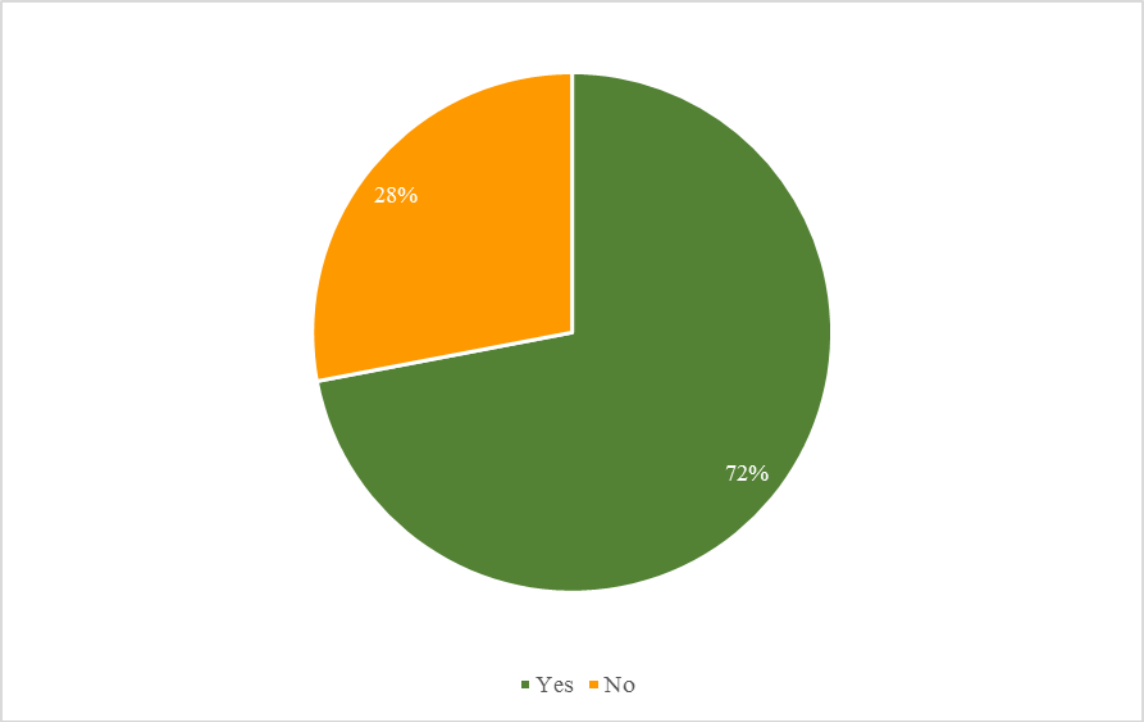
Supervisory Review of Third Parties. Sixteen schemes address direct review by the supervisor of third parties, such as vendors, that may affect an organisation's cybersecurity. In some cases, a supervisor reviews critical IT activities on-site in external parties' premises. Supervisory access to an institution's service providers may be obtained directly in applicable law or by requiring the institution to include this access right in outsourcing contracts.

Joint Public-Private Testing. Fourteen of the reported supervisory practices schemes address joint public-private testing of cybersecurity readiness. Some of these exercises are conducted within the financial sector or parts thereof, and others are cross-sectoral, e.g. involving multiple critical infrastructure sectors. Some may involve multiple jurisdictions.

1.3 Reported Future Plans

FSB member jurisdictions remain active in the area of financial sector cybersecurity. Each of the following jurisdictions reported publicly released plans to issue, within the next year, new regulations, guidance or supervisory practices that address cybersecurity for the financial sector: Argentina, Australia, Brazil, China, European Union, France, Germany, Hong Kong, India, Italy, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain and the United States. These plans include development of cybersecurity regulations, guidance and strategy for the financial sector; a self-assessment exercise to gauge the cyber resilience of FMIs; guidance on conducting threat intelligence based testing of cyber resilience; developing a set of standards for industry on Information Technology Risk (including cyber) and updating existing guidance in this area; and establishment of a computer emergency response team (together with computer security incident response team referred to hereinafter as CERT) for the financial sector. Each jurisdiction's plans are described in Annex C. Figure 13 shows the percentage of FSB member jurisdictions that reported near-term future plans.

Figure 13: Percentage of Jurisdictions Reporting Near-Term Plans to Issue New Regulations, Guidance or Supervisory Practices



1.4 Reported Effective Practices

The FSB's Cybersecurity Survey asked member jurisdictions to identify practices that they deem effective in addressing cybersecurity through regulations, guidance and/or supervisory practices. Jurisdictions provided a wide range of responses, which are highlighted below. This section is not a comprehensive list of practices that are in place in member jurisdictions; rather, it is an enumeration of practices that one or more jurisdictions identified as **effective**.

Existing Guidance and Standards. Specific, existing international guidance and standards, most frequently the CPMI-IOSCO Guidance, were cited by some jurisdictions.

Principles-based, risk-based or proportional supervision. Another effective practice cited was principles-based or risk-based supervision, requiring the application of sound judgment in identifying and assessing risks and determining, from among available supervisory and regulatory options, the most appropriate methods to ensure that the risks a financial institution faces are adequately managed. Supervision should be proportional to the nature, size, complexity and risk profile of a financial institution.

Role of board and senior management. The importance of senior management, and creation of the attention to, awareness of and responsibility for cybersecurity on the board level, as well as management accountability, were cited as important factors. The appointment of a CISO was also cited.

Independence of risk management. The importance of independent technological risk management was cited.

Policies and procedures. Regulated institutions should establish policies, procedures and processes concerning information systems management.

Communications between authorities and regulated entities. Effective regulation and guidance is better achieved through constant dialogue between authorities and regulated entities; authorities must have a good understanding of what is at stake for regulated entities in order to fit regulations and guidance to reality.

Coordination and information sharing. Coordination and information sharing among domestic and foreign authorities, including law enforcement authorities, and working with international organisations, was cited as an effective practice. More generally, the establishment of an emergency coordination system and improvement of emergency coordination plans was cited. Information sharing, including information about threat intelligence, cyber incidents and industry best practices, between authorities and regulated entities, and/or among regulated entities, was also noted.

Identification and updating of cybersecurity requirements. One effective practice cited was identifying and updating a set of cybersecurity requirements for the financial sector, including requirements to address specific areas that are considered more important.

Outsourcing Risks. The importance of strong control of outsourcing risks was noted.

Specific supervisory tools. A number of specific supervisory tools were cited, including:

- Review of institution's cyber roadmap;
- On-site examinations, including examinations focused on assessing the adequacy of controls regarding cyber risk management, and off-site reviews;
- Industry-wide preparedness exercises;
- Third-party audits and assessments;
- Self-assessments by financial institutions, including with authority-created tools that create repeatable and measurable process;
- Testing, including penetration testing, vulnerability testing and red-teaming exercises;
- Review of institution's controls for preventing and detecting cyber incidents;
- Notification to authorities of cyber incidents;
- Review of past cyber incidents;
- Compliance reviews;
- Thematic reviews of cybersecurity that provide authorities up-to-date industry-wide assessment of risk and key common issues;
- Requiring timely remediation of gaps in cybersecurity preparedness;
- Issuance of advisories and guidelines on specific areas of concern; and
- Administrative fines and penalties.

Systemic Risk Assessment. The importance of assessing cross-border and cross-sector threats and systemic risk for the financial sector was noted.

2. Guidance and other work of international bodies

The following 10 international bodies responded to the FSB cybersecurity survey: Basel Committee on Banking Supervision (BCBS), Committee on the Global Financial System (CGFS), Committee on Payments and Market Infrastructures (CPMI), G7 Cyber Expert Group (G7 CEG), International Association of Insurance Supervisors (IAIS), International Accounting Standards Board (IASB), International Monetary Fund (IMF), International Organization of Securities Commissions (IOSCO), Organisation for Economic Co-Operation and Development (OECD) and World Bank (WB).

Five international bodies reported having issued guidance that addresses cybersecurity. This includes BCBS, CPMI, G7, IOSCO and OECD. In the case of CPMI and IOSCO, the guidance was issued jointly. Four international bodies, CPMI, IAIS, IOSCO and OECD, reported publication of other documents relating to cybersecurity. In addition, eight of the 10 international bodies reported that they are currently conducting, or planning to conduct, work regarding cybersecurity. This includes BCBS, CPMI, G7, IAIS, IMF, IOSCO, OECD and WB.

2.1 Guidance issued by international bodies

This Section describes cybersecurity guidance that international bodies have reported issuing. There is enormous variation in the scope of the entities and activities covered by the guidance, from e-banking (BCBS) and FMIs (CPMI-IOSCO) to firms and supervisory and regulatory authorities throughout the financial sector (G7 CEG) to critical information infrastructures generally and all economic and social activities across all sectors, from businesses, governments and individuals (OECD). The guidance was issued over a period of more than a decade, a time of rapidly evolving technology, with the earliest issued in 2003 (BCBS) and the latest issued in 2016 (CPMI-IOSCO, G7 CEG). Notwithstanding these considerable differences in scope of coverage and time of issuance, there are striking similarities across the guidance, with many of the same topics addressed. Common topics addressed by the guidance of international bodies include:

- ***Governance***, including a framework to address cyber resilience and defined roles for the board and senior management (BCBS, CPMI-IOSCO, G7 CEG);
- ***Risk Analysis and Assessment*** (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Information Security***, including confidentiality, integrity and availability (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Security Controls and Incident Prevention***, including access controls and audit trails (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Expertise and Training*** to competently manage and address risks (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Monitoring, Testing and/or Auditing***, to include incident detection and evaluation of the effectiveness of controls, including through monitoring, testing, audits and exercises (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Incident Response and Recovery*** to investigate, manage, contain and recover from attacks (BCBS, CPMI-IOSCO, G7 CEG, OECD);

- ***Communications and Information Sharing*** with relevant internal and external stakeholders, which includes authorities, other market participants and media, including in the event of security breaches, online attacks or system failures (BCBS, CPMI-IOSCO, G7 CEG, OECD);
- ***Oversight of Interconnections***, including management of outsourcing relationships and other third-party dependencies (BCBS, CPMI-IOSCO, G7 CEG, OECD); and
- ***Continuous Learning*** to re-evaluate and improve cyber resilience on an ongoing basis (CPMI-IOSCO, G7 CEG, OECD).

BCBS

BCBS published *Risk Management Principles for Electronic Banking* in 2003.[5] This guidance for banks sets out how risks associated with e-banking development should be considered and addressed in the risk management process.

Some key areas covered by the guidance include the following:

- ***Governance.*** The roles of the board of directors and senior management in determining whether to provide e-banking; risk analysis, mitigation and monitoring related to e-banking; and addressing operational and security risk dimensions of e-banking are addressed.
- ***Information Security.*** Banks should ensure appropriate measures to ascertain the accuracy, completeness and reliability of e-banking transactions, records and information that is transmitted over the internet, resident on internal databases, or transmitted/stored by third-party service providers.
- ***Security Controls.*** Those addressed include authentication of e-banking customers; proper authorisation controls within e-banking systems, databases and applications; data integrity of e-banking transactions, records and information; establishment of clear audit trails for e-banking transactions; and confidentiality of key banking information.
- ***Expertise.*** Board and senior management should ensure the bank has the necessary expertise to provide competent risk management oversight.
- ***Incident Recovery.*** Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks.
- ***Communications.*** Incident response plans should include a communication strategy to adequately address external market and media concerns that may arise in the event of security breaches, online attacks and/or failures of e-banking systems.
- ***Outsourced Operations***. The board of directors and senior management should establish a comprehensive and ongoing diligence and oversight process of managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

---

[5] See www.bis.org/publ/bcbs98.pdf.

CPMI-IOSCO

CPMI and IOSCO issued the *Guidance on cyber resilience for financial market infrastructures* in 2016.[6] The purpose of the guidance was to provide guidance for FMIs to enhance their cyber resilience. It discussed risk management themes that should be addressed across an FMI's cyber resilience framework, including governance, identification, protection, detection, and response and recovery. The guidance was intended to provide supplemental detail to CPMI-IOSCO's existing *Principles for Financial Market Infrastructures*, primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).[7]

Some key areas addressed by the guidance include the following:

- ***Cyber Resilience Framework.*** FMIs should have a clear and comprehensive cyber resilience framework that accords a high priority to the safety and efficiency of the FMI's operations while supporting broader financial stability objectives. The framework should clearly articulate how the FMI determines its cyber resilience objectives and cyber risk tolerance, as well as how it effectively identifies, mitigates and manages its cyber risks. The framework should outline the FMI's people, processes and technology requirements for managing cyber risks and include timely communication to enable effective collaboration with relevant stakeholders.
- ***Governance.*** Effective governance should start with a clear and comprehensive cyber resilience framework that prioritises the security and efficiency of the FMI's operations, and supports financial stability objectives. It is essential that the framework is supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon the board and management to create a culture which recognises that staff at all levels, as well as interconnected service providers, have important responsibilities in ensuring the FMI's cyber resilience.
- ***Risk Assessment.*** An FMI should identify its business functions and supporting processes and conduct a risk assessment in order to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the FMI's prioritisation of its protective, detective, response and recovery efforts. FMIs should also carry out risk assessments of information assets.
- ***IT Security.*** It is critical that FMIs identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of an FMI's assets and services.

---

6 See www.bis.org/cpmi/publ/d146.htm and www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf.

7 See www.bis.org/cpmi/publ/d101a.pdf.

- ***Training.*** FMIs should ensure that all their relevant staff receive training to develop and maintain appropriate awareness of and competencies for detecting and addressing cyber-related risks. They should also be trained on how to report any unusual activity and incidents. High-risk groups should be identified and receive targeted information security training.
- ***Monitoring, Testing and Auditing.*** FMIs should establish capabilities to continuously monitor (in real time or near time) and detect anomalous activities and events. FMIs should seek to detect both publicly known vulnerabilities and vulnerabilities that are not yet publicly known. Detection capabilities should also address misuse of access by service providers or other trusted agents, potential insider threats and other advanced threat activity. The elements of an FMI's cyber resilience framework should be rigorously tested to determine their effectiveness. The scope of testing includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams. The adequacy of and adherence to an FMI's cyber resilience framework should be assessed and measured regularly through independent compliance programmes and audits carried out by qualified individuals.
- ***Response and Recovery.*** FMIs should perform a thorough investigation to determine an incident's nature and extent as well as the damage inflicted. FMIs should take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning. FMIs should be able to resume critical operations within two hours and also plan scenarios where this objective is not achieved, prioritising resumption and recovery actions, which may facilitate the processing of critical transactions. FMIs should also plan for situations where critical people, processes or systems may be unavailable for significant periods.
- ***Communications and Information Sharing.*** The cyber resilience framework should include timely communication to enable effective collaboration with relevant stakeholders. FMIs should inform relevant oversight and regulatory authorities promptly of potentially material or systemic events. To facilitate sector-wide response to large-scale incidents, FMIs should plan for information-sharing through trusted channels in the event of an incident, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants. FMIs should actively participate in information-sharing groups and distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats.
- ***Continuous Learning.*** The guidance emphasises the importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks to enable effective management of those risks. FMIs should aim to demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation.
- ***Interconnections with Third Parties.*** An FMI's cyber resilience framework should consider how the FMI would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other FMIs, vendors, vendor products and service providers. The guidance defines the FMIs' responsibilities for addressing cybersecurity matters arising from connections with third parties.

G7 CEG

G7 CEG published the *G7 Fundamental Elements for Cybersecurity* (G7 Fundamental Elements) in 2016.[8] This guidance applies to both firms and supervisory and regulatory authorities throughout the financial sector, including FMIs, trading venues, banks, insurance companies, broker-dealers, asset managers and pension funds.

The G7 Fundamental Elements describe their purpose as follows.

> "The elements 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 cybersecurity 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. Working together, informed by the elements, private and public entities and public authorities can help bolster the overall cybersecurity and resiliency of the international financial system."

Some key areas covered by the guidance include the following:

- ***Cybersecurity strategy and framework.*** Firms and authorities should establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national and industry standards and guidelines. These should be tailored to an entity's nature, size, complexity, risk profile and culture.
- ***Governance.*** Firms and authorities should 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 (e.g. board of directors or senior officials at public authorities). Boards of directors (or similar oversight bodies for public entities or authorities) should establish the cyber risk tolerance for their entities and oversee the design, implementation and effectiveness of related cybersecurity programmes.
- ***Risk Assessment.*** Firms and authorities should identify functions, activities, products and services – including interconnections, dependencies and third parties – prioritise their relative importance, and assess their respective cyber risks. They should 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. Protection mechanisms can include avoiding or eliminating risk by not engaging in an identified activity. They can also include mitigating the risk through controls or sharing or transferring the risk. Risk and control assessments should consider as appropriate any cyber risks the entity presents to others and the financial sector as a whole.
- ***Information Security.*** Ideally as part of an enterprise risk management programme, entities should evaluate the inherent cyber risk (or the risk absent any compensating

[8] See www.treasury.gov/resource-center/international/g7g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf.

controls) presented by the people, processes, technology and underlying data that support each identified function, activity, product and service. Entities should then identify and assess the existence and effectiveness of controls to protect against the identified risk to arrive at the residual cyber risk.

- ***Training.*** Training is one of a range of possible controls to protect against and mange cyber risks.
- ***Monitoring, testing and auditing.*** Firms and authorities should 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. Depending on the nature of an entity and its cyber risk profile and control environment, the testing and auditing functions should be appropriately independent from the personnel responsible for implementing and managing the cybersecurity programme. Through examinations, on-site and other supervisory mechanisms, comparative analysis of entities' testing results, and joint public-private exercises, public authorities can better understand sector-wide cyber threats and vulnerabilities, as well as individual entities' relative risk profiles and capabilities.
- ***Incident response and recovery.*** In a timely manner, firms and authorities should assess the nature, scope and impact of a cyber incident; contain the incident and mitigate its impact; notify internal and external stakeholders; and coordinate joint response activities as needed. Firms and authorities should resume operations responsibly, while allowing for continued remediation, including by eliminating harmful remnants of the incident; restoring systems and data to normal and confirming normal state; identifying and mitigating all vulnerabilities that were exploited; remediating vulnerabilities to prevent similar incidents; and communicating appropriately internally and externally.
- ***Information sharing.*** Firms and authorities should 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 defences, limit damage, increase situational awareness and broaden learning.
- ***Continuous learning.*** Firms and authorities should review the cybersecurity strategy and framework regularly and, when events warrant, address changes in cyber risks, allocate resources, identify and remediate gaps and incorporate lessons learned.

OECD

OECD reported the publication of two guidance documents, a *Recommendation of the Council on the Protection of Critical Information Infrastructures*, and *a Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*.

OECD's *Recommendation of the Council on the Protection of Critical Information Infrastructures* was published in 2008.[9] The Recommendation provides guidance to assist governments in the development of their policies for the protection of critical information

[9] See www.oecd.org/sti/ieconomy/ciip.htm.

infrastructures. OECD stated that in most countries, some actors of the financial sector would be critical information infrastructures. The OECD is currently reviewing the Recommendation.

Some key areas covered by the guidance include the following:

- ***Responsibility for Identifying Critical Information Infrastructures.*** "Critical information infrastructures" are defined as "those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy". While the Recommendation contains guidance on how to identify critical information infrastructures, it is up to governments to make the identification.
- ***Risk Assessment.*** The identification of critical information infrastructures should be based on risk assessment.
- ***Scope of Recommendation.*** The Recommendation includes prevention, protection, response and recovery from national and malicious threats.
- ***Incident Response.*** The Recommendation calls on governments to develop an incident response capability, such as a CERT, in charge of monitoring, warning, alerting and carrying out recovery measures for critical information infrastructures; and mechanisms to foster closer cooperation and communications among those involved in incident response.
- ***Communications and Information Sharing.*** According to the Recommendation, governments should work in partnership with the private sector by: (i) establishing trusted public-private partnerships with a focus on risk management, incident response and recovery; and (ii) enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.
- ***Continuous Learning.*** Governments should develop, and periodically review, a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:
  - The appropriate organisational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure preparedness, including prevention, protection, response and recovery from natural and malicious threats; and
  - A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.
- ***International Cooperation.*** The Recommendation addresses international cooperation in the protection of critical information infrastructures.

OECD's *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* was published in 2015.[10] The recommendation applies to all economic

[10] See http://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm.

and social activities, across all sectors, from businesses, governments and individuals. Thus, the Recommendation applies to the financial sector and all subsectors thereof.

The purpose of the Recommendation is to help governments, businesses and individuals address digital security as an economic and social risk (i.e. in addition to a technical matter) in order to elevate digital trust and maximise the benefits of the digital transformation. It provides a set of high-level principles for leaders and decision makers in public and private organisations to guide the development of corporate digital security policies and government national security strategies. It also includes more detailed public policy guidance for national strategies.

Some key areas covered by the Recommendation include the following:

- ***Risk Management.*** A key message of the Recommendation is that instead of being treated as a technical problem that calls for technical solutions, digital risk should be approached as an economic risk; it should therefore be an integral part of an organisation's overall risk management and decision-making processes. The notion that digital security risk merits a response fundamentally different in nature from other categories of risk needs to be countered.
- ***Risk Assessment.*** Risk assessment is a fundamental aspect of the risk management cycle, and leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment. Digital security risk assessment should guide the selection, operation and improvement of security measures to reduce digital security risk to an acceptable level. Based on digital security risk assessment, a preparedness and continuity plan should be adopted to reduce the adverse effect of security incidents, and support the continuity and resilience of economic and social activities.
- ***Training.*** The Recommendation states that all stakeholders should understand digital security risk and how to manage it.
- ***Preparedness and Continuity.*** The Recommendation addresses measures to ensure resilience and business continuity, including prevention, detection, response and recovery from digital security incidents.
- ***Information Sharing.*** Governments should create the conditions for all stakeholders to collaborate in the management of digital security risk, notably by fostering active participation from relevant stakeholders in mutually trusted initiatives and partnerships whether private or public-private, formal or informal, at domestic, regional and international levels to:
  - Share knowledge, skills and successful experience and practices in relation to digital security risk management at policy and operational levels;
  - Exchange information related to digital security risk management; and
  - Anticipate and plan for future challenges and opportunities.
- ***Continuous Learning.*** The digital security risk management framework should be based on an ongoing cycle of review and improvement, which is essential to ensure effective risk management and further increase trust. This generally includes processes to test, audit and optimise the measures in place.

- ***Interconnections with Third Parties.*** Digital security risk stemming from interconnections with third parties is fully covered by the Recommendation.
- ***National Strategies.*** The Recommendation addresses national strategies, including many issues affecting private organisations. This includes the need for governments to identify incentives to foster digital security risk management, innovation, research, and development and to develop training and skills.

2.2 Other publications of international bodies

This Section describes documents relating to cybersecurity, other than guidance, that international bodies have reported publishing.

CPMI published a November 2014 report that analyses the relevance of cyber resilience issues for FMIs and their overseers within the context of CPMI-IOSCO's *Principles for Financial Market Infrastructures*.[11]

IAIS published a 2016 issues paper on cyber risk to the insurance sector.[12] The objectives of the paper were to raise awareness for insurers and supervisors of the challenges presented by cyber risk, including current and contemplated supervisory approaches for addressing these risks. It provides background, describes current practices, identifies examples, and explores related regulatory and supervisory issues and challenges. The paper focuses on cyber risk to the insurance sector and the mitigation of such risks. It does not cover IT security risks more broadly, cyber insurance (insurers' selling or underwriting that type of insurance product) or risks arising from cybersecurity incidents involving supervisors. The paper was intended to be primarily descriptive and was not meant to create supervisory expectations.

IOSCO published the results of a study of regulatory approaches and tools to deal with cyber risk in April 2016.[13] It addressed the key regulatory issues, challenges and implementation approaches related to cyber security for segments of securities markets, including some of the practices put in place by market participants. Sectors covered include trading venues, market intermediaries, asset managers and FMIs. The study also covered issues related to cooperation and sharing of information among market participants and regulators.

OECD reported the publication of eight documents relating to cybersecurity. These documents, while not focused on the financial sector, address a number of important topics. These include digital security risk management, cybersecurity in the broader context of the digital transformation, how increased connectivity and data-driven innovation have brought about significant economic and social opportunities while changing the scale and scope of digital security and privacy challenges, comparative analysis of national cybersecurity strategies and policies for the protection of critical information infrastructures, and guidance on developing more internationally comparable CERT statistics.[14]

---

[11] Cyber resilience in financial market infrastructures, http://www.bis.org/cpmi/publ/d122.pdf. Principles for financial market infrastructure, http://www.bis.org/cpmi/publ/d101a.pdf (international standards for FMIs, harmonising other pre-existing standards by raising minimum requirements, providing more detailed guidance and broadening the scope of the standards to cover new risk management areas and new types of FMIs).

[12] Issues Paper on Cyber Risk to the Insurance Sector, http://www.iaisweb.org/page/supervisory-material/issues-papers.

[13] Cyber Security in Securities Markets – an International Perspective, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.

[14] Companion Document to the OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity (October 2015), http://oe.cd/dsrm (discusses 2015 recommendation on digital security risk

2.3 Future plans

This Section describes work regarding cybersecurity that international bodies reported that they are currently conducting, or planning to conduct.

BCBS reports that, building on its previous initiatives, it will consider developing additional policy and/or supervisory measures related to cyber risk over the next two years.

CPMI currently has two workstreams addressing cybersecurity. First, a CPMI-IOSCO working group on cyber resilience for FMIs has an approved workplan that it intends to execute through year-end 2018. The plan includes monitoring and advancing the implementation of the published CPMI-IOSCO Guidance, and collaborating with, coordinating and educating FMI supervisors and overseers and other international bodies with a financial stability mandate. Among other things, the working group is currently engaged in thematic, cross border information sharing of best practices and assessment methodologies among members, and is exploring mechanisms to encourage both information sharing among regulators and overseers as well as implementation of the published CPMI-IOSCO Guidance.

Second, in July 2016, CPMI established a task force to look into the endpoint security of wholesale payments that involve banks, FMIs and other financial institutions. The task force is currently developing a high-level strategy to reduce the risk of wholesale payments fraud related to endpoint security. Its primary aim is to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud and, in doing so, support financial stability. The task force recently published a discussion note on the key elements of the strategy to seek input from relevant stakeholders.

G7 CEG reported that it will develop a set of high level and non-binding fundamental elements for effective assessment of cybersecurity by October 2017. The G7 CEG will also advance work on third-party risks and the coordination with non-financial critical sectors, as well as exploring further topics as directed by G7 Finance Ministers and Central Bank Governors.

IAIS reported that it is examining existing Insurance Core Principles[15] and expects to publish a paper on the application of the Core Principles to cybersecurity in late 2018.

---

management); Key issues for digital transformation in the G20 (January 2017), http://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (discusses cybersecurity in the broader context of the digital transformation); Managing Digital Security and Privacy Risk (June 2016), http://www.oecd-ilibrary.org/science-and-technology/managing-digital-security-and-privacy-risk_5jlwt49ccklt-en (discusses how increased connectivity and data-driven innovation have brought about significant economic and social opportunities while changing the scale and scope of digital security and privacy challenges); Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (November 2012), http://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm (comparative analysis of national cybersecurity strategies); The Development of Policies for the Protection of Critical Information Infrastructures (December 2007), http://www.oecd.org/sti/ieconomy/ciip.htm (comparative analysis of policies in 7 OECD countries); Digital identity management: Enabling Innovation and Trust in the Internet Economy (2011), http://www.oecd.org/sti/ieconomy/49338380.pdf (analytical work to achieve a shared understanding among government policymakers about digital identity management, its role in the Internet economy and how to develop better public policies in the area); Guidance for CSIRT statistics (June 2015), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en (guidance on developing more comparable CERT statistics); and Measuring the evidence base for security and privacy (December 2012), http://www.oecd-ilibrary.org/science-and-technology/improving-the-evidence-base-for-information-security-and-privacy-policies_5k4dq3rkb19n-en (explores potential for development of better indicators to inform policy making process in areas of security and privacy risk management).

[15] See https://www.iaisweb.org/page/supervisory-material/insurance-core-principles (the Insurance Core Principles provide a globally accepted framework for the supervision of the insurance sector).

IMF reported that it is undertaking some pilot work on cyber risks in the context of its formal system of surveillance, pursuant to which the IMF monitors member country policies as well as national, regional and global economic and financial developments in order to maintain stability and prevent crises in the international monetary system. The IMF also intends to hold a workshop on cyber risk in 2017.

IOSCO, as described in more detail under CPMI above, has a CPMI-IOSCO working group on cyber resilience for FMIs that has an approved workplan that it intends to execute through year-end 2018.

OECD is currently working on improving the evidence base for digital security and privacy through the development of statistical indicators in this area. It is also reviewing the 2008 OECD *Recommendation on the Protection of Critical Information Infrastructures* as well as the OECD 1997 *Guidelines on Cryptography Policy*.[16]

WB reported that it is committed to supporting jurisdictions addressing challenges posed by cyber risk and enumerated the following recent initiatives that have been taken or are being considered.

- In partnership with the International Telecommunication Union, the World Bank Group (WBG) is convening a workstream on cybersecurity for financial infrastructure under the security and trust working group of the newly created Financial Inclusion Global Initiative (FIGI), funded by the Bill & Melinda Gates Foundation. The workstream will include representatives from the public and private sector to develop practical guidelines on how to make payment and securities settlement systems and credit reporting systems more resilient to cyber attacks. These guidelines will be based on already existing principles, such as the G7 Fundamental Elements and the CPMI-IOSCO Guidance.
- The WBG will finalise a digest of existing and proposed regulations on cybersecurity preparedness by the end of October 2017.
- The WBG continues to support governments in developing national cybersecurity strategies. A Cybersecurity Diagnostic Toolkit has been developed to assess the current-state maturity of an organisation's cybersecurity posture based upon the NIST Cybersecurity Framework covering the five functions i.e., identify, protect, detect, respond and recover. The tool is comprised of 80 questions, mostly multiple-choice, and is designed to obtain a preliminary understanding of an organisation's cybersecurity maturity and identify areas where a deeper assessment is needed.
- The WBG has been conducting crisis simulation exercises to provide financial sector authorities an opportunity to discover their role in handling cyber incidents (i.e. the type of business decisions that these incidents demand) and the new types of stakeholders (such as national security agencies) they must interact with in those circumstances.

---

[16] As detailed in footnote 16: The Development of Policies for the Protection of Critical Information Infrastructures (December 2007), http://www.oecd.org/sti/ieconomy/ciip.htm; and Guidelines for Cryptography Policy (March 1997) http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm (recognises the important role encryption plays in helping to ensure the security of data and the protection of privacy in national and global information and communication infrastructures, networks and systems).

- In the area of combating cybercrime, the WBG has developed a toolkit under a project titled "Combating Cybercrime: Tools and Capacity Building for Emerging Economies", financed by a grant from the Korean Ministry of Strategy and Finance under the Korea-World Bank Group Partnership Facility Trust Fund. The toolkit aims to build capacity to combat cybercrime among policy makers, legislators, prosecutors and investigators. It looks at national legal frameworks, safeguards, capacity building, international cooperation and in-country assessments. The toolkit was formally launched in December 2016 in Seoul, and is expected to be published, released and posted online at www.combattingcybercrime.org soon.

Annex A:
Additional Tables

Table 6: Number of Jurisdictions Reporting Use of Existing National or International Guidance or Standards in their Regulatory and/or Supervisory Practices Schemes

Jurisdiction	Reflects National or International Guidance or Standards	Issuing Organisation(s)					
		CPMI-IOSCO	FFIEC	G7	ISACA (COBIT)	ISO IEC	NIST
Argentina	✓		■	■	■	■	■
Australia	✓	■					■
Brazil	✓	■			■	■	
Canada	✓	■	■		■	■	■
China	✓				■	■	
European Union	✓	■					■
France	✓	■	■				■
Germany	✓	■				■	
Hong Kong	✓	■	■		■		■
India	✓	■			■	■	■
Indonesia	✓				■	■	
Italy	✓	■		■		■	
Japan	✓	■				■	■
Korea	✓					■	
Mexico	✓	■	■	■	■		■
Netherlands	✓	■			■	■	■
Russia	✓	■				■	
Saudi Arabia	✓	■				■	■
Singapore	✓	■		■		■	■
South Africa	✓	■					
Spain	✓	■					
Switzerland	✓						■
Turkey	✓				■	■	
United Kingdom	✓	■				■	■
United States	✓	■	■		■	■	■
Total	**25**	**19**	**6**	**4**	**11**	**17**	**15**

■ Jurisdictions with coverage

Blank cell indicates no coverage

Table 7: Aggregate Annex A Response Data for Targeted Regulatory Schemes

Ref.	Question	Yes	No
8.1	Do the regulations/guidance define "cybersecurity"?	16	40
8.3	Do the regulations/guidance address the establishment or maintenance of a cybersecurity strategy and/or framework?	50	6
8.5	Do the regulations/guidance address the role of the board of directors or other body responsible for general oversight of the regulated entity?	49	7
8.7	Do the regulations/guidance address the role of senior or other management responsible for day-to-day operations of the regulated entity?	45	11
8.9	Do the regulations/guidance address the cybersecurity expertise of the board of directors or senior management?	22	34
8.11	Do the regulations/guidance address the creation of a cybersecurity or other role or function responsible for cybersecurity matters, such as a chief information security officer?	38	18
8.13	Do the regulations/guidance address the independence of any organisational structure or individual (e.g. cybersecurity risk management function) from other business functions (e.g. by establishing a direct reporting line to the board of directors or other oversight body)?	34	22
8.15	Do the regulations/guidance address the establishment and maintenance of cybersecurity policies and procedures?	53	3
8.17	Do the regulations/guidance address risk assessment, e.g. gathering threat intelligence, identifying vulnerabilities?	55	1
8.19	Do the regulations/guidance address the creation of an inventory of information technology assets?	41	15
8.21	Do the regulations/guidance address the creation of an inventory of business functions and/or processes (e.g. showing interconnections and dependencies, both internal and external)?	30	26
8.23	Do the regulations/guidance address the security of information systems, e.g. matters such as data integrity, back-up systems and data confidentiality?	53	3
8.25	Do the regulations/guidance address physical protection of assets?	46	10
8.27	Do the regulations/guidance address systems access controls?	48	8
8.29	Do the regulations/guidance address training (e.g. employee, customer or contractor training in the area of cybersecurity awareness or ongoing professional education of cybersecurity personnel)?	43	13
8.31	Do the regulations/guidance address ongoing monitoring, including surveillance of emerging threats, with respect to cybersecurity risks?	47	9
8.33	Do the regulations/guidance address testing (e.g. penetration testing, vulnerability scanning) related to cybersecurity?	44	12
8.35	Do the regulations/guidance address auditing related to cybersecurity, such as the establishment of audit trail systems or data and transaction traceability?	47	9
8.37	Do the regulations/guidance address investigation and/or assessment of cybersecurity incidents?	49	7
8.39	Do the regulations/guidance address containment and/or other mitigation of cybersecurity incidents?	43	13

Ref.	Question	Yes	No
8.41	Do the regulations/guidance address notification of stakeholders in the event of cybersecurity incidents?	46	10
8.43	Do the regulations/guidance address recovery from a cybersecurity incident?	46	10
8.45	Do the regulations/guidance address business continuity in the event of impaired functioning resulting from a cybersecurity incident?	52	4
8.47	Do the regulations/guidance address the consideration of cyber risk insurance as a financial mitigant to cyber risk incidents?	15	41
8.49	Do the regulations/guidance address information sharing internal and/or external to an organisation (e.g. sharing of sensitive data or sharing cybersecurity knowledge within the organisation or across the industry)?	31	25
8.51	Do the regulations/guidance address regular updating of information technology systems, including regular reviews to determine whether updating is needed?	46	10
8.53	Do the regulations/guidance address cybersecurity matters arising from interconnections and other arrangements with third parties, such as vendors, customers, and entities performing outsourced functions?	49	7
8.55	Do the regulations/guidance address regulatory reporting (e.g. cybersecurity incident reports)?	50	6
8.57	Do the regulations/guidance address authorities' access to information relating to regulated entities' cybersecurity?	39	17
8.59	Do the regulations/guidance address supervisory actions and other oversight or civil or criminal enforcement mechanisms?	28	28
8.61	Do the regulations/guidance address areas not covered by the specific questions above?	20	36
8.63	Do the regulations/guidance incorporate any existing national or international guidance or standards of public authorities (e.g. G7 Fundamental Elements of Cybersecurity for the Financial Sector, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity) or private bodies (e.g. International Organization for Standardization (ISO) 27001, ISACA COBIT)?	41	15
8.65	Do the regulations/guidance include a method to measure, rate, or benchmark cybersecurity risk or cybersecurity risk management at organisations?	18	38

Table 8: Aggregate Annex B Response Data for Supervisory Practices Schemes

Ref.	Question	Yes	No
11.1	Do the supervisory practices address the cybersecurity expertise of supervisory team members assigned to review and assess cybersecurity?	17	18
11.3	Do the supervisory practices address the circumstances when the supervisor should conduct a cybersecurity review (e.g. frequency of routine review, particular incidents or other circumstances that are cause for review)?	30	5
11.5	Do the supervisory practices address review of an organisation's cybersecurity strategy or framework?	29	6
11.7	Do the supervisory practices address review of an organisation's governance arrangements with respect to cybersecurity?	30	5
11.9	Do the supervisory practices address review of an organisation's policies and procedures related to cybersecurity?	32	3
11.11	Do the supervisory practices address review of an organisation's risk assessment process?	30	5
11.13	Do the supervisory practices address review of an organisation's controls with respect to physical information technology assets?	27	8
11.15	Do the supervisory practices address review of an organisation's mapping of business functions and processes (which mapping shows, for example, interconnections and dependencies between functions and processes, both internally and with external parties)?	20	15
11.17	Do the supervisory practices address review of an organisation's controls with respect to data security, e.g. data integrity, data traceability, data back-up and data confidentiality?	31	4
11.19	Do the supervisory practices address review of an organisation's controls with respect to systems security?	29	6
11.21	Do the supervisory practices address review of an organisation's programs for training personnel, such as training in cybersecurity awareness and professional training of cybersecurity personnel?	27	8
11.23	Do the supervisory practices address review of an organisation's programs for monitoring (including surveillance of emerging threats), testing (e.g. penetration testing, vulnerability scanning) and auditing (e.g. audit trail systems, data and transactions traceability) its cybersecurity?	31	4
11.25	Do the supervisory practices address testing by the supervisor of an organisation's cybersecurity preparedness and/or submission to the supervisor of the results of testing by the organisation of its cybersecurity preparedness?	21	14
11.27	Do the supervisory practices address review of an organisation's readiness to assess, mitigate and recover from cybersecurity incidents?	29	6
11.29	Do the supervisory practices address review of past cybersecurity incidents and the organisation's response to, and recovery from, those incidents?	27	8
11.31	Do the supervisory practices address review of cybersecurity incidents in order to evaluate the potential impact of cybersecurity incidents at one financial institution on other financial institutions or the financial sector?	21	14
11.33	Do the supervisory practices address review of an organisation's communications plans with respect to cybersecurity incidents?	25	10

Ref.	Question	Yes	No
11.35	Do the supervisory practices address plans for communications by the supervisor with other domestic and/or international authorities and/or other parties in the event of a cybersecurity incident?	21	14
11.37	Do the supervisory practices address review of an organisation's business continuity plans in the event of impaired ability to carry on business functions as a result of a cybersecurity incident?	27	8
11.39	Do the supervisory practices address review of an organisation's information sharing regarding cybersecurity, with internal and/or external parties?	18	17
11.41	Do the supervisory practices address review of an organisation's oversight of its relationships with third parties, such as vendors and customers, that may affect the organisation's cybersecurity?	27	8
11.43	Do the supervisory practices address direct review by the supervisor of third parties, such as vendors and customers, that may affect an organisation's cybersecurity?	16	19
11.46	Do the supervisory practices address joint public-private testing of cybersecurity readiness, such as through simulations of cyber incidents?	14	21
11.48	Do the supervisory practices include a method to measure, rate, or benchmark cybersecurity risk or cybersecurity risk management at organisations?	12	23
11.50	Do the supervisory practices define "cybersecurity"?	12	23
11.52	Do the supervisory practices address areas not covered by the specific questions above?	12	23
11.54	Do the supervisory practices incorporate any existing national or international guidance or standards of public authorities (e.g. G7 Fundamental Elements of Cybersecurity for the Financial Sector, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity) or private bodies (e.g. International Organization for Standardization (ISO) 27001, ISACA COBIT)?	28	7

Annex B:
Glossary of Existing National and International Guidance and Standards

CPMI-IOSCO. The *Guidance on cyber resilience for financial market infrastructures* was published in June 2016 by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The purpose of the guidance was to provide guidance for FMIs to enhance their cyber resilience. It discussed risk management themes that should be addressed across an FMI's cyber resilience framework, including governance, identification, protection, detection and response and recovery. The guidance was intended to provide supplemental detail to CPMI-IOSCO's existing *Principles for Financial Market Infrastructures*, primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).

FFIEC. The Federal Financial Institutions Examination Council (FFIEC), a US interagency body that prescribes uniform principles and standards for the examination of banks and other financial institutions supervised by the federal and state banking regulators, has developed an IT Handbook to identify supervisory objectives to ensure safety and soundness of regulated entities. The Handbook covers the following topics: audit; business continuity planning; development and acquisition; e-banking; information security; management; operations; outsourcing technology services; retail payment systems; supervision of technology service providers; and wholesale payment systems. FFIEC has also developed the Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity maturity. The content of the assessment is consistent with the principles of the FFIEC IT Handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It provides institutions with a repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness.

G7. The *G7 Fundamental Elements of Cybersecurity for the Financial Sector* were published in October 2016. They provide a concise set of principles on best practices in cybersecurity for public and private entities in the financial sector. The G7 Fundamental Elements help address cyber risks facing the financial sector from both entity-specific and system-wide perspectives. The elements are building blocks that public or private entities in the financial sector can use to design and implement their cybersecurity strategy. Public authorities, including finance ministries, central banks and regulators, can also use the elements to inform their efforts to both protect the financial sector from cyber attacks and to effectively respond to and recover from incidents when they occur.

ISACA (COBIT). The Control Objectives for Information and Related Technology (COBIT) were first released in 1996 by the Information Systems Audit and Control Association (ISACA) and are continually updated to meet current needs and remain relevant. ISACA is a non-profit, global association that provides knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, cybersecurity and IT-related risk and compliance. COBIT is a comprehensive framework of globally accepted practices, analytical tools and models that can help enterprises effectively address business issues through governance and management of information and technology.

ISO/IEC. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published the 27000 family of standards on information security management systems to help organisations keep information assets secure. The 27000 family of standards is designed to help organisations 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.

NIST. The *Framework for Improving Critical Infrastructure Cybersecurity* was published in February 2014 by the US National Institute of Standards and Technology (NIST), and an updated version was recently published for comment. It is a voluntary, risk-based framework of industry standards and best practices to help organisations manage cybersecurity risks. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organisation's risk management process. The framework enables organisations, regardless of size, degree of cybersecurity risk or cybersecurity sophistication, to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. Because it references globally recognised standards for cybersecurity, the framework can also be used by organisations located outside the US.

Annex C:
Summaries of Jurisdiction Responses to FSB Survey

This Annex provides a summary of information reported by jurisdictions in response to the FSB Cybersecurity Survey, which was limited to publicly released information. The Annex provides a table that summarises basic information for all jurisdictions, followed by a brief summary for each jurisdiction, consisting of: (i) national cybersecurity strategy; (ii) regulations/guidance; (iii) supervisory practices; (iv) future plans; and (v) citations for publicly available regulations, guidance and supervisory practices.

Jurisdiction	National Strategy?	Regulations/ Guidance?	Supervisory Practices?	Future Plans?
Argentina		●	●	●
Australia	●	●	●	●
Brazil	●	●	●	●
Canada	●	●		
China	●	●	●	●
European Union	●	●	●	●
France	●	●	●	●
Germany	●	●		●
Hong Kong	●	●	●	●
India	●	●	●	●
Indonesia		●	●	
Italy	●	●	●	●
Japan	●	●	●	
Korea		●	●	
Mexico		●	●	●
Netherlands	●	●	●	●
Russia	●	●	●	●
Saudi Arabia		●		●
Singapore	●	●	●	●
South Africa	●	●		●
Spain	●	●		●
Switzerland	●	●		
Turkey	●	●	●	
United Kingdom	●	●	●	
United States	●	●	●	●

Argentina

National Strategy: None reported.

Regulations/Guidance: Argentina reported one scheme of regulations/guidance issued by the Central Bank of Argentina that covers **financial market infrastructures (FMIs) and banks**. It is targeted to cybersecurity and/or information technology (IT) risk. The scheme is based on five information security processes: awareness, access control, integrity and register, control and monitoring and incident management. It addresses governance, including the role of the board of directors, senior management, responsibility for information security, and the independence of security management from business roles. The scheme also addresses risk analysis, creation of IT inventories, security of information systems, training, monitoring, audit trails, access control, incident management, continuous maintenance of IT infrastructure and interconnections with third parties.

Supervisory Practices: Argentina reported one scheme of supervisory practices issued by the Central Bank of Argentina that covers **banks**. Most Central Bank IT and information security supervisors have international certifications from the Information Systems Audit and Control Association (ISACA). There is a bi-annual review and assessment of the risks of each critical financial entity, which includes every operating channel that is based on internet infrastructures. The supervisor reviews whether the bank has security policies and strategies, as well as implementation, monitoring and control, including incident follow-up. The supervisor also reviews whether there is an independent role with information security responsibility; risk assessment and mitigation processes; physical security; controls for data security, integrity, traceability, backups, confidentiality and encryption; threat monitoring; audit trails and recovery preparedness. The supervisor reviews the critical IT and information security processes of both internal and external parties.

Future Plans: Argentina reported that the Securities and Exchange Commission of Argentina is in the final stage of adopting a new regulation on cybersecurity following the principles of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000 family of standards and the *Guidance on cyber resilience for financial market infrastructures* published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO Guidance).

Publicly Available Sources: The official website of the Central Bank of Argentina, http://www.bcra.gob.ar, includes a section with all banking and supervisory regulation.

Australia

National Strategy: Australia reported that its Cyber Security Strategy establishes five themes of action for the country's cybersecurity over the next four years to 2020. These are:

- A national cyber partnership between government, researchers and business;
- Strong cyber defences to better detect, deter and respond to threats and anticipate risks;
- Global responsibility and influence to champion a secure, open and free internet while building capacity to crack down on cyber criminals and close safe havens for cybercrime;
- Growth and innovation to support the Australian cybersecurity sector to grow and prosper, and to ensure all Australian businesses can operate securely online; and
- A cyber smart nation to grow a highly skilled cybersecurity workforce and ensure all Australians are aware of the risks and benefits of being online.

Australia reported that much has already been achieved as part of the Strategy. This includes: the release of the Australian Securities Exchange (ASX) 100 Cyber Health Check Report, which highlighted the state of cybersecurity governance in Australia's top companies; and the updating of national guidance which outlines practical steps organisations can implement to make their networks and data more secure.

Regulations/Guidance: Australia reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Australian Prudential Regulation Authority (APRA), covers **banks, insurance companies and pension funds**. It is targeted to cybersecurity and/or IT risk. Prudential Practice Guides (PPG) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss statutory requirements from legislation, regulations or APRA's prudential standards but do not themselves create enforceable requirements. The PPG on Management of Security Risk in Information Technology is designed to provide guidance to senior management, risk management and IT security specialists in managing security risk in information and IT.

The second scheme, issued by the Australian Securities and Investments Commission (ASIC), covers **FMIs, trading venues, banks, insurance companies, broker-dealers, asset managers and pension funds**. It is targeted to cybersecurity and/or IT risk. The guidance considers the US National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* of particular relevance to the regulated entities. The guidance addresses the role of the board and the members' expertise and notes that ultimate accountability resides with the board, which should consider the use of an independent external cyber expert to review and challenge the information presented by senior management. The guidance also addresses integration of cybersecurity into normal business risk management; continuous monitoring; testing to identify vulnerabilities; maintaining inventory of information asset and identification of critical services; physical and electronic security arrangements; access controls; training; audit trails; tested response plans, including plans for communicating internally and externally; recovery and business continuity; cyber insurance; updating of software; assessment of third-party suppliers and partners for compliance with security standards; and regulatory reporting.

The third scheme, issued by the Reserve Bank of Australia (RBA), covers **FMIs**. It addresses operational risk generally. The scheme addresses governance arrangements, specifying that the risk management and internal control functions should have sufficient authority, independence, resources and access to the board, including through the maintenance of a separate and independent internal audit function. RBA requires central counterparties and securities settlement facilities to identify the plausible sources of operational risk and mitigate their impact through the use of appropriate systems, policies, procedures and controls. Business continuity management should aim for timely recovery of operations and fulfilment of obligations. Central counterparties and securities settlement facilities that establish links with one or more FMIs should identify, monitor and manage link-related risks. The scheme also addresses notification to RBA of events that may materially impact risk management or the ability to continue operations.

Supervisory Practices: Australia reported one scheme of supervisory practices, issued by ASIC, and covering **FMIs**. A regulatory guide for operators of licensed markets outlines ASIC's role in, and approach to, the regulation of financial markets operating in Australia, with a particular focus on Australian operators. The guidelines are principles based. A separate regulatory guide issued by ASIC relating to derivative trade repositories requires holders of an Australian Derivative Trade Repository Licence to ensure that adequate security arrangements are implemented, reviewed and tested periodically. There are also requirements for adequate risk management and availability of services, including business continuity and recovery. APRA has a set of supervisory practices targeting this area; however, these are not released publicly and therefore were not within scope of the FSB survey.

Future Plans: Australia reported that APRA is developing a set of standards for industry on Information Security Risk (including cyber) and updating its existing guidance in this area (e.g. the PPG on Management of Security Risk in Information Technology) in order to address areas of weakness identified as part of its supervisory activities.

Australia also noted a number of actions are currently being taken as part of Australia's national strategy (the Cyber Security Strategy) that, while not specific to the financial sector, will have some impact on the sector. These include: the release of voluntary cybersecurity guidelines that will identify best practice and help businesses to understand what they need to do to make their business secure; and the establishment of a Cyber Resilience taskforce, which will build on the Strategy to drive action on Australia's capability and response to cybersecurity and cybercrime threats and incidents.

Publicly Available Sources:

Australia's Cyber Security Strategy:
https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

APRA Management of Security Risk in Information Technology:
http://apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-234-Management-of-Security-Risk-May-2013.pdf

APRA Information Paper: Outsourcing involving Shared Computing Services (including Cloud): http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Outsourcing-Involving-Shared-Computing-Services.pdf

Insights from APRA's 2016 Cyber Security Survey: http://www.apra.gov.au/Insight/Pages/insight-issue3-2016.html

ASIC Cyber Resilience: Health Check: http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

Cyber Resilience: ASX Group and Chi-X Australia: http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-468-cyber-resilience-assessment-report-asx-group-and-chi-x-australia-pty-ltd/

ASX Cyber Health-Check Report: http://www.asx.com.au/documents/asx-news/ASX_100Cyber_Health_Check_Media_Materials.pdf

RBA Financial Stability Standards for Central Counterparties: http://www.rba.gov.au/payments-and-infrastructure/financial-market-infrastructure/clearing-and-settlement-facilities/standards/central-counterparties/2012/

RBA Financial Stability Standards for Securities Settlement Facilities: http://www.rba.gov.au/payments-and-infrastructure/financial-market-infrastructure/clearing-and-settlement-facilities/standards/securities-settlement-facilities/2012/

ASIC Regulatory Guide for Australian market licenses: http://www.asic.gov.au/media/1240949/rg172-reissued-24-september-2013-1.pdf

ASIC Derivative Trade Repository Rules for licensed trade repositories: https://www.legislation.gov.au/Details/F2013L01344; and the regulatory guide http://www.asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-249-derivative-trade-repositories/

Brazil

National Strategy: Brazil has reported that Normative Instruction GSI/PR No 1 (June 13 2008) defines guidelines for information security and communications management that should be implemented by entities of the federal public administration. The Office of Institutional Security of the Presidency of the Republic (GSI), through the Department of Information Security and Communications, is responsible for, among other things, planning and coordination of the information security and communications activities in the federal public administration. In addition, in 2010, the Institutional Security Office published the Green Paper on Cybersecurity in Brazil, which brings together proposals for basic guidelines aimed at initiating broad social, economic, political and technical-scientific debate on cybersecurity in Brazil.

Regulations/Guidance: Brazil reported four schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Central Bank of Brazil (BCB) on behalf of the National Monetary Council, covers **financial institutions and other institutions licensed by the BCB**. It addresses operational risk generally. Covered institutions must have a risk management framework in place. This framework is required to adequately address operational risk events and, more specifically, flaws in systems, processes or infrastructures related to IT. Moreover, the framework must ensure the integrity, security and availability of IT systems and infrastructures and must include mechanisms to prevent and detect the occurrence of digital attacks and reduce the institution's vulnerability to such events.

The second scheme is the Brazilian regulation regarding **insurance, reinsurance, open pension funds and the capitalisation sector**, where cybersecurity is addressed as part of internal controls and risk management requirements. SUSEP Circular No 249 of February 20 2004, states that insurers, reinsurers, open pension entities and other institutions authorised by the Superintendence of Private Insurance (SUSEP) should implement internal controls with respect to their activities, information systems and compliance with applicable laws and regulation. SUSEP Circular No 521 of November 24, 2015, states that insurers, reinsurers, open pension entities and other institutions authorised should adopt a risk management framework that addresses IT management and business continuity management. In addition, insurers that are part of financial conglomerates normally share the IT structure with the banks within the conglomerate and therefore their IT facilities should also comply with the Brazilian Central Bank regulation.

The third scheme, issued by the Securities Commission of Brazil (CVM), covers **trading venues, FMIs, asset managers and fiduciary administrators**. It addresses operational risk generally. The managing entities of an **exchange market** must maintain risk control systems adequate to the supervision of the risks inherent to its activities and must establish adequate procedures to ensure the regular operation and security of its information systems. An independent auditor must report on the quality and safety of the operating procedures and systems, including those measures provided for in rupture, contingency or emergency situations. **Centralised securities depository services** must have computerised processes and systems that are safe and adequate to carry out their activities, and establish and maintain controls and monitoring mechanisms to ensure the security and integrity of equipment, installations and systems, including the creation of access controls and measures to protect the confidentiality of information. They are also required to maintain appropriate risk control

systems to monitor the risks inherent to their activities, and those systems should establish appropriate procedures to ensure the regular operation and security of the system of accounts maintained. **Asset managers and fiduciary administrators** of investment funds must establish mechanisms to ensure periodic security tests of their information systems.

The fourth scheme, issued by BCB, covers **FMIs**. It addresses operational risk generally. The FMIs should apply the operational risk principle (Principle 17) of the CPMI-IOSCO *Principles for Financial Market Infrastructures* (CPMI-IOSCO Principles). Moreover, the FMIs must adopt the guidelines set by the CPMI-IOSCO Guidance, as a supplemental guidance of the CPMI-IOSCO Principles. In addition, the regulatory framework requires FMIs to: establish an operational infrastructure with adequate level of security and reliability; hold contingency and recovery plans to be adopted in the event of an operational fail; maintain the stated level of operational availability; set up a contingency centre that enables the recovery within a period stated (specified recovery time objective); and provide notice to BCB about any event that may impede or delay the normal functioning of the settlement system.

Supervisory Practices: Brazil reported one scheme of supervisory practices, published by CVM and covering **asset managers and fiduciary administrators**. The scheme addresses review of organisations' cybersecurity governance arrangements and policies and procedures, as well as controls with respect to data security. Brazil reported that non-observance of applicable regulation by service providers is considered a risk event by the CVM's risk-based supervision biennial plan. Under relevant regulation, portfolio managers must appoint a director responsible for the implementation of, and compliance with, rules, procedures and internal controls. This director must ensure that information systems used by the entity, especially electronic systems, undergo periodic security tests.

Cyber and information security and IT risks assessments have been fully integrated into the Supervisory Framework of the BCB for at least 10 years. BCB employs industry best practices in its Supervisory Framework. For cybersecurity issues, BCB's supervisory practices observe the guidelines present in the ISACA Control Objectives for Information and Related Technology (COBIT) and ISO/IEC 27000 family of standards, although some work has been done to incorporate NIST and the Payment Card Industry Data Security Standard (PCI DSS). The CPMI-IOSCO Guidance is also considered in the surveillance of FMIs.

Regarding the BCB's Supervisory Framework assessment, supervisory practices considered to address cybersecurity include the evaluation of the establishment of:

- Information Security Governance: risk appetite; policies, roles and responsibilities; dissemination of culture; resources (budget, HR, etc.) to implement action plans;
- Information Security Programme: risk mapping; execution of action plans; establishment of controls and mechanisms to ensure the security of information, data and systems; definition of an information security master plan;
- Mechanisms to manage the information life cycle: classification criteria; information life-cycle controls (creation, storage, processing and discard);
- Information security incident treatment: incident classification; monitoring; response plans; crisis management;
- Physical and logical security mechanisms to protect assets;

- Network security mechanisms: periodic security tests; vulnerability scans; monitoring and prevention (e.g. intrusion detection/prevention systems);
- Cyber intelligence: information sharing; trend analysis; and
- Information security policies and controls related to outsourcing.

Future Plans: The Office of Institutional Security of the Presidency of the Republic published in February 2017 the institution of an interministerial working group to prepare a proposal for a National Information Security Policy. Brazil noted that the policy should: (i) recognise information as an economic good and of social value, generating work and income and promoting citizenship; (ii) address social, cultural, economic and technological variables; (iii) promote cooperation between public entities, the business sector and civil society; and (iv) contemplate security of critical national infrastructures and protection of personal and biometric information. Furthermore, Brazil noted that the policy should also ratify society's right to information, treat education and culture as a fundamental foundation for the improvement of information security in Brazil and define a national structure and governance model. Brazil reported that the proposal is being finalised for public consultation.

Brazil also reported that the BCB is evaluating the issuance of specific regulation on information security and cybersecurity and issued a public consultation on the regulation in September 2017. Furthermore, Brazil noted that the BCB's supervisory departments are working towards publicly releasing guidelines on supervisory practices, including IT and information security assessments.

Publicly Available Sources:

Normative Instruction GSI No. 1 on Information Security and Communications in the Federal Public Administration: http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

Institutional Security Office Green Paper on Cybersecurity in Brazil (Portuguese version): http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

BCB Resolution on Risk and Capital Management: http://www.bcb.gov.br/ingles/norms/brprudential/Resolution4557.pdf

BCB Resolution on Operational Risk: http://www.bcb.gov.br/ingles/norms/brprudential/Resolution3380.pdf

BCB Policy Statement (Principles for Financial Market Infrastructures): http://www.bcb.gov.br/pom/spb/ing/Comunique_DEBAN_25097_en.pdf

BCB Resolution on payments system and clearing and settlement systems: http://www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/Resolution2882amended.pdf

BCB Circular on payments system and clearing and settlement systems: http://www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/Circular3057amended.pdf

CVM Instruction 461 (exchanges): http://www.cvm.gov.br/export/sites/cvm/subportal_ingles/menu/investors/anexos/CVM-Instruction-461.pdf

CVM Instruction 541 (centralised securities depository services): http://www.cvm.gov.br/legislacao/inst/inst541.html

CVM Instruction 558 (asset managers and fiduciary administrators):
http://www.cvm.gov.br/legislacao/inst/inst558.html

CVM Risk-Based Supervision Biennial Plan:
http://www.cvm.gov.br/menu/acesso_informacao/planos/sbr/bienio_2017_2018.html

SUSEP Circular 249 on implementation of a system of internal controls in Insurance Companies:
http://www2.susep.gov.br/bibliotecaweb/docOriginal.aspx?tipo=2&codigo=14777

SUSEP Circular 521 on Insurers, Reinsurers, Open Pension Entities Risk Management:
http://www2.susep.gov.br/bibliotecaweb/docOriginal.aspx?tipo=1&codigo=37077

BCB's public consultation website (see Edital 5/2017):
https://www3.bcb.gov.br/audpub/AudienciasAtivas?1

Press release on BCB public consultation: http://www.bcb.gov.br/pt-br/#!/c/notas/16269

Canada

National Strategy: Canada reported that its Cyber Security Strategy and related Action Plan were published in 2010. The Strategy rests on three pillars:

- Securing government systems;
- Partnering to secure vital cyber systems outside the federal government; and
- Helping Canadians to be secure online.

In 2016, a public consultation was conducted to support the government's commitment to review measures to protect critical infrastructure and Canadians from cyber threats, and a report summarising views shared during the consultation was published in January 2017.

Regulations/Guidance: Canada reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, a Staff Notice issued by the Canadian Securities Administrators (CSA), covers **FMIs, trading venues, asset managers, broker-dealers and reporting issuers**. It is targeted to cybersecurity and/or IT risk. The Staff Notice states the expectation that regulated entities will adopt a cybersecurity framework provided by a regulatory authority or standard setting body that is appropriate to their size and scale and identifies a number of reference documents for market participants. It states that there is no one-size-fits-all approach to cybersecurity and that organisations should establish and view their cybersecurity frameworks accordingly. The Notice highlights some of the main themes from the reference documents, including the need for organisations to manage cybersecurity at an organisational level with responsibility for governance and accountability at executive and board levels; establish and maintain a robust cybersecurity awareness programme for staff; consider methodology to protect individual privacy as well as any obligations to report cybersecurity breaches to a regulatory authority; consider whether to share information about cyber incidents with market participants; establish plans to restore capabilities or services that may be impaired due to a cyber incident in a timely fashion; communicate, collaborate and coordinate with other entities; and manage cybersecurity risk exposures that arise from using third-party vendors for services.

The second scheme was also issued by CSA and covers **FMIs and trading venues**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of areas, including the role of the board of directors and a requirement for a report to the board or audit committee of an independent systems review; the ultimate accountability of senior management for day-to-day operations; development and maintenance of internal controls over systems and controls over information security; containment and mitigation of cybersecurity incidents; business continuity and disaster recovery plans; vulnerability assessments and systems testing; and notification to regulators regarding material systems failures and security breaches.

The third scheme, issued by the Office of the Superintendent of Financial Institutions Canada (OSFI), covers **banks, insurance companies, federally regulated trust and loan companies and federally regulated cooperative credit associations**. It is targeted to cybersecurity and/or IT risk. The guidance addresses a number of matters, including the role of the board of directors and senior management, including board review of the implementation of the organisation's cybersecurity framework and implementation plan; staff expertise and enhanced background and security checks of cybersecurity specialists; staff training; adequate funding and resources

to implement the organisation's cybersecurity framework; centrally managed group of cybersecurity specialists responsible for threat intelligence, threat management and incident response; independent control group responsible for cybersecurity risk assessments; regular and comprehensive cyber risk assessments that consider people, processes, data and technology across all business lines and geographies; cyber risk arising from critical IT service providers; tracking of industry developments in cybersecurity; monitoring, analysing and responding to cybersecurity incidents; vulnerability hardware and software scans and testing; penetration testing; inventory of IT assets and business functions and processes; physical protection of assets and access controls; investigation and assessment of cybersecurity incidents; business continuity planning; cyber risk insurance; updating of IT systems; and external communication plans for cybersecurity incidents.

Supervisory Practices: None reported.

Future Plans: None reported.

Publicly Available Sources:

Cyber Security Strategy: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

Action Plan 2010-15 for the Cyber Security Strategy: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf

Cyber Review Consultations Report: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf

CSA Staff Notice on Cyber Security: https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2016/2016sept27-11-332-avis-acvm-en.pdf

CSA National Instrument on Marketplace Operation: http://osc.gov.on.ca/documents/en/Securities-Category2/ni_20170201_21-101_unofficial-consolidation-forms-cp.pdf

CSA National Instrument on Clearing Agency Requirements: http://osc.gov.on.ca/en/SecuritiesLaw_ni_20160218_24-102_clearing-agency-requirements-forms-companion.htm

OSFI Cyber Security Self-Assessment Guidance (Cyber Guidance): http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

OSFI Outsourcing of Business Activities, Functions and Processes: http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_let.aspx

China

National Strategy: China reported a Cybersecurity Law, a National Cyberspace Security Strategy and an International Strategy of Cooperation on Cyberspace.

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

The National Cyberspace Security Strategy is applicable to China's industries, including the financial sector. The strategy is formulated to clarify China's major position on cyberspace development and security; guide China's network security work; and safeguard the country's sovereignty, security and development interests in cyberspace. It is divided into four aspects: opportunities and challenges, goals, principles and strategic tasks.

The International Strategy of Cooperation on Cyberspace is also applicable to China's industries, including the financial sector. It aims to guide China's participation in international exchange and cooperation in cyberspace and encourage the international community to come together to enhance dialogue and cooperation and build a peaceful, secure, open, cooperative and orderly cyberspace and a multilateral, democratic and transparent global internet governance system. It is divided into four aspects: opportunities and challenges, basic principles, strategic goals and a plan of action.

Regulations/Guidance: China reported six schemes of publicly released regulations/guidance that address cybersecurity for the financial sector. The first, issued by the People's Bank of China, covers **FMIs, trading venues, banks and insurance companies**. It is targeted to cybersecurity and/or IT risk. It is based on the basic idea of equal emphasis on technology and management. The scheme addresses a variety of topics, including responsibilities of the board of directors and management; personnel responsible for cybersecurity; reporting procedure for information security incidents; vulnerability scanning; inventory of IT assets, their importance and corresponding protection and management; data security and backup, including confidentiality; physical and data security; access control; security awareness training; intrusion monitoring and surveillance and monitoring of anti-virus, malicious code and other security risks; penetration testing; audit trails; investigation and evaluation of incidents; and risk assessment by outsourced service providers.

The second scheme, also issued by the People's Bank of China, covers **FMIs and banks**. It is targeted to cybersecurity and/or IT risk. This standard applies to organisations that provide electronic certification services in the financial sector, including certification services of third-party electronic certification bodies, electronic certification systems built by a financial institution for its own use and non-bank payment agencies. The guidance addresses various topics, including formation of a committee on security policy, consisting of management and core personnel; risk assessment, including internal and external risk assessment at least annually; archiving and maintaining critical information; confidentiality and encryption; data protection and backup; training of personnel; notification of breaches; backup centres and disaster recovery ability; and business continuity.

The third scheme, also issued by the People's Bank of China, covers **banks**. It is targeted to cybersecurity and/or IT risk. The scheme is a general specification of information security for internet banking systems. It addresses a variety of topics, including role of board of directors and senior management and staffing of various departments; the creation of an inventory of IT assets, including the value of the asset, the owner, administrator and user, the security level and the appropriate security protection measures; data integrity, confidentiality, backup and recovery; physical access control and other physical protection, such as water and fire; access control; staff training and customer education; risk assessment; monitoring; vulnerability scanning; audit trails, including customer login history; security incident procedures; incident response and recovery; contingency planning exercises; data backup; business continuity; and regulatory reporting of significant security incidents within two hours in writing, follow-on reporting every four hours and summary report within seven working days after the end of the event.

The fourth scheme, issued by the China Banking Regulatory Commission (CBRC), covers **commercial banks**. It is targeted to cybersecurity and/or IT risk. It addresses a variety of topics, including formulation of an IT strategy and IT risk assessment and operational plans; role of board of directors and chief information officer; IT risk management department and its reporting lines to chief information officer and chief risk officer; training; testing; zero tolerance for security violation; activity logs; reduction of likelihood of disruptions (including system resilience and dual processing) and impact of disruptions (including by contingency arrangements and insurance); regulatory incident reporting; outsourcing management; risk measurement and monitoring; and information security policy, which should include IT security policy management, organisation information security, asset management, personnel security, physical and environment security, communication and operation security, access control and authentication, acquisition, development and maintenance of information system, information security incident management, business continuity management and compliance.

The fifth scheme, issued by the China Insurance Regulatory Commission, covers **insurance companies**. It is targeted to cybersecurity and/or IT risk. It has currently been published as a draft. The scheme addresses a variety of topics, including establishing of cybersecurity strategy, with clearly defined responsibilities, internal controls and requiring regular assessments and updates based on the risk situation; roles of board of directors, cybersecurity committee and chief information security officer; management system and risk assessment scheme for outsourcing; no outsourcing of management functions of cybersecurity; access controls; training; assessment of cloud computing value and risks; connections of organisation's system with insurance agencies or other third parties; reporting of significant cybersecurity incidents; and cyber risk insurance.

The sixth scheme, issued by the China Securities Regulatory Commission (CSRC), is an Information System Audit Standard for the Securities and Futures Industry that covers **securities and futures exchanges, securities and futures dealers and fund companies**. It is targeted to cybersecurity and/or IT risk. The Standard addresses a variety of topics, including risk assessment; formulation of plans for information security; establishing a committee or leading group for the guidance and management of information security and a department for information security management; vulnerability scanning, attack testing, virus scanning and Trojan Horse detection; inventory of IT assets; requirements for data integrity, confidentiality, backup and recovery; physical protection of assets; access control; staff training; recording and

maintenance of logs required for audit; incident response, recovery and reporting, including producing a summary report within five working days after the emergency disposal of an information security incident ends; and regulatory access to an institution's network for field inspection.

Supervisory Practices: China reported two schemes of supervisory practices. The first, issued by CBRC, covers **commercial banks**. The scheme addresses a variety of topics, including cybersecurity expertise of authorities' IT supervisory officials; off-site supervision, risk evaluations and on-site examinations; review of effectiveness and integrity of banks' cybersecurity management framework and policies; evaluation of governance; review of risk assessment process; review of physical security and network management, mapping and access control policies; review of data backup and recovery policies, data traceability and routine recovery of backup data; review of institutions' vulnerability scanning and repair, penetration tests, access control, anti-virus measures and auditing of user operations; penetration tests by authorities; review of regularity of cybersecurity incident drills and review of past incidents; review of communication plan; review of business continuity management; review of outsourcing security control mechanisms; authorities' communication to regulated entities with regard to defects discovered and enforcement mechanisms; and IT supervisory ratings.

The second scheme, issued by the CSRC, covers **securities and futures exchanges, securities and futures dealers and fund companies**. The scheme addresses a variety of topics, including authorities' access to regulated entities' information security materials; IT governance framework; monitoring and testing; information security inspections by authorities; incident investigation by authorities and internal investigations and remediation by institutions; incident response and recovery; authorities' ability to suspend or restrict operations when an institution fails to meet requirements; information sharing by authorities with industry; and emergency response drills.

Future Plans: China reported that it plans to release the following items within the next year:

- Securities and Futures Fund Management Organization Information Technology Management Regulations;
- Securities and Futures Industry Data Security Classification Guide;
- Securities and Futures Industry Cloud Technology Application Safety Norms;
- Mobile Terminal Application Software Security Testing Standards; and
- Securities and Futures Industry Information System Emergency Case Library.

Publicly Available Sources:

Cybersecurity Law: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

National Cyberspace Security Strategy:
https://www.easyaq.com/newsdetail/id/1642853648.shtml

International Strategy of Cooperation on Cyberspace: http://china.org.cn/chinese/catl/2017-03/07/content_40498343.htm

Note: The links in English above are to non-governmental official translations, and are provided for reference only.

Implementation guide for classified protection of information system of financial industry: http://www.docin.com/p-1100929193.html

Specification for financial electronic authentication: http://doc.mbalib.com/view/35b2ec9c9d33c3ea0c68b3a179022fd5.html

General specification of information security for internet banking system: http://www.doc88.com/p-316626513956.html

Guidelines on the Risk Management of Commercial Banks' Information Technology: http://www.cbrc.gov.cn/chinese/files/2009/20090601A5AC687B78068B60FFDAB8BD0E6FF100.doc

Supervisory Guidelines on IT Outsourcing Risk of Commercial Banks: http://www.cbrc.gov.cn/govView_48B06C23FFA64F6D93EAE2DD9C9DFB7D.html

Information System Audit Standard for Securities and Futures Industry: http://www.csrc.gov.cn/pub/shanghai/xxfw/gfxwj/201503/t20150323_273935.htm

Supervisory Guidelines on IT Outsourcing Risk of Commercial Banks: http://www.cbrc.gov.cn/govView_48B06C23FFA64F6D93EAE2DD9C9DFB7D.html

Measures for Information Security Guarantee and Management in Securities and Futures Industry: http://www.csrc.gov.cn/pub/zjhpublic/G00306201/201209/t20120927_215375.htm

European Union

National Strategy: The first cybersecurity strategy of the European Union (EU) was presented in 2013. Together with the European Agenda on security, it provides the overall strategic framework for the EU initiatives on cybersecurity and cybercrime. This framework is meant to safeguard the online environment, providing the highest possible freedom and security.

The EU cybersecurity strategy lays out a set of actions aimed at: (i) achieving cyber resilience by increasing capabilities, preparedness, cooperation, and information exchange; (ii) reducing cybercrime by strengthening the expertise in the investigation and prosecution phases; (iii) developing an EU cyber defence policy and capabilities; (iv) fostering the industrial and technological resources to stimulate the emergence of an EU cybersecurity industry; (v) enhancing the EU's international cyberspace policy to define norms for responsible behaviour, to advocate the application of existing international law, best practices and guidelines in cyberspace, and to assist countries outside the EU in building cybersecurity capacity.

In July 2016, the Directive on security of network and information systems was adopted by the EU legislature. It aims at ensuring a common level of network and information security across the EU by providing legal requirements boosting the overall level of cybersecurity in the EU by promoting a culture of security across sectors that are vital for the economy and society.

The European Commission published in September 2017 its Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, accompanied by a legislative proposal reviewing the mandate of the European Union Agency for Network and Information Security (ENISA), which proposes a wide-ranging set of measures to build strong cybersecurity in the EU. Furthermore, in its proposal, the European Commission put forward the creation of an EU certification framework for IT security products. Certification plays a critical role in increasing trust and security in products and services that are crucial for the EU and it will help avoiding fragmentation and barriers in the single market.

Regulations/Guidance: The EU reported 10 schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the European Parliament and the Council of the European Union, covers **credit institutions and investment firms**. It addresses operational risk generally. The scheme includes the Regulation on Prudential Requirements for Credit Institutions and Investment Firms (CRR) and the Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV). The scheme stipulates that authorities shall ensure that (i) institutions implement policies and processes to evaluate and manage exposure to operational risk, including model risk, and to cover low-frequency high-severity events; and (ii) contingency plans are in place to ensure an institution’s ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

The second scheme, issued by the European Parliament and the Council of the European Union, covers **payment service providers**. The Directive on payment services (PSD2) is targeted to cybersecurity and/or IT risk. The scheme granted the European Banking Authority (EBA) and the European Central Bank (ECB) the mandate to develop three Regulatory Technical Standards and Guidelines, which are: Regulatory Technical Standard on strong customer authentication and common and secure communication; Guidelines on security measures for operational and security risks of payment service providers; and Guidelines on major incident

reporting. The Draft Guidelines on security measures require that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks. The framework covers governance, risk management and control models, and outsourcing; risk assessment, including the identification, classification and risk assessment of functions, processes and assets; and the protection of the integrity of data, systems and confidentiality, physical security and asset control. The Guidelines also cover the monitoring, detection and reporting of security incidents; business continuity management, scenario-based continuity plans including their testing, incident management and crisis communication; the testing of security measures; situational awareness and continuous learning; and the management of the relationship with payment service users. The Guidelines also cover sharing information with third parties to achieve broader awareness of payment fraud and cybersecurity issues.

The Guideline on major incident reporting sets out criteria, thresholds and methodology to be used by payment service providers in order to determine whether an operational or security incident should be considered major and therefore should be reported to the relevant competent authority, as well as the format and procedures for reporting. The Guidelines also address criteria for competent authorities to take into account when assessing the relevance of an incident, as well as the sharing of incident reports with other domestic authorities, EBA and ECB.

The third scheme, issued by the EBA, covers **banks (in their capacity as payment service providers) and non-bank payment service providers**, such as payment institutions and e-money institutions. It is targeted to cybersecurity and/or IT risk. The EBA issued draft Guidelines on fraud reporting requirements under PSD2 with the aim of ensuring that the high-level provisions of PSD2 related to fraud are implemented consistently across the member states of the EU and the European Economic Area. They also aim to ensure that aggregated statistical data on fraud will be provided to the EBA and the ECB in comparable and reliable fashion.

The fourth scheme (SIPS Regulation), issued by the ECB, covers **systemically important payment systems (SIPS)**. Among other things, it is targeted to comprehensive risk management and operational risk. The scheme covers a number of matters. For example, the scheme requires that a SIPS operator establish a robust operational risk framework that includes appropriate systems, policies, procedures and controls; the SIPS operator shall establish and review at least annually comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats; and the SIPS operator shall establish, test and review at least annually a business continuity plan that addresses events posing a significant risk of disrupting the SIPS' operations. The plan shall incorporate the use of a secondary site and be designed to ensure that critical IT systems can resume operations within two hours following disruptive events. The plan shall be designed to enable the SIPS to complete settlement by the end of the business day on which the disruption occurs, even in case of extreme circumstances.

The fifth scheme, issued by ECB, covers **FMIs, specifically retail payment systems**. It addresses operational risk generally, based on the key elements of Principle 17 of the CPMI-IOSCO Principles.

The sixth scheme, issued by the European Parliament and the Council of the European Union, **covers FMIs, specifically central counterparties and trade repositories**. It is targeted to

cybersecurity and/or IT risk. The scheme covers a number of matters. For example, the scheme requires that a central counterparty maintain a robust information security framework that includes at least access controls; adequate safeguards against intrusions and data misuse; specific devices to preserve data authenticity and integrity, including cryptographic techniques; reliable networks and procedures for accurate and prompt data transmission without major disruptions; and audit trails. This framework shall be reviewed at least on an annual basis and be subject to independent audit assessments.

The seventh scheme, issued by the European Parliament and the Council of the European Union, covers **insurance companies**. It addresses operational risk generally; in such instance, operational risk should be understood as the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events. The scheme covers capital requirements for operational risk. It also requires that national competent authorities ensure that the risk management policy of a company covers identification of operational risks and assessment of the way to mitigate them; activities and internal processes for managing operational risks, including the IT system supporting them; and risk tolerance limits with respect to the company's main operational risk areas. National competent authorities also should ensure that the company has processes to identify, analyse and report on operational risk events, and that the company develops and analyses an appropriate set of operational risk scenarios.

The eighth scheme, issued by the European Parliament and the Council of the European Union, covers **credit rating agencies**. It is targeted to cybersecurity and/or IT risk. The scheme requires that a firm have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems. The scheme also covers the role of senior management, inventory of information processing systems and oversight (including identification, managing and monitoring risks) of outsourced IT systems and IT support.

The ninth scheme, issued by the European Parliament and the Council of the European Union, covers **Central Securities Depositories (CSD)**. It is targeted to cybersecurity and/or IT risk. The IT systems and information security framework in relation to CSD core services are required to be reviewed at least annually and are subject to independent audit assessments, the results of which shall be reported to the CSD's management body and the competent authority. A CSD is required to maintain appropriate IT tools that ensure a high degree of security and operational reliability and have adequate capacity. IT tools shall ensure high standards of security, and the integrity and confidentiality of the information maintained. The information security framework shall include access control; adequate safeguards against intrusions and data misuse; specific devices to preserve data authenticity and integrity, including cryptographic techniques; reliable networks and procedures for accurate and prompt data transmission without major disruptions; and audit trails. The recovery time objective for each critical operation shall not be longer than two hours. The scheme also covers maintenance of a secondary processing site; comprehensive framework for physical security and information security; protection of data from loss, leakage, unauthorised access and other processing risks; notification to authorities of operational incidents; and plans for IT recovery.

The tenth scheme, issued by the European Parliament and the Council of the European Union, covers **FMIs, trading venues, broker-dealers, investment firms and parts of credit institutions**. It is targeted to cybersecurity and/or IT risk. The scheme is contained in the

Markets in Financial Instruments Directive and Regulation (MiFID II and MiFIR). The scheme addresses a number of matters, including IT strategy based on reliable IT organisation and complying with effective IT security management; physical and electronic security to address unauthorised access, system interferences that seriously hinder or interrupt functioning, data interferences that delete, damage or render data inaccessible, and interception of non-public data transmissions; incident reporting to authorities; and annual penetration tests and vulnerability scans.

Supervisory Practices: The EU reported two schemes of supervisory practices. The first, issued by the EBA, covers **payment service providers**. As noted above, these are draft Regulatory Technical Standards and Guidelines under PSD2 regarding strong customer authentication and common and secure communication, security measures for operational and security risks for payment service providers, and major incident reporting. Payment service providers will be required to comply with the aforementioned Regulatory Technical Standards and Guidelines, and supervisors will need to include these within their scope of supervision, from 2018.

The second scheme, issued by the EBA, covers **banks and investment firms**. The ICT Risk Assessment Guidelines provide guidance for EU competent authorities for the IT risk assessment of institutions. The assessment of the institutions' cybersecurity governance, strategy and management is part of the overall assessment of the institutions' general IT risk governance, strategy and management covered in these Guidelines. In summary, while these Guidelines are not specifically focused on cybersecurity, they provide guidance for the general supervisory IT risk assessment also touching on cybersecurity aspects. They address a number of matters, including frequency of supervisory IT risk assessment; review of cybersecurity strategy, framework and governance; framework for effectively identifying, understanding measuring and mitigating IT availability and continuity risks, including material IT security risks, and IT data integrity risks; measures to protect IT systems from attacks from the internet or other external networks; contingency planning; IT system backup and recovery procedures for critical software and data; incident management and escalation process; and framework for identifying, understanding and measuring IT outsourcing risk and controls.

Future Plans: The European Commission is undertaking a public consultation on the digitisation of the financial sector, which includes cybersecurity. The aim is to seek stakeholders' views on whether the EU regulatory framework is fit for the progressive digitisation of financial services. Taking account of the results of this consultation, the European Commission plans to set out policy conclusions around the end of 2017.

The ECB/Eurosystem is currently in the process of updating the SIPS Regulation. The proposed change, due in force in September 2017, sets out specific cybersecurity requirements based on the CPMI-IOSCO Guidance. The regulatory amendment requires that a SIPS operator establish an effective cyber resilience framework with appropriate governance measures in place to manage cyber risk. In addition, a SIPS operator is required to identify its critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyber attacks. These measures are to be regularly tested. A SIPS operator must ensure that it has a sound level of situational awareness of cyber threats. In addition, a SIPS operator shall ensure that there is a process of continuous learning and evolving to enable it to adapt its cyber resilience framework to the dynamic nature of cyber risks, in a timely manner, whenever needed.

The ECB/Eurosystem, in parallel, launched a cyber survey assessment of all payment systems in the euro area in the second quarter of 2017. The survey covered the key elements of a cyber security framework, including governance, identification, protection, detection, response and recovery. The ECB/Eurosystem will use the survey results to conduct further work with the payment systems. In parallel, the ECB/Eurosystem is developing cyber resilience oversight expectations, which will act as a dedicated assessment guide on cybersecurity based on the principles in the CPMI-IOSCO Guidance and an EU red team testing framework for FMIs.

The ECB/Single Supervisory Mechanism has initiated a reporting framework for significant cyber incidents. Since July 2017, all significant institutions from the 19 euro area countries have to report significant cyber incidents as soon as they 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. Some countries already have an incident reporting process in place, requiring significant banks to report noteworthy cyber incidents to their national supervisor. In those countries, the banks will still report incidents to the national supervisors, who will then forward them to the ECB on behalf of the supervised entities.

Publicly Available Sources:

Directive on security of network and information systems (NIS Directive): https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=EN

Legislative proposal reviewing the mandate of the European Union Agency for Network and Information Security: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

EU cybersecurity certification framework: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

EU Regulation on Prudential Requirements for Credit Institutions and Investment Firms (CRR): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0575

EU Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0036

EBA Final Draft Regulatory Technical Standards on the specification of the assessment methodology under which competent authorities permit institutions to use Advanced Measurement Approaches for operational risk in accordance with Article 312 of CRR: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0036

EU Directive on payment services in the internal market (PSD2): http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015L2366

ECB Regulation on oversight requirements for systemically important payment systems: https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf

ECB oversight framework for retail payment systems: https://www.ecb.europa.eu/pub/pdf/other/Revised_oversight_framework_for_retail_payment_systems.pdf

EU Regulation on OTC Derivatives, central counterparties and trade repositories: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0648

Commission Delegated Regulation supplementing the regulation above with regard to regulatory technical standards on requirements for central counterparties (RTS on CCPs): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2013:052:FULL&from=FR

EC Directive on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0138

EC Regulation amending regulation on credit rating agencies: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:146:0001:0033:EN:PDF

Commission Delegated Regulation supplementing EC Regulation above on credit rating agencies with regard to regulatory technical standards on information for registration and certification of credit rating agencies: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22017D0282

EU Regulation on improving securities settlement in the EU and on central securities depositories: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014R0909

EU Directive MiFID II: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

Commission Delegated Regulations supplementing MiFID II: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:087:FULL&from=EN; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.087.01.0350.01.ENG&toc=OJ:L:2017:087:TOC; and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0589.

EU Regulation MiFIR: https://ec.europa.eu/info/law/markets-financial-instruments-mifir-regulation-eu-no-600-2014_en

EBA Draft Guidelines on the security measures for operational and security risks of payment services under PSD2: https://www.eba.europa.eu/documents/10180/1836621/Consultation+Paper+on+the+security+measures+for+operational+and+security+risks+of+payment+services+under+PSD2+%28EBA-CP-2017-04%29.pdf

EBA Draft Guidelines on major incidents reporting under PSD2: http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

EBA Final draft Regulatory Technical Standards on strong customer authentication and secure communication under PSD2: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

EBA Draft Guidelines on fraud reporting requirements under Article 96(6) of Directive (EU) 2015/2366 (PSD2): http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

EU Guidelines on the Supervisory Review and Evaluation Process (SREP):
http://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-

EBA Final Guidelines on the assessment of ICT risk in the context of SREP:
https://www.eba.europa.eu/-/eba-publishes-final-guidelines-to-assess-ict-risk?doAsGroupId=10180

ECB press release on cyber incident reporting:
https://www.bankingsupervision.europa.eu/press/publications/newsletter/2017/html/ssm.nl170517_3.en.html

France

National Strategy: France reported that a national strategy for the defence and security of information systems was published in 2011. The strategy recognised the risk of sabotage against a critical infrastructure as a major threat to national security. In October 2015, a revised strategy was published which emphasised five key objectives:

- Fundamental interests, defence and security of state information systems and critical infrastructures, major cybersecurity crisis;
- Digital trust, privacy, personal data, cyber malevolence;
- Raising awareness, initial training, continuing education;
- The environment of digital technology businesses, industrial policy, export and internationalisation; and
- Europe, digital strategic autonomy, cyberspace stability.

The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), the French national digital security strategy agency, announced in October 2015, is designed to support this strategy.

Regulations/Guidance: France reported two schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Autorité de Contrôle Prudentiel et de Résolution (ACPR), the Autorité des Marchés Financiers (AMF) and the Banque de France (BdF), covers **FMIs, trading venues, banks, insurance companies, broker-dealers, asset managers, pension funds, payments domain and data reporting services providers**. It addresses operational risk generally.

- FMIs are required to apply the operational risk principle (Principle 17) of the CPMI-IOSCO Principles. In conducting risk-based oversight of FMIs, BdF uses the CPMI-IOSCO Guidance.
- Credit institutions are entrusted with the obligation to have an IT security commensurate with their business needs and the cybersecurity of institutions is expected to be handled so as to comply with principle-based regulatory requirements.
- Asset management companies are required to establish and maintain effective systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question. Furthermore, EU regulation specifies requirements for investment firms, trading venues, data reporting service providers, central counterparties and central depositories.

The second scheme, issued by ACPR, covers **banks, insurance companies and investment firms**. It is targeted to cybersecurity and/or IT risk. The guidance focuses specifically on cloud computing and recommended measures to take, such as encryption, when sensitive data is stored in public cloud computing infrastructures. The guidance addresses oversight by senior management in the decision to outsource data or systems in a public or hybrid cloud computing environment and in keeping control of the outsourced service. The guidance also addresses risk assessment prior to outsourcing; continuing responsibility of financial institutions for data integrity and confidentiality, as well as business continuity; control of access management; and

auditing of the service provider by the outsourcing institution and the supervisor; business continuity.

Supervisory Practices: France reported one scheme of supervisory practices, issued by ACPR, that covers **FMIs, banks and insurance companies**. For significant institutions, action is decided by the ECB. For less significant institutions, the ACPR takes action. A cybersecurity self-assessment questionnaire was launched for these institutions in the second quarter of 2017. For other entities under AMF supervision, the AMF can send specific questionnaires on cybersecurity. On operational risk matters for systemically important payment systems, central counterparties, central securities depositories and securities settlement systems, BdF bases its action on various EU regulation and on the CPMI-IOSCO Principles.

Future Plans: ACPR developed a self-assessment questionnaire directed to less significant institutions (LSIs). This questionnaire, structured along six thematic blocks (governance, risk identification, protection, detection, response and recovery) has been completed by LSIs and is currently being processed. A public dissemination of the results will be presented before the year-end.

BdF engaged with the major French FMIs in an exercise to gauge the state of the cyber resilience of FMIs, in the form of a self-assessment which took place in May-June 2017. The exercise will produce a score for the FMIs, a spot on a heat map (so that the FMI can compare itself with the current European cyber-resilience state of art) and some regulatory advice in order to remedy any weaknesses identified.

Publicly Available Sources:

2011 Cybersecurity Strategy: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

2015 National Cybersecurity Strategy: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Explanatory webpage for measures introduced by the Military Law Chapter IV: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

ACPR guidance on cloud computing: http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/analyses-syntheses/201307-The-risks-associated-with-cloud-computing.pdf

Germany

National Strategy: The Federal Ministry of the Interior in Germany has released a strategy for cybersecurity, which has four key elements:

- Remaining safe and autonomous in a digital environment;
- Government and private industry working together;
- Strong and sustainable cybersecurity architecture for every level of government; and
- Germany's active role in European and international cybersecurity policy.

Regulations/Guidance: Germany reported seven schemes of regulations/guidance that address cybersecurity for the financial sector. The first of these is the German IT Security Act, issued by the German Parliament, which covers **FMIs, trading venues, banks, insurance companies, pension funds, providers of critical infrastructure in sectors other than the financial sector and cash centres**. It is targeted to cybersecurity and/or IT risk. The regulation applies to providers of critical infrastructure. Providers of critical infrastructure are obliged to implement appropriate organisational and technical measures to avoid breaches of availability, integrity, authenticity and confidentiality of all IT systems, components or processes which are essential for the functioning of their operated critical infrastructures. Certain financial institutions and their service providers may be identified as providers of critical infrastructure.

The second scheme is contained in the German Banking Act, also issued by the German Parliament, and covers **banks.** It addresses operational risk generally. The Act requires institutions to ensure a proper business organisation, which encompasses adequate and effective risk management. This includes suitable technical and organisational resources and adequate contingency plans for IT systems as essential parts of a proper business organisation. On the basis of the German Banking Act, the Federal Financial Supervisory Authority (BaFin) has developed a circular on Minimum Requirements for Risk Management (third scheme, below), which provides a principles-based framework that gives institutions discretion to develop individual solutions for the implementation of adequate and effective risk management.

The third scheme, issued by BaFin, is the Minimum Requirements for Risk Management, and covers **banks**. It addresses operational risk generally. The underlying principles-based approach gives institutions discretion while implementing adequate and effective controls. This means that company-specific risks, the complexity of a company's business model and the nature and scale of its business should be taken into account when following the requirements. Institutions are to adopt appropriate measures to take account of operational risk, identify and assess any material operational risk at least once a year and analyse the causes of material damage events promptly. The management board is to be informed at least once a year of any such events and of material operational risk in a report. This report is to serve as a basis for deciding whether, and, if so, what measures are to be taken to eliminate the causes or what risk management measures are to be taken (e.g. insurance, backup procedures, reorientation of business activities, catastrophe protection measures). Monitoring of the implementation of these measures is required.

The fourth scheme, also issued by BaFin, covers **banks**. It is currently in draft form and would, if finalised, be targeted to cybersecurity and/or IT risk. This scheme is based on the second and third schemes above (German Banking Act; Minimum Requirements for Risk Management).

This scheme covers a number of areas, including definition of an IT strategy by the management board, the establishment of an independent information security officer who regularly reports to the board, maintenance of an inventory of the components of IT systems, access controls, training, acceptance testing of newly developed and changed applications, investigation and follow-up of information security incidents updating of IT systems, and risk assessment and monitoring with respect to external procurements.

The fifth scheme, issued by BaFin, covers **banks, payment institutions and e-money institutions**. It addresses operational risk generally. The guidance describes measures to ensure the security of internet payments, dealing with the following aspects: governance, risk assessment, incident monitoring and reporting, risk control and mitigation, traceability of transactions, initial customer identification and customer information, strong customer authentication, enrolment in and delivery of authentication tools, maximum login attempts and session time outs, transaction monitoring, protection of sensitive payment data and customer education.

The sixth scheme is contained in the German Insurance Supervision Act, issued by the German Parliament, and covers **insurance companies and pension funds**. It addresses operational risk generally. The Act requires insurance companies and pension funds to have in place a proper business organisation, including proper management of IT infrastructure. These governance requirements also apply to outsourced functions and activities.

The seventh scheme is contained in the Securities Trading Act, issued by the German Parliament, and covers **broker-dealers and asset managers**. It addresses operational risk generally. The Act requires a proper business organisation, parallel to the German Banking Act. This includes suitable technical and organisational resources, which implies a proper risk management and an appropriate level of IT security. In parallel with the Minimum Requirements for Risk Management (third scheme, above), Minimum Requirements for Risk Management in Asset Management have been published.

Supervisory Practices: None reported.

Future Plans: Development of supervisory requirements for the IT of insurance companies.

Publicly Available Sources:

Cybersecurity Strategy:
http://bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.html

Information Security Act: https://www.gesetze-im-internet.de/bsig_2009/

German Banking Act: https://www.gesetze-im-internet.de/kredwg/__25a.html

Minimum Requirements for the Risk Management of Banks:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html

Supervisory Requirements for the IT of Banks:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2017/kon_0217_bankaufsichtliche_anforderungen_it_ba.html

German Insurance Supervision Act: https://www.gesetze-im-internet.de/vag_2016/__23.html

Securities Trading Act: https://www.gesetze-im-internet.de/wphg/BJNR174910994.html

Hong Kong

National Strategy: The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) was established in 2015 to centrally coordinate the computer emergency response and incident handling within the government. Outside the government, GovCERT.HK proactively collaborates with the Hong Kong Computer Emergency Response Team Co-ordination Centre ("HKCERT"), the industry and critical internet infrastructure in providing and disseminating information and advice on cybersecurity to enterprises and the public, so that they can have a better understanding of various potential security risks and the corresponding mitigation measures, thereby enhancing the cybersecurity capabilities of Hong Kong as a whole against the challenges of emerging cyber threats. GovCERT.HK and HKCERT also keep close contact with computer emergency response teams (together with computer security incident response team referred to hereinafter as CERT)) of other places to share information on cybersecurity threats and coordinate incident response.

The government adopts various information security standards such as the ISO/IEC 27001 and applies the corresponding techniques to develop its comprehensive set of security documents, including the information security regulations, policies, guidelines and procedure. The government also promotes the adoption of international standards and best practices among business sectors (including, but not limited to, the financial sector) through active collaboration with different stakeholders from the industry, academia and professional bodies.

Regulations/Guidance: Hong Kong reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Hong Kong Monetary Authority (HKMA), covers **FMIs and banks**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of areas, including adoption of cybersecurity strategy, roles of the board and senior management, board expertise, risk assessment, inventory of IT assets, identification of critical business processes that are dependent on external connections, data protection controls, physical security controls, access controls, staff training, continuous monitoring against cybersecurity risk, penetration testing and vulnerability scanning, audit log records, business impact analysis of cyber incidents, process to contain and control cyber incidents, communication procedures, disaster recovery, cyber insurance, sharing of cyber threat intelligence, notice to regulators of cyber incidents, supervisor's access to information and available supervisory actions. For **stored value facilities** (SVF), based on the Guideline and Practice Note on Supervision of Stored Value Facilities Licensees issued by HKMA, an SVF licensee should guard against current and upcoming cybersecurity risks associated with its SVF by monitoring the trends in cyber threats, implementing adequate protective measures and performing periodic security testing.

The second scheme, issued by the Insurance Authority, covers **insurance companies**. It addresses operational risk generally. It specifies that authorised insurers are required to have policies and procedures that are commensurate with the scale and complexity of their business to identify, detect and mitigate cybersecurity threats. Periodic testing of the mitigation measures, and regular review and assessment of the cybersecurity policies and procedures, are also required to ensure the ability of authorised insurers to deal with cybersecurity threats in a timely and effective way.

The third scheme, issued by the Hong Kong Securities and Futures Commission (SFC), covers **intermediaries** such as **broker-dealers** and **asset managers**. It addresses operational risk

generally. The scheme sets out general principles and specific requirements on system security, backup and contingency planning that apply to a licensed or registered person who conducts electronic trading of securities and futures contracts that are listed or traded on an exchange.

Supervisory Practices: Hong Kong reported two schemes of supervisory practices. The first scheme, issued by HKMA, covers **FMIs and banks**. For banks, the HKMA has a dedicated specialist supervision team on cybersecurity and technology risk, composed of supervisory officers with relevant experience and professional qualifications, who receive ongoing training. Under a risk-based supervisory approach, HKMA maintains risk profiles of banks' operational and technology risk and banks are classified into different supervisory priorities, which are subject to different examinations/review cycles. In addition, banks that have more material technology risk are requested to engage qualified assessors (e.g. internal or external auditors) to conduct regular independent assessment of their technology controls, and all banks are requested to conduct the Cyber Resilience Assessment Framework (C-RAF) on their cybersecurity controls. The HKMA's specialist supervision team performs sample validation or follow-up reviews of these assessments. The HKMA also performs post-mortem reviews of banks' technology incidents. For FMIs, HKMA involves an external IT security consulting firm to help assess the cybersecurity adequacy of firms based on the requirements of C-RAF and to recommend measures to close any gaps. The HKMA FMIs oversight team reviews the assessments and the recommendations of the consulting firm and monitors the compliance work done by the firms to ensure that they are in compliance with the C-RAF requirements. On-site examinations will be conducted if needed.

The second scheme is issued by the SFC. Since 2014, the SFC has conducted a number of internet trading and cybersecurity reviews, with assistance from an external consultant and issued circulars to draw the industry's attention to the common deficiencies and vulnerabilities identified. The SFC suggested a wide range of control measures, including a self-assessment questionnaire, to supplement the existing principles and requirements in the SFC Code of Conduct. The last of these reviews was the 2016 cybersecurity review, which focused on hacking risks associated with internet trading.

Future Plans: The SFC conducted a two-month public consultation on proposed guidelines that contain 20 cybersecurity baseline requirements for any licensed or registered person that conducts internet trading of securities and futures contracts that are listed or traded on an exchange or internet trading of securities that are not listed or traded on an exchange. The consultation ended in early July 2017 and the feedback was generally supportive. Feedback details are being deliberated for fine-tuning and enhancing the proposed baseline requirements. The SFC aims to conclude the consultation and issue the guidelines in October 2017.

Publicly Available Sources:

Cybersecurity Fortification Initiative (for banks and FMIs):
http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf

Circular on Cybersecurity Risk Management (for banks and FMIs):
http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf

Circular on Enhanced Competency Framework on Cybersecurity (for banks): http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf

Supervisory Policy Manual, General Principles for Technology Risk Management (for banks): http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf

Supervisory Policy Manual, Risk Management of E-banking (for banks): http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf

Circular on security controls related to internet banking services (for banks): http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160526e1.pdf

Circular on Customer Data Protection (for banks): http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf

Supervisory Policy Manual on Outsourcing (for banks): http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf

Supervisory Policy Manual on Business Continuity Planning (for banks): http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2002/tm-g-2.pdf

Banking Ordinance: http://www.blis.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/5A827AA51F496D08482575EE004568BC/$FILE/CAP_155_e_b5.pdf

Guideline on Supervision of Stored Value Facility Licensees: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Guidelines-on-supervision-of-SVF-licensees_Eng.pdf

Practice Note on Supervision of Stored Value Facility Licensees: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/PN_on_supervision_of_SVF_licensees_eng.pdf

Guideline on the corporate governance of authorised insurers: https://www.ia.org.hk/en/legislative_framework/files/GL10.pdf

Payment systems and stored value facilities ordinance (for FMIs and stored value facilities): http://www.blis.gov.hk./blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/C5DBCF5A5D99246D482575EF001F294D/$FILE/CAP_584_e_b5.pdf

The Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission: http://www.sfc.hk/web/EN/assets/components/codes/files-current/web//code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission.pdf

Fund Manager Code of Conduct: http://www.sfc.hk/web/EN/assets/components/codes/files-current/web/codes/fund-manager-code-of-conduct/Fund%20Manager%20Code%20of%20Conduct.pdf

SFC Cybersecurity Review on Internet/Mobile Trading Systems: http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=16PR103; http://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/openFile?refNo=16EC46

Consultation paper on proposals to reduce and mitigate hacking risks associated with internet trading: http://www.sfc.hk/edistributionWeb/gateway/EN/consultation/intermediaries-supervision/doc?refNo=17CP4

Circular to All Licensed Corporations Alert for Ransomware Threats: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC26

Circular to All Licensed Corporations Alert for Cybersecurity Threats: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=17EC8

Circular to All Licensed Corporations on Cybersecurity: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=16EC17

Circular to All Brokers Tips on Protection of Online Trading Accounts: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=16EC3

Circular to All Licensed Corporations on Internet Trading Internet Trading Self-Assessment Checklist: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=15EC34

Circular to Licensed Corporations Mitigating Cybersecurity Risks: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC49

Circular to All Licensed Corporations on Internet Trading Information Security Management and System Adequacy: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC48

Circular to All Licensed Corporations on Internet Trading Reducing Internet Hacking Risks: http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC3

India

National Strategy: India reported that the key elements of its National Cyber Security Policy include:

- Creation of a secure cyber ecosystem and an assurance framework;
- Encourage open standards;
- Strengthening the regulatory framework;
- Creation of mechanisms for security threat early warning;
- Vulnerability management and response to security threats;
- Protection and resilience of critical information infrastructure;
- Promotion of research and development in cybersecurity;
- Human resource development;
- Creation of cybersecurity awareness; and
- Information sharing and cooperation.

Regulations/Guidance: India reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Reserve Bank of India (RBI), covers **banks**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of areas, including cybersecurity policy appropriate to complexity of business and appropriate levels of risk approved by board, roles of board; board-level IT Strategy Committee, senior management and chief information security officer; evaluation of risks and controls in place; periodic vulnerability assessment and penetration testing, and prompt remediation, for all critical systems throughout life cycle, including pre-implementation, post-implementation and after modifications; inventory of IT assets, business data and information, business applications, key personnel and services, including criticality and sensitivity classifications; data protection applicable to data stored internally and at vendor managed facilities and to transmitted data; data backup; physical security; access control; staff training and customer education and awareness; audit trails; incident response and recovery, including communication and coordination with stakeholders; insurance to replace IT resources in event of disaster; information sharing; updating systems; and reporting to regulation within two to six hours of incident detection.

The second scheme, issued by the Securities and Exchange Board of India (SEBI), covers **FMIs and trading venues**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of areas, including board-approved cybersecurity policy, chief information security officer, continuous security monitoring and monitoring of capacity utilisation, inventory of IT assets, physical access control, training, regular vulnerability assessment and periodic penetration tests and immediate remediation, user access logs, network security devices and intrusion detection and prevention systems, anti-virus software, regulatory reporting and sharing of reported information by regulator with other regulated entities in anonymous manner, and incident response and recovery.

The third scheme, issued by the Insurance Regulatory and Development Authority of India (IRDAI), covers **insurance companies**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of areas, including board-approved cyber security policy; role of senior

management, including an Information Security Committee headed by a senior level executive with a reporting line to the board to take overall responsibility for the information security governance framework; role of chief information security officer; risk assessment, categorisation, treatment, transfer and mitigation; inventory of assets associated with information and information processing facilities; physical and environmental security; access control; training; surveillance, vulnerability assessments and penetration tests; audit trail of critical data access; incident response and resumption of services; contingency planning and regular testing thereof; incident reporting; business continuity; IT infrastructure updates; information security with respect to vendors and other third parties who have access to systems and data; reporting to regulator of incidents critically affecting business within 48 hours upon knowledge; regulatory access to information; cloud security; and mobile security.

Supervisory Practices: India reported one scheme of supervisory practices, issued by the Board for Financial Supervision, that covers **banks**. The scheme covers a number of areas, including cybersecurity expertise of supervisory team members; review of cybersecurity framework and board involvement in cybersecurity; assessment of cybersecurity framework, policies and procedures and risk assessment process; review of systems security controls, training, monitoring, testing, auditing and incident preparedness; supervisory access to records held by third parties and supervisory actions.

Future Plans: The Government of India has announced a proposal to establish a CERT for the financial sector (CERT-Fin), to work in close coordination with all financial sector regulators and other stakeholders. A Working Group including, among others, all financial sector regulators, was set up to study and recommend measures for setting up a computer emergency response system in the financial sector. The report of the Working Group for setting up CERT-Fin was submitted in May 2017 and published in the public domain for comment.

In February 2017, the RBI constituted an inter-disciplinary Standing Committee on Cyber Security to review threats inherent in existing and emerging technology, study adoption of various security standards and protocols, interface with stakeholders and suggest appropriate policy interventions to strengthen cybersecurity and resilience in the banks and other regulated entities of the RBI.

In August 2016, SEBI constituted a High Powered Steering Committee on Cyber Security (HPSCCS) to, among other things, oversee and provide overall guidance on cybersecurity initiatives for SEBI and for the entire capital market, advise SEBI in developing and maintaining cybersecurity and cyber resilience requirements aligned with global best practices and industry standards and identify measures to improve cyber resilience and related business continuity and disaster recovery processes in the Indian securities market.

Publicly Available Sources:

National Cyber Security Policy:
http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

Circular on the establishment of cyber security frameworks in banks:
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

Guidelines on the implementation of recommendations of the working group on Information Security, Electronic Banking, Technology Risk Management and Cyber Fraud: https://rbi.org.in/SCRIPTs/BS_CircularIndexDisplay.aspx?Id=6366

Circular on Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories: http://www.sebi.gov.in/sebi_data/attachdocs/1436179654531.pdf

Guidelines on Information and Cyber Security for insurers: https://www.irdai.gov.in/ADMINCMS/cms/frmGuidelines_Layout.aspx?page=PageNo3118&flag=1

Report of Working Group for setting up Computer Emergency Response Team in the Financial Sector: http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf

Terms of Reference and Membership of SEBI Steering Committee on Cyber Security: http://www.sebi.gov.in/sebiweb/about/AboutAction.do?doMember=yes&committeesId=38

Indonesia

National Strategy: None reported.

Regulations/Guidance: Indonesia reported four schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Financial Services Authority (OJK), covers **banks**. It addresses operational risk generally, providing guidance on how to implement risk managements in the use of IT for operational activity. Topics covered include the scope of IT; implementation of risk management in the use of IT, including supervision by the board of commissioner and director, risk management process, and control system and internal audit; IT implementation by banks and IT service providers, including data centre and disaster recovery centre location, transaction processes by IT service providers, and bank IT services; electronic banking; and IT implementation report.

The second scheme, also issued by OJK, covers **FMIs, broker-dealers and asset managers**. It addresses operational risk generally. Broker-dealers and FMIs are required to have a business plan that includes a security plan against cybercrime (unauthorised access, virus attack, software sabotage, password breach) and backup system and conduct regular cybersecurity tests. Asset managers are required to have an organisational function for IT, conduct continuous review and maintenance of their IT systems and processes to ensure proper operational upkeep and compliance with regulations on electronic reporting, and periodically back up all their IT systems. Users of Indonesia's Integrated Investment Management System (S-INVEST) are required to maintain secrecy and confidentiality of user information and maintain a disaster recovery centre within the jurisdiction of Indonesia and significantly remote from the main data centre of the user.

The third scheme, issued by the Bank of Indonesia, covers **FMIs, banks and non-bank institutions**. It addresses operational risk generally. For payment transaction processing operations, the scheme covers responsibility for ensuring and implementing an information security standard, system security and reliability eligibility required to obtain a license, and submission of an information system audit report. For card-based payment instruments, the scheme covers a number of areas, including two-factor authentication, data confidentiality, data and system integrity, system availability, audit trail, business continuity plan, IT audit report from an independent auditor and use of chip technology and online PIN. For e-money operations, the scheme covers business continuity planning, as well as periodic IT audit by external audit covering operational security; network, application and system security; data or information security; environment and physical security, including control on data and system access; system change management; system implementation management; and written procedures. For fund transfer operations, the scheme covers database security, backup, internal control and audit trail, as well as an IT audit report from an independent auditor.

The fourth scheme, issued by the OJK, covers **peer-to-peer lending activity**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including establishment of a strategic plan; the role of the board of directors, which must conduct comprehensive supervision related to IT risk; prevention and resolution that addresses threats, cyber attacks and loss; monitoring, assessing and addressing IT gaps regularly in order to support business process; confidentiality and availability of data; training; testing; independent IT audit; incident handling management process; regulatory and customer reporting within one hour of a system

failure with serious impact; business continuity planning; system updates; and regulatory access to information.

Supervisory Practices: Indonesia reported three schemes of supervisory practices. The first, issued by OJK, covers **banks**. The scheme covers specialist supervisory teams for review and assessment of cybersecurity of a bank when it plans to develop or implement a system; annual submission by banks of IT development plan and requested follow-on documentation relating to risk mitigation; required documentation for e-banking, including infrastructure diagram, physical and logical security, audit report and penetration testing report; cyber threat reporting; supervisory review of third-party interconnections, data security, system security, training, monitoring, testing, auditing, incident handling procedure and implementation, and business continuity plan; and joint public-private testing of cybersecurity readiness.

The second, also issued by OJK covers **FMIs and broker-dealers**. OJK reports that supervision with respect to FMIs and broker-dealers is included within the risk-based supervision and regular audit programme for these entities. If cybersecurity incidents are found at a financial institution, it is an alert for supervisory focus and a follow-up normally will be undertaken to check whether the same incidents occurred at other institutions and how it will impact the sector overall.

The third, issued by the Bank of Indonesia, covers **FMIs, banks, and non-bank institutions**. Related to payment transaction processing operation, the Bank of Indonesia supervise FMIs, banks and non-bank institutions' operational risks, including their IT risks. In the licensing process, the Bank of Indonesia assess the adequacy of operational readiness, system security and reliability, risk management and customer protection. During the off-site and on-site supervision, the Bank of Indonesia also audit the adequacy of information system control, business continuity plans, disaster recovery and information security providers. Furthermore, the Bank of Indonesia requires the providers to submit independent information system audit reports once every three years.[17]

Future Plans: None reported.

Publicly Available Sources:

Regulation concerning the Implementation of Risk Management in the Use of IT by Commercial Banks: http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf

Regulation concerning IT Standard Rural Bank and Syariah Rural Bank have to implement for their operational activity: http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/POJK-tentang-Standar-Penyelenggaraan-Teknologi-Informasi-bagi-Bank-Perkreditan-Rakyat-dan-Badan-Pembiayaan-Rakyat-Syariah.aspx

Regulation concerning Securities Exchange: http://www.ojk.go.id/en/kanal/pasar-modal/regulasi/klasifikasi-bapepam/bursa-efek/Default.aspx

[17] This scheme is included in Table 1 and Table 3 in the main body of the report but is not included in other data because complete survey information has not been submitted for the scheme.

Regulation concerning Clearing Guarantee Institutions: http://www.ojk.go.id/en/kanal/pasar-modal/regulasi/klasifikasi-bapepam/lembaga-kliring-dan-penjaminan/Default.aspx

Regulation concerning Central Securities Depository: http://www.ojk.go.id/en/kanal/pasar-modal/regulasi/klasifikasi-bapepam/lembaga-penyimpanan-dan-penyelesaian/Default.aspx

Regulation concerning Internal Control and Bookkeeping of Securities Companies: http://www.ojk.go.id/en/kanal/pasar-modal/regulasi/klasifikasi-bapepam/perusahaan-efek/Default.aspx

Regulation concerning IT-based Direct Lending and Borrowing Services: http://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/peraturan-ojk/Pages/POJK-Nomor-77-POJK.01-2016.aspx

Circular letter on governance and risk management regarding IT-based direct lending and borrowing services: http://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/surat-edaran-ojk-dan-dewan-komisioner/Pages/SEOJK-Tata-Kelola-dan-Manajemen-Risiko-Teknologi-Informasi-pada-Layanan-Pinjam-Meminjam-Uang-Berbasis-Teknologi-Informasi.aspx

Circular letter intended for All Commercial Banks in Indonesia regarding Risk Management in the Use of IT by Commercial Banks: http://www.ojk.go.id/en/kanal/perbankan/regulasi/surat-edaran-bank-indonesia/Documents/sebi093007_eng_1392373361.pdf

Regulation on Payment Transaction Processing Operation: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/pbi_184016.aspx

Circular Letter on Payment Transaction Processing Operation: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/SE_184116.aspx

Circular Letter on Card Based Payment Instrument Operation: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/se_111009.aspx

Circular Letter on Implementation of Chip Technology National Standard and Utilisation of 6 Digits Online Personal Identification Number for ATM Cards and/or Debit Cards Issued in Indonesia: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/se_175215.aspx

Circular Letter on Electronic Money Operation: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/se_161114.aspx

Circular Letter on Fund Transfer Operation: http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/se_152313.aspx

Italy

National Strategy: Italy reported that its National Cyber Security Strategy responds to the challenges affecting cybersecurity in Italy and consists of two strategic documents. These are:

- The National Strategic Framework for Cyberspace Security, which identifies goals, roles and tasks for the public and private sectors in handling cyber threats; and
- The National Plan, which identifies a set of priorities and actions for implementing the Strategy and achieving the goals. Tasks and action plans assigned to each entity are intended to reduce vulnerability, enhance risk prevention capability, provide timely response to cyber attacks and enable the quick and safe resumption of critical digital services in case of disruption.

Regulations/Guidance: Italy reported seven schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Bank of Italy (BDI), covers **FMIs, specifically retail payment systems**, in accordance with the Eurosystem Oversight Policy Framework. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including establishment of a cybersecurity framework, oversight roles, risk governance, risk analysis and the IT security management process (including asset identification and protection, detection and incident handling, and response and recovery), and business continuity and disaster recovery.

The second scheme, issued by BDI, the National Commission for Companies and the Stock Exchange (CONSOB) and the EU, covers **FMIs, specifically post-trading infrastructure** in accordance with the Eurosystem Oversight Policy Framework. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including establishment of a cybersecurity framework, oversight roles, risk governance, risk analysis and the IT security management process (including asset identification and protection, detection and incident handling, and response and recovery), and business continuity and disaster recovery.

The third scheme, issued by BDI, covers **banks.** It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including establishment of a cybersecurity framework; oversight, management and IT security roles; risk analysis; creation and updating of inventory of IT resources, including hardware, software, data and procedures; physical and logical security safeguards; user training and awareness; monitoring, including through access logs; incident handling and prompt regulatory reporting; IT outsourcing agreements; and supervisory access to information.

The fourth scheme, issued by BDI, covers **payment institutions and e-money institutions** and implements the EBA Final Guidelines on the Security of Internet Payments. It is targeted to cybersecurity and/or IT risk. In general, the regulation provides requirements for IT security, including physical and logical controls, backup and disaster recovery. It describes the roles and responsibilities of the board of directors and senior management. Institutions should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the services and regularly thereafter. Other matters covered include customer education and awareness; monitoring, logs and audit trails; incident handling and reporting; IT security of third-party interconnections; and supervisory access to information and supervisory tools and sanctions.

The fifth scheme, issued by BDI, covers **asset managers, financial intermediaries, investment firms and custodian banks**. It addresses operational risk generally. The regulations are principles-based and are focused on the efficiency and effectiveness of the institution's information systems. The information systems should be adequate to the risks; data should be available, reliable, updated and stored with adequate granularity; and information security should be assured. With respect to information security, the regulation addresses logical and physical security; data backup, disaster recovery and business continuity; access rights and user authentication; and traceability.

The sixth scheme, issued by BDI and CONSOB, covers **trading venues and banks and investment firms operating a multilateral trading facility**. It is targeted to cybersecurity and/or IT risk. This scheme covers a number of matters, including internal audits of IT systems, with information on the audit plans and the relevant audit outcomes provided to the authorities; business continuity and recovery plans; physical and logical safeguards; ongoing monitoring with respect to cybersecurity risks, including where outsourcing arrangements are in place; incident reporting to authorities; and authorities' access to information.

The seventh scheme, issued by the Institute for Insurance Supervision (IVASS), covers **insurance companies**. The regulation currently in force addresses operational risk generally and requires internal procedures to ensure the security of hardware, software and databases, including processes to maintain business continuity, with proper continuity and disaster recovery plans and related organisational, IT and communication measures. A full revision of the regulation has been issued for public consultation, addressing IT governance, cybersecurity, incident reporting and other IT risk issues.

Supervisory Practices: Italy reported two schemes of supervisory practices. The first, issued by BDI and CONSOB covers **retail payment systems and post-trading infrastructures** in accordance with the Eurosystem Oversight Policy Framework and the Eurosystem Oversight Cyber Resilience Strategy for FMIs. The scheme addresses review of a number of matters, including policy and procedures relating to cybersecurity; cyber risk assessment and mitigation measures; physical security controls; data security, including authentication and authorisation, cryptography, security systems such as anti-malware and data loss detection and prevention, monitoring and logging, backup, and data governance and classification; training and awareness; testing and auditing; readiness to assess, mitigate and recover from cybersecurity incidents; communications plans; outsourcing; and authorities' right to access and audit third-party providers; sanctions.

The second scheme, issued by the BDI and CONSOB, **covers trading venues and banks and investment firms operating a multilateral trading facility**. Reviews are carried out on an ongoing basis through off-site, desk-based reviews and routine and non-routine on-site inspections. The supervisory approach is risk-based. Desk-based reviews are based on ongoing and periodic reporting from market operators and ad hoc requests. As regards periodic and ongoing reporting relevant for cybersecurity purposes, market operators are required to provide authorities with regular (at least on a yearly basis) reporting on their internal organisation, policies and procedures, including, among others, on the measures adopted to identify, mitigate and manage the risks to which they are exposed (including systems disruptions), on the contingency arrangements established to cope with risks of system disruptions, as well as on any other arrangements for the sound management of the technical operations and resilience of their systems. Authorities receive the results of the main internal controls and tests actually

implemented within market operators at various organisational levels. Authorities also receive business continuity plans for the management of critical situations and recovery systems to back up data on a periodic basis. Market operators should promptly submit incident reports to competent authorities. Authorities receive information on the characteristics of any new IT infrastructure/system or major changes to existing ones. Trading venue operators must also submit to authorities an audit plan relating to the auditing of the main IT structures, including the IT security measures and planned business continuity procedures. Authorities must be informed of the results of such audits once performed without delay, together with the measures adopted or to be adopted to remedy any deficiency.

Future Plans: Italy reported that BDI is currently reviewing its Strategic Plan for 2017-19, which envisages action plans focused on the digital innovation and resilience of financial services, including the enhancement of cyber resilience for the Italian financial sector. BDI reported that, within the next year, it will update its incident (including cyber incident) reporting framework in order to align the current BDI regulation regarding banks and payment institutions to the requirements of recent European directives.

Both BDI and CONSOB have identified adapting national supervisory actions to the upcoming EU directive on markets in financial instruments (MiFID II) as a priority.

CONSOB's Strategic Plan for 2016-18 envisages supervisory actions on the risks posed by financial innovation and, specifically, on the means employed by market infrastructures and financial professional operators to ensure cybersecurity and resiliency of their IT systems.

Publicly Available Sources:

National Strategic Framework for Cyberspace Security:
http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

National Plan for Cyber Protection and Information Security:
http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

Consolidated Law on Banking (CLB):
http://www.bancaditalia.it/compiti/vigilanza/intermediari/Testo-Unico-Bancario.pdf

Under the CLB, the BDI issued the following regulations:

Guidelines for business continuity for FMIs: https://www.bancaditalia.it/compiti/sispaga-mercati/codise/Guidelines_business_continuity_market_infrastructures.pdf?language_id=1

Oversight regulation on retail payment systems: https://www.bancaditalia.it/compiti/sispaga-mercati/sistemi-pagamenti/Provvedimento_sistemi_retail.pdf

Consolidated Law on Finance (CLF):
http://www.consob.it/mainen/documenti/english/laws/fr_decree58_1998.htm

Regulation on bank supervision:
https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_19_Aggto_Testo_integrale.pdf

Supervision regulation on Payment institutions and e-money institutions: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/disp-ip-20120620/Disposizioni_IP_con_frontespizio.pdf

Supervision regulation on asset managers: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/regolamenti/20120508/Regolamento_Gestione_collettiva_risparmio_1_aggiornamento.pdf; and https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/regolamenti/20071029/Regolamentocongiunto_291007.pdf

Supervision regulation on security firms: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c164/iv_imm_164.pdf

Supervision regulation on financial intermediaries: http://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c288/Circ_288_2_AGGTO_integrale_segnalibri.pdf

CONSOB regulation on Markets, (non-official translation): http://www.consob.it/web/consob-and-its-activities/laws-and-regulations

CONSOB resolution on the application of the above CONSOB regulation on Markets: http://www.consob.it/documents/46180/46181/c9085378.pdf/401a8ecc-cd07-44f8-bc3e-c2b8dc51b802

Minister of the Treasury, Budget and Economic Planning Decree: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:1998-02-24;58!vig

BDI Supervisory Instructions: https://www.bancaditalia.it/compiti/sispaga-mercati/consultazioni-pubbliche/consultazione-120412/Istruzioni-Vigilanza-mercati.pdf

Working Group for operational crisis management coordination in the Italian financial marketplace (CODISE) guide: https://www.bancaditalia.it/compiti/sispaga-mercati/codise/CODISE_guide.pdf?language_id=1

IVASS Draft Regulation laying down provisions on corporate governance – public consultations under way. The regulation includes articles on data management, IT governance and cybersecurity: https://www.ivass.it/normativa/nazionale/secondaria-ivass/pubb-cons/2017/02-pc/Schema_Regolamento_2_2017_pc.pdf?language_id=3

CONSOB resolution concerning the application of ESMA Guidelines on Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities: http://www.consob.it/documents/46180/46181/c12027074.pdf/517df64e-db6d-44fb-bf92-f2e3c92ef123

CONSOB's Strategic Plan 2016-18: http://www.consob.it/documents/11973/912772/ps1618.pdf/7a462189-574c-4a20-9dc2-198c08a29956

Japan

National Strategy: Japan reported that the Basic Act on Cybersecurity, enacted in January 2015, stipulates the government's responsibilities and strategies for the assurance of cybersecurity for critical infrastructure operators, including those in the financial sector.

Regulations/Guidance: Japan reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector issued by the Financial Services Agency (JFSA). The scheme covers **FMIs, trading venues, banks, insurance companies, broker-dealers and asset managers**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including development of strategy for managing IT risk; role of board of directors and senior management; risk assessment; protection of confidential information, encryption and masking; backup systems; access control and monitoring of access logs; cybersecurity awareness training; vulnerability testing and penetration testing; investigation and remediation of cybersecurity incidents; public communication with respect to cyber incidents; contingency planning and related exercises; information sharing; updating operating system; security requirements for contractors; and incident reporting to regulator.

Supervisory Practices: Japan reported one scheme of supervisory practices, issued by JFSA, that covers **FMIs, trading venues, banks, insurance companies and broker-dealers**. JFSA has established a division for cybersecurity to strengthen cybersecurity in the financial sector, and is enhancing its functions through outside expertise and staff training and secondment. The supervisor reviews institutions' risk assessment frameworks; senior management role; specified technical requirements; contingency planning; training; and monitoring, testing and auditing. JFSA conducted industry-wide exercises for the first time in October 2016. In addition, the National Center of Incident Readiness and Strategy for Cybersecurity conducts an annual cross-sectoral exercise in which 13 critical infrastructures, including the financial sector, participate.

Future Plans: JFSA will continue to review its policies in response to changes in the cybersecurity environment. However, there are no specific measures contemplated at present.

Publicly Available Sources:

National Center of Incident Readiness and Strategy for Cybersecurity:
https://www.nisc.go.jp/eng/index.html

The Basic Act on Cybersecurity:
http://www.japaneselawtranslation.go.jp/law/detail/?id=2760&vm=04&re=02

JFSA publication on Policy Approaches to Strengthen Cyber Security in the Financial Sector:
http://www.fsa.go.jp/en/news/2015/20151105-1.html

JFSA publication on strategic directions and priorities from 2016-17:
http://www.fsa.go.jp/en/news/2016/20161130-1/01.pdf

Korea

National Strategy: None reported.

Regulations/Guidance: Korea reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector. This is the Electronic Financial Transactions Act, administered by the Financial Services Commission, covering **FMIs, trading venues, banks, insurance companies and asset managers**. It is targeted to cybersecurity and/or IT risk. The Act addresses the safety and reliability of electronic financial transactions. It covers a number of matters, including the role of the chief information security officer; vulnerability analysis and assessment; training; incident investigation, reporting and containment; and contingency planning.

Supervisory Practices: Korea reported one scheme of supervisory practices, issued by the Financial Supervisory Service (KFSS). It covers **FMIs, trading venues, banks, insurance companies and asset managers**. KFSS conducts examinations on a regular basis and upon outbreak of incidents. KFSS examines and oversees the cybersecurity framework and compliance therewith to ensure safety and soundness of digital finance business. KFSS also assesses adequacy of IT planning and IT system risk analysis. In addition, KFSS examines the development and implementation of an organisation's education and training programme for cybersecurity purposes, business continuity planning, and cybersecurity framework of third-party outsourcing contractors to financial institutions.

Future Plans: None reported.

Publicly Available Sources:

Electronic Financial Transactions Act:
http://www.law.go.kr/eng/engLsSc.do?menuId=1&query=electronic+financial&x=0&y=0%20-%20liBgcolor0

Enforcement Decree of the Electronic Financial Transactions Act:
http://www.law.go.kr/eng/engLsSc.do?menuId=1&query=electronic+financial&x=50&y=17%20-%20liBgcolor6

Mexico

National Strategy: None reported.

Regulations/Guidance: Mexico reported five schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the National Banking and Securities Commission (CNBV), covers **FMIs, trading venues, banks, broker-dealers, asset managers and popular and micro-financial entities**. It is targeted to cybersecurity and/or IT risk. While all the enumerated entities are subject to general operational risk requirements, more specific requirements apply only to banks. The scheme covers a number of matters, including development of IT security strategy, including cybersecurity issues; roles of board, general manager and chief information security officer; independence of chief information security officer from audit, systems, business and operational areas; risk assessment; inventory of critical processes and applications; protection of data integrity, confidentiality and availability; business continuity plans; physical protection; systems access control, including need-to-know and segregation of duties; monitoring, vulnerability assessment and penetration testing; incident response, including mitigation, recovery and notification of financial authorities and customers; system updates; controls to assess IT security of outsourced services and infrastructures before outsourcing and on a regular basis; and authorities' access to information.

The second scheme, issued by the Banco de México (Banxico), covers **banks**. It is targeted to cybersecurity and/or IT risk. The scheme is focused on the computational and telecommunication assets, software and applications used by the regulated entities to interconnect and operate with Banxico ("technological infrastructure"). The scheme covers a number of matters, including creation of a department responsible for cybersecurity and a compliance officer; policies and procedures to address maintaining robustness of technological infrastructure, implement a formal software development life cycle where cybersecurity is considered, ensure safe handling of information, control access and allow secure and efficient communication with Banxico; bi-annual evaluation of technological infrastructure; inventory of IT assets; physical and logical access controls; penetration testing by regulated entity or external auditor; auditing and tracking user access; incident detection, management, containment and investigation; notification of Banxico; business continuity; system updates; requirements for external IT providers; and Banxico access to information and supervisory and sanctioning authority.

The third scheme, from Banxico, covers **banks, insurance companies, broker-dealers, asset managers and pension funds**. It is targeted to cybersecurity and/or IT risk. It is currently in draft form and has been shared with interested parties for comment. The regulation of cybersecurity is identical to that in the second scheme. Like that scheme, this scheme is focused on the computational and telecommunications assets, software and applications used by the regulated entities to interconnect and operate with Banxico.

The fourth scheme, issued by Banxico, covers **card payments clearing houses and mobile payments clearing houses**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including senior management responsibilities, business continuity planning, bi-annual evaluation and certification of compliance with IT security standards, risk and vulnerability assessment, provision of operational plan to Banxico that includes architecture of technological infrastructure and connections to other participants, cryptographic tools, access

controls, incident notification to Banxico within five days and customer notification, requirements for third parties, and Banxico access to information and supervisory authority.

The fifth scheme, issued by the Insurance and Surety National Commission (CNSF), covers **insurance companies and insurance and reinsurance brokers**. It addresses operational risk generally. The Insurance and Surety Institutions Law establishes that institutions' solvency capital requirement shall cover, among other risks, operational risk, which will reflect the potential loss for deficiencies or failures in operational processes, IT, human resources or any other adverse external events related to the operation of the institution. Technological risk is considered as part of operational risk and includes the potential loss from damage, disruption, alteration or failures resulting from the use or dependence of systems, applications, networks and any other channel of distribution of information on the operations of the institution. Regulations require that an institution's risk management manual include a performance report that considers operational risk, including technological risk.

Supervisory Practices: Mexico reported three schemes of publicly released supervisory practices. The first, issued by the CNBV, covers **FMIs, trading venues, banks, broker-dealers, asset managers and popular and micro-financial entities**. The CNBV has a division that reviews IT security, including security related to cyber risks. It has implemented a risk-based supervisory methodology that assigns IT risk levels. These risk levels are taken into account for the annual assessment and supervisory visits programme, and specific investigation reviews can be carried out whenever relevant incidents require them. Reviews cover a number of matters, including cybersecurity strategy; management practices; procedures to protect confidentiality of information; framework for risk models; physical protections; inventory of business processes; implementation of systems security controls; annual audit report and vulnerability assessments; incident mitigation; results of continuity plan testing; and outsourced services, including on-site reviews of third parties.

The second scheme, issued by the Banxico, covers **FMIs and banks**. Cybersecurity reviews are carried out by a specialist team and designated examiners who come from a wide range of professional backgrounds. In addition, institutions must also contract the services of an independent external auditor, at least once every two years, to certify the level of compliance with the requirements to interconnect and operate with Banxico, including those relating to cybersecurity, and send the report to Banxico for review. The supervisory process includes on- and off-site examinations, including an annual programme of audits; "for cause" inspections, such as for cybersecurity incidents; and desk-based audits. Reviews cover a number of matters, including cybersecurity policy; risk management policies and procedures; physical protections; procedures regarding data integrity, traceability, backup and confidentiality; penetration testing; communication protocols; management of computer security vulnerabilities and incidents; procedures for incident containment, recovery and recordkeeping; and vendors and customers that may affect an institution's cybersecurity.

The third scheme, issued by CNSF, covers **insurance companies**. CNSF receives an institution's risk manual, which covers cybersecurity, and supervises compliance with the manual. CNSF may carry out inspections and evaluations related to IT.

Future Plans: Mexico reported that Banxico is in the process of updating the third scheme of regulation described above, to align with the second scheme. The draft regulation is currently

being discussed with financial institutions. These regulations will serve as a basis for the preparation of regulation for new services currently being developed by Banxico.

Publicly Available Sources:

http://www.banxico.org.mx/disposiciones/normativa/circular-4-2016/%7BE16FD70F-0959-C43C-79B0-7481292FBF95%7D.pdf

http://www.banxico.org.mx/disposiciones/normativa/circular-3-2016/%7BFABCE0E7-EF80-DEE5-C382-F9DF6DA44AB4%7D.pdf

http://www.banxico.org.mx/disposiciones/normativa/circular-4-2014/%7BA29B4521-A321-6047-0D7C-B074C58C03F9%7D.pdf

http://www.banxico.org.mx/sistemas-de-pago/informacion-general/politica-del-banco-de-mexico-respecto-de-las-infra/%7B577DD3EA-8C22-A309-0800-D5A71B2F8F11%7D.pdf

https://www.gob.mx/cnsf/acciones-y-programas/normativa-25263

General supervisory framework of Banxico: http://www.banxico.org.mx/disposiciones/marco-juridico/reglas-de-supervision-programas-de-autocorreccion-/%7B76528BB8-B7DA-BDCE-BFF3-4CC6F3544473%7D.pdf

https://www.gob.mx/cnsf/documentos/leyes-y-reglamentos-25281?state=draft

Netherlands

National Strategy: Netherlands reported that the government has issued a national cybersecurity strategy that is broadly applicable to all sectors, including the financial sector. With the National Cyber Security Strategy, the government has committed itself to five strategic objectives, namely that Netherlands is: (i) resilient to cyber attacks and protects its vital interests in the digital domain; (ii) tackles cybercrime; (iii) invests in secure IT products and services that protect privacy; (iv) builds coalitions for freedom, security and peace in the digital domain; and (v) has sufficient cybersecurity knowledge and skills and invests in IT innovation.

Regulations/Guidance: Netherlands reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector, namely, the CPMI-IOSCO Guidance for **financial market infrastructures**. Netherlands noted that the guidance is targeted to cybersecurity and/or IT risk. Netherlands noted that a framework for ethical security testing has been developed and implemented for the financial critical infrastructure in the country, called Threat Intelligence Based Ethical Redteaming (TIBER). TIBER is a public-private test of the cyber resilience of financial institutions.

Supervisory Practices: Netherlands reported one scheme of supervisory practices, issued by De Nederlandsche Bank (DNB), that covers **banks, insurance companies, asset managers, pension funds and payment service providers**. Supervision is supported through a self-assessment completed by financial institutions and, thereafter, challenged by a supervisory IT expert. After the challenge sessions, the outcome of the self-assessment is benchmarked with other similar financial institutions. The self-assessment is usually repeated every two years. The assessment covers information security policy (including cybersecurity), governance of cybersecurity, risk assessment, physical security, systems security, personnel training and awareness, monitoring and testing, incident assessment, communications, business continuity and third parties. In addition, DNB has issued a circular on cloud computing, stating that the supervisor must be informed and provided with the financial institution's risk analysis before an institution's use of a cloud service.

Future Plans: In late 2017, DNB will publish guidance on how to conduct a TIBER test. DNB, as part of the Eurosystem of central banks and coordinated by the ECB/Eurosystem, is currently in the process of updating the ECB regulation on systemically important payment systems to include requirements on cybersecurity. The Eurosystem is also in the process of developing cyber resilience oversight expectations and an EU-wide red team testing framework for FMIs that is closely aligned with the TIBER framework.

Publicly Available Sources:

National Cyber Security Strategy: https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

Circular on Cloud Computing: http://www.toezicht.dnb.nl/en/binaries/51-224828.pdf

Russia

National Strategy: Russia reported that the Doctrine of Information Security of the Russian Federation is a system of principles for maintaining information security in Russia. The doctrine addresses national defence against cyber threats and covers state and public security, economy, science, technology, education and strategic partnership. The major components of the doctrine are:

- List of main threats in the field of information security;
- Strategic aims and principles for ensuring information security; and
- Organisational framework for information security.

Regulations/Guidance: Russia reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector, issued by the Bank of Russia and others, that covers **FMIs, trading venues and banks**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including the establishment and maintenance of a cybersecurity strategy, requiring that this should be based on principles prescribed by the State Doctrine of Cybersecurity and standards of the Bank of Russia. The Standards of the Bank of Russia are aimed at information exchange coordination, analysis of the facts of the malicious use of IT and development of recommendations in the field of information security. The scheme covers the cybersecurity responsibilities and expertise of senior management; the role of the chief information security officer; risk assessment, including gathering threat intelligence and identifying vulnerabilities; inventory of IT assets and business processes; data confidentiality; physical protection of assets; training; monitoring of cyber threats and potential risk; incident investigation, assessment, containment, mitigation and recovery; cyber risk insurance; information sharing internal to an organisation; systems updating; interconnections with third parties; regulatory reporting; and supervisory actions in the investigation of incidents.

Supervisory Practices: Russia reported one scheme of supervisory practices, issued by the Bank of Russia, that covers **banks**. The scheme covers a number of matters, including cybersecurity expertise of supervisory team members; circumstances when a cybersecurity review should be conducted; and the content of the review, including cybersecurity strategy or framework, governance arrangements, risk assessment process, data security controls, training, monitoring and auditing, incident preparedness, past incidents, business continuity plans and the integration of cybersecurity risks in the overall operational risk landscape.

Future Plans: The Bank of Russia intends to develop the following:

- Comprehensive cybersecurity strategy for the financial sector; and
- Series of guidance to ensure cybersecurity in the financial sector, including outsourcing activities guidance, technology risk management guidance and business continuity management guidance.

Publicly Available Sources:

Standards of the Bank of Russia in the field of information security:
http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd

Doctrine of Information Security of the Russian Federation approved by Decree of the President of the Russian Federation No 646 of December 5 2016: http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1

Saudi Arabia

National Strategy: None reported.

Regulations/Guidance: Saudi Arabia reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector. This covers **FMIs, banks, insurance companies and financing companies**. It is targeted to cybersecurity and/or IT risk.

A cybersecurity strategy has been developed by the Saudi Arabia Monetary Authority (SAMA) in collaboration with the banking sector. The key components are to:

- Proactively protect Saudi banking sector critical information assets such as payment systems;
- Detect, respond to and recover from cybersecurity incidents and imminent threats through timely information sharing, collaboration and action;
- Foster a cybersecurity culture that promotes safe and appropriate use of information assets and services among all stakeholders in the Saudi banking sector;
- Understand and manage the interdependencies on national and international levels, and work with national authorities and international organisations to reduce the risks to the Saudi banking sector; and
- Maintain an adaptive cybersecurity framework taking into consideration regulatory requirements, new technologies and emerging cybersecurity threats.

SAMA has established a Cybersecurity Framework to enable financial institutions regulated by SAMA (the Member Organisations) to effectively identify and address risks related to cybersecurity. To maintain the protection of information assets and online services, the Member Organisations must adopt the Framework. The objectives of the Framework are as follows:

- To create a common approach for addressing cybersecurity within the Member Organisations;
- To achieve an appropriate maturity level of cybersecurity controls within the Member Organisations; and
- To ensure cybersecurity risks are properly managed throughout the Member Organisations.

The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the cybersecurity controls at Member Organisations, and to compare these with other Member Organisations. The Framework is based on the SAMA requirements and industry cybersecurity standards, such as NIST, Information Security Forum, ISO, CPMI-IOSCO and PCI DSS.

Overall, the Framework specifies that the board of directors has the ultimate responsibility for cybersecurity and endorsing cybersecurity governance, strategy and policy. The framework also addresses the role of senior management and the chief information security officer and the independence of the cybersecurity function from the IT function. Other matters addressed include cybersecurity policy, risk analysis, inventory of assets, access management, application security, change management, physical security, cyber security awareness and training for staff, incident management, and penetration tests for customer and internet facing services.

Supervisory Practices: None reported. However, the Framework states that "The implementation of the Framework at the Member Organization will be subject to a periodic self-assessment. The self-assessment will be performed by the Member Organization based on a questionnaire. The self-assessments will be reviewed and audited by SAMA to determine the level of compliance with the Framework and the cyber security maturity level of the Member Organization."

Future Plans: SAMA has developed a cybersecurity strategy comprised of five main objectives which are further split into 14 initiatives. One of the initiatives is the development of a cybersecurity framework, which has been developed and communicated to regulated entities for compliance. In addition, SAMA has already put a plan in place to implement the remaining objectives and initiatives in the coming years.

Publicly Available Sources:

SAMA Cyber Security Framework: http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

SAMA Business Continuity Management Framework: http://www.sama.gov.sa/en-US/Laws/BankingRules/BCM%20framework.pdf

Singapore

National Strategy: Singapore reported that its Cybersecurity Strategy is underpinned by the following four pillars:

- Strengthen the resilience of Singapore's critical information infrastructures, including in the financial sector;
- Mobilise businesses and the community to make cyberspace safer by countering cyber threats, combatting cybercrime and protecting personal data;
- Develop a vibrant cybersecurity ecosystem comprising a skilled workforce, technologically advanced companies and strong research collaborations; and
- Step up efforts to forge strong international partnerships.

Regulations/Guidance: Singapore reported one scheme of regulations and guidance, with two parts, that addresses cybersecurity for the financial sector, issued by the Monetary Authority of Singapore (MAS). The regulations and guidance cover **FMIs, trading venues, banks, insurance companies, broker-dealers, asset managers and credit bureaus, as well as stored value facilities,** and are targeted to cybersecurity and/or IT risk.

The first part, the **MAS Notice on Technology Risk Management**, contains a set of regulatory requirements that financial institutions have to meet. Under the notice, institutions are required to put in place a framework and process to identify critical systems, implement measures to maintain high availability and establish the requisite recovery time objectives, notify MAS of any relevant incident (including cybersecurity incidents) and submit a root case and impact analysis report on the incident, and implement IT controls to protect customer information from unauthorised access or disclosure.

The second part, the **MAS Technology Risk Management Guidelines**, contains statements of industry best practices that financial institutions are expected to adopt to manage their technology and cyber risks. The guidelines cover areas, such as:

- Establishment of technology risk management framework;
- Roles of board and senior management;
- Guidance on acquisition and development of IT systems, as well as IT outsourcing;
- IT security awareness for staff and contractors;
- Inventory of software and hardware components, and identification of criticality of information system assets;
- Implementing system, network and data security controls;
- Security monitoring;
- User access and privileged access controls;
- Managing changes, incidents and problems in IT systems;
- Data backup and system recovery management; and
- Conduct of vulnerability assessment, penetration testing and IT audit.

In addition, MAS has also issued circulars to provide further guidance to institutions on managing cyber risk. These include:

- **Circular on IT Security Risks Posed by Personal Mobile Device** (September 2014): This circular provides guidance to institutions on managing the cybersecurity risks pertaining to "Bring Your Own Device" (BYOD);
- **Circular on Early Detection of Cyber Intrusions** (August 2015): This circular provides further guidance to institutions on the implementation of measures for continuous monitoring to detect network and system intrusions; and
- **Circular on Technology Risk and Cyber Security Training for Board** (October 2015): This circular sets MAS' expectations on the roles and responsibilities of an institution's board of directors and senior management for oversight on technology risks and cybersecurity, including the need for the board to endorse the institution's IT strategy and risk tolerance, ensuring an appropriate accountability structure and organisational risk culture to support the effective implementation of the institution's cyber resilience programme, as well as putting in place a comprehensive technology risk and cybersecurity training programme for the board.

Supervisory Practices: Singapore reported one scheme of supervisory practices, with two parts, issued by MAS.

The first part is **MAS' Framework for Impact and Risk Assessment of Financial Institutions**, which describes MAS' methodology for risk-based supervision of financial institutions and applies to all **licensed banks and merchant banks, finance companies, insurance companies and brokers, capital market intermediaries, and financial advisers**. It covers the supervisory processes that underpin the MAS' supervisory framework, including how MAS assesses the impact of financial institutions and the use of the Comprehensive Risk Assessment Framework and Techniques (CRAFT) to assess their risks. CRAFT covers technology risk as one of the inherent risk areas, and considers risks pertaining to network vulnerabilities, control weaknesses, security shortcomings, malicious attacks and hacking incidents. Under CRAFT, MAS will examine the ability of an institution to manage and control the inherent risks appropriately, through assessing four broad areas of control factors, namely: (i) risk management systems and controls; (ii) operational management; (iii) internal audit; and (iv) compliance. Specific to cybersecurity, MAS' IT inspectors would assess an institution's controls and cybersecurity posture based on an established list of cyber-related components identified for each of the four control factor areas.

The second part is the **MAS Monograph on Supervision of Financial Market Infrastructures in Singapore**, which describes MAS' approach on the supervision of **FMIs**, based on the CPMI-IOSCO Principles and the application of the CRAFT framework, to ensure the safety and efficiency of FMIs in Singapore.

Future Plans: Singapore reported intentions to issue a Cybersecurity Bill. The Ministry of Communications and Information and the Cyber Security Agency of Singapore have invited the public to provide feedback on the draft Cybersecurity Bill (the period of public consultation was from 10 July to 24 August 2017). The draft bill includes clauses on critical information infrastructure protection, which covers critical information infrastructure in various sectors,

including the financial sector. The draft bill also includes regulations pertaining to managing and responding to cybersecurity incidents, and the sharing of cybersecurity information.

Publicly Available Sources:

Cybersecurity Strategy: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

MAS webpage on technology risk management (including links to the technology risk management notices, guidelines and circulars issued by MAS, and incident reporting instructions and template): http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx

MAS webpage on operational risk management (including links to the guidelines on outsourcing and business continuity management): http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/operational-risk.aspx

MAS Framework for Impact and Risk Assessment of Financial Institutions: http://www.mas.gov.sg/news-and-publications/monographs-and-information-papers/2007/mas-framework-for-impact-and-risk-assessment-of-financial-institutions.aspx

MAS Monograph on Supervision of Financial Market Infrastructures in Singapore: http://www.mas.gov.sg/news-and-publications/monographs-and-information-papers/2013/supervision-of-financial-market-infrastructures-in-singapore.aspx

MAS Annual Reports (section on the conduct of industry tests, including industry penetration-testing exercise, cybersecurity table-top exercise and industry-wide business continuity exercise):

- 2014: http://www.mas.gov.sg/annual_reports/annual20142015/chapter_2/industry_tests.html
- 2015: http://www.mas.gov.sg/annual_reports/annual20152016/chapter_2/industry_tests.html

Public Consultation on Proposed Cybersecurity Bill: https://www.csa.gov.sg/news/news-articles/public-consultation-on-proposed-cybersecurity-bill

South Africa

National Strategy: South Africa reported that the government has released the National Cybersecurity Policy Framework. This framework broadly aims to set policy goals, measures and institutional responsibilities to ensure the confidentiality, integrity and availability of South African data and IT systems. The framework also deals with critical information infrastructure protection as well as with the criminal justice response to cybercrime.

Regulations/Guidance: South Africa reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector, issued by the South African Reserve Bank (SARB), that covers **banks**. It is targeted to cybersecurity and/or IT risk. This guidance states that the CPMI-IOSCO Guidance is applicable to banks. The Bank Supervision Department of the SARB therefore expects banks to adhere to the guidance in principle and in their individual contexts. Furthermore, the guidance states that if the outcome of a review of a bank's policies, processes and practices is unsatisfactory, SARB may require the bank to strengthen its risk management policies, processes or procedures, or to hold additional capital. Work has also been done with some specific sectors (i.e. FMIs) by way of either assessments/surveys, bilateral letters and memorandums and informal sharing of information. None of these has been issued publicly.

The Prudential Standards to be made under the Insurance Bill (currently being deliberated on by Parliament) will address cyber risks. The draft Prudential Standards have not been formally released for consultation as this can only be done once the Insurance Bill has been enacted, but have been released for informal public consultation.

Supervisory Practices: None reported.

Future Plans: South Africa reported that the National Cybersecurity Policy Framework and the Cybercrimes and Cybersecurity Bill will pave the way for the State Security Agency (SSA) to issue regulations or supervisory practices for cybersecurity at the national level. This Bill is currently being considered by Parliament, and it specifically addresses the financial sector. The SSA has the authority to establish minimum security standards and a regulatory framework for critical infrastructures. It will also have the authority to test compliance with the standards and regulations, for example through security testing and audits, in addition to critical infrastructure having to evidence compliance with minimum standards themselves through audits. Furthermore, the National Cybersecurity Hub has been launched and is evolving. The Hub issues guidance for CERTs and has a reporting platform for incidents and guidance.

Publicly Available Sources:

National Cybersecurity Policy Framework:
http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Cyber Resilience Guidance Note: https://www.resbank.co.za/publications/detail-item-view/pages/publications.aspx?sarbweb=3b6aa07d-92ab-441f-b7bf-bb7dfb1bedb4&sarblist=21b5222e-7125-4e55-bb65-56fd3333371e&sarbitem=7803

Cybercrimes and Cybersecurity Bill:
http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Draft Prudential Standards under Insurance Bill:
https://www.fsb.co.za/Departments/insurance/Pages/assesManage1.aspx

Spain

National Strategy: Spain reported that it has published a National Cyber Security Strategy that establishes the guiding principles of cybersecurity, namely:

- National leadership and the coordination of efforts;
- Shared responsibility;
- Proportionality, rationality and efficiency; and
- International cooperation.

The general objective of the strategy is to ensure that Spain makes secure use of information and telecommunication systems, strengthening cyber attack prevention, defence, detection, analysis, investigation, recovery and response capabilities. To achieve this, the strategy lays down specific objectives and action lines and sets up an ad hoc organisational structure under the direction of the Prime Minister.

Regulations/Guidance: Spain reported one scheme of regulations/guidance that addresses cybersecurity for the financial sector, issued by the National Centre for Protection of Infrastructures and Cybersecurity, that covers **FMIs, banks, central securities depositories and stock exchanges**. It addresses operational risk generally. Critical operators are required to elaborate a specific protection plan for each critical infrastructure that they operate. The main element of the plan is a risk assessment covering both physical security and cybersecurity risks.

Supervisory Practices: Not publicly released.

Future Plans: Spain reported upcoming national regulations that will adopt EU regulations, specifically, the EU Directive on payment systems in the internal market and the EU Directive on security of network and information systems.

Publicly Available Sources:

National Cyber Security Strategy: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

Law and regulation related to the protection of critical infrastructure: http://www.cnpic.es/Legislacion_Aplicable/Generico/index.html

Switzerland

National Strategy: In 2012, Switzerland adopted the National strategy for the protection of Switzerland against cyber risks (NCS). The general objective of the NCS is to support the cooperation between public authorities, the private sector and operators of critical infrastructure in order to ensure early recognition of cyber threats, increase the resilience of critical infrastructures and minimise cyber risks.

The strategy covers this need for action with 16 concrete measures that are to be implemented by 2017 and can be consolidated into seven spheres of action, including:

- Research and development;
- Risk and vulnerability analysis;
- Analysis of the threat situation;
- Competence building;
- International relations and initiatives;
- Continuity and crisis management; and
- Legal basis.

Regulations/Guidance: Switzerland reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Swiss Financial Market Supervisory Authority (FINMA), covers **banks, broker-dealers, FMIs, trading venues and financial groups and conglomerates**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including risk management framework; roles, expertise and reporting lines of board of directors, senior management and cybersecurity oversight body; identification of cyber threats, especially with respect to critical and/or sensitive data and IT systems; inventory of network infrastructure and critical applications; confidentiality and integrity of technology infrastructure and/or sensitive data and IT systems; measures to increase employee awareness; penetration testing and vulnerability scanning; systematic monitoring and log of cyber attacks; investigation, response and recovery with respect to cyber attacks; information sharing among financial institutions; identification and assessment of cyber risks from acquisitions or outsourcing agreements; supervisory access to information; and enforcement tools.

The second scheme, issued by the Federal Assembly of the Swiss Confederation, the Swiss Federal Council and FINMA, covers **asset managers, fund management companies, representatives of foreign Collective Investment Schemes (CIS), distributors of CIS, custodian banks of Swiss CIS and other collective investment vehicles**. It addresses operational risk generally. Fund management companies and asset managers of collective investment vehicles generally are required to set down appropriate risk management and risk control principles as well as the organisation of risk management and risk control in internal guidelines. They are to include the risks that they are or could be exposed to as a result of their business activities and also the risks to which the collective investment schemes and other assets managed by them could be exposed. Cyber risks must be included in risk management.

The third scheme, also issued by FINMA, **covers insurance companies, financial groups and conglomerates**. It addresses operational risk generally. Insurance companies must identify,

address and monitor all material risks and install an effective internal control system covering all business activities. Operational risks and loss events related to operational risk need to be identified and analysed. This includes risks and loss events related to IT and cyber risk. The internal controls system must mitigate all material risks related to operations and compliance, which includes risks related to IT and cyber risk. As part of the regulatory audit, insurance companies' external auditors have to conduct an audit programme related to internal control systems. This programme covers several control objectives related to data and IT security.

Supervisory Practices: None reported.

Future Plans: None reported.

Publicly Available Sources:

National strategy for the protection of Switzerland against cyber risks (NCS): https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

FINMA Circular on operational risks, banks: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-01-07-2017.pdf?la=de%20

Collective Investment Schemes Act: https://www.admin.ch/opc/en/classified-compilation/20052154/index.html

Collective Investment Schemes Ordinance: https://www.admin.ch/opc/en/classified-compilation/20062920/index.html

FINMA Collective Investment Schemes Ordinance: https://www.admin.ch/opc/en/classified-compilation/20140344/index.html

Federal Insurance Supervisory Act: https://www.admin.ch/opc/de/classified-compilation/20022427/index.html

Federal Insurance Supervisory Ordinance: https://www.admin.ch/opc/de/classified-compilation/20051132/index.html

FINMA Circular on Corporate Governance, insurers: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-02.pdf?la=en%20

Turkey

National Strategy: Turkey reported that the National Cyber Security Strategy and Action Plan for 2013-14 was prepared and published in 2013. The strategy defines cybersecurity risks and principles for maintenance of cybersecurity and will be updated with national level coordination with respect to demands received from the public and private sector, and with consideration to developing technology, changing conditions and requirements. To this end, an updated version of the strategy was published for the period 2016-19.

Regulations/Guidance: Turkey reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, issued by the Banking Regulation and Supervision Agency of Turkey (BRSA), covers **banks**. It is targeted to cybersecurity and/or IT risk and is based on BCBS's *Risk Management Principles for Electronic Banking* and COBIT. The scheme covers a number of matters, including establishment and management of security control process, management surveillance, expertise of senior management, organisational responsibility for cybersecurity, risk management, data integrity, business continuity, backup systems, data confidentiality, authorisation and authentication, maintenance of audit trails, physical protection and access controls, training, monitoring, testing, auditing, incident investigation and recovery, information sharing, updating systems, third-party interconnections, process of independent IT auditing and regulatory reporting. There is also a similar regulation for payment service providers, issued by BRSA, that was not separately reported by Turkey.

The second scheme, issued by the Central Bank of the Republic of Turkey (CBRT), covers **FMIs, specifically payment systems and securities settlements systems**. It is targeted to cybersecurity and/or IT risk. The scheme covers a number of matters, including information security management framework that ensures confidentiality, integrity and availability of information assets; responsibility of board of directors and other personnel; risk identification, measurement, monitoring and management; inventory of information assets; physical security; identity authentication and access control; personnel security awareness; investigation of, and response to, security violations; vulnerability scans and penetration testing; audit trail; investigation and mitigation of cybersecurity incidents; stakeholder notification of cybersecurity incidents; incident recovery and business continuity; outsourcing; system updates; regulatory reporting; authorities' access to information; and supervisory actions.

The third scheme, issued by the Capital Markets Board of Turkey (CMBT), covers **FMIs, trading venues, broker-dealers, asset managers and pension funds**. It is targeted to cybersecurity and/or IT risk. It has currently been published as a draft. The scheme addresses a number of matters, including responsibilities of administrative board and top-level management; role and expertise of information systems security officer; asset inventory; measures to ensure confidentiality of transactions and transaction data; system backup; physical protection and access controls; awareness training; risk assessment, mitigation and monitoring; annual penetration testing by certified persons; audit trail; and information systems continuity plan.

Supervisory Practices: Turkey reported four schemes of supervisory practices. The first, issued by BRSA, covers **banks**. This scheme of supervisory practices relates to the first scheme of regulation/guidance above. There are three types of practices: periodic independent IT audits by external auditors, which are performed every two years; BRSA officers' IT audits; and

penetration tests conducted by independent non-executive internal or external IT staff, which are performed at least once a year. The competence of the external audit firms is proven by certification and oral interviews performed by BRSA.

The second scheme, also issued by BRSA, covers **payment service providers**. Management and audit of payment and e-money institutions is mainly based on BCBS's E-Banking Principles, ECB's Recommendations for the Security of Internet Payments and ECB's Recommendations for the Security of Mobile Payments. There are three types of practices as reported in the first scheme of supervisory practices above.

The third, issued by CBRT, addresses cybersecurity for **FMIs**. This scheme of supervisory practices relates to the second scheme of regulation/guidance above. System operators perform a self-assessment related to the system at least once a year and share this with CBRT. The assessment measures their adherence to policy, rules, principles and standards. In addition, CBRT may require that information systems be audited by independent auditing firms in addition to CBRT's oversight activities. Specialists with IT background support CBRT's oversight team during review and assessment activities.

The fourth scheme, issued by CMBT, covers **FMIs, trading venues, broker-dealers, asset managers and pension funds**. This scheme of supervisory practices relates to the third scheme of regulation/guidance above. Audit is applied in accordance with the information systems management principles set out in the scheme. The auditee is obliged to make information systems documentation suitable and ready and makes commitments to address findings of the audit report through an action plan. An institution's management is responsible for ensuring the action plan is executed and the commitments in the plan are met.

Future Plans: None reported.

Publicly Available Sources:

National Cyber Security Strategy and Action Plan for 2013-14:
http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm&main=http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm

National Cyber Security Strategy 2016-19:
http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf

Communique on Principles to be Considered in Information Systems Management in Banks:
http://www.bddk.org.tr/WebSitesi/english/Legislation/152348799ilkelerteblig_ing.pdf

Communique on principles to be considered in informatıon systems management and audit of payment and e-money institutions:
http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Odeme_Hizmetleri_Kanunu/13265odeme_hizmetleri_ve_elektronik_para_teblig.pdf

Regulation on Bank Information Systems and Banking Processes Audit to be Performed by External Audit Institutions:
http://www.bddk.org.tr/WebSitesi/english/Legislation/152358800bagimsizdenetimyonetm_ing.pdf

Communique on information systems used in payment and securities settlement systems:
http://www.tcmb.gov.tr/wps/wcm/connect/419d4a10-caa0-4898-af14-5d0a1f128be0/Communique+on+Information+Systems+Used+in+Payment+and+Securities+

Settlement+Systems.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE419d4a10-caa0-4898-af14-5d0a1f128be0

Communique on Information Systems Management Principles (draft regulation): http://www.spk.gov.tr/duyurugoster.aspx?aid=20131115&subid=0&ct=c&submenuheader=null

CBRT's oversight framework for Payment and Securities Settlement Systems: http://www.tcmb.gov.tr/wps/wcm/connect/3b819845-1ef8-4e16-a871-67b43a10a301/Odeme+ve+Menkul+Kiymet+Mutabakat+Sistemlerine+Iliskin+Gozetim+Cercevesi.pdf?MOD=AJPERES

United Kingdom

National Strategy: The United Kingdom (UK) reported that the National Cyber Security Strategy sets out the UK's vision that, by 2021, the UK is secure and resilient to cyber threats. To realise this vision, the UK will work to achieve the following objectives:

- Defend against evolving cyber threats and respond effectively to incidents;
- Detect, understand, investigate and disrupt hostile action;
- Develop cybersecurity industry analysis and expertise; and
- Pursue international action, both bilaterally and multilaterally.

Regulations/Guidance: The UK reported three schemes of regulations/guidance that address cybersecurity for the financial sector. The first, reported by the Bank of England (BoE), covers **FMIs** and is targeted to cybersecurity and/or IT risk. For all FMIs supervised by BoE, the regulatory context is framed by the CPMI-IOSCO Principles and the supplementary guidance.

The second scheme, issued by the Prudential Regulation Authority (PRA), which is part of BoE, covers **banks, building societies, credit unions and investment firms**. It addresses operational risk generally. The PRA Rulebook sets out fundamental rules and provisions so that financial sector institutions in the UK should take reasonable steps to ensure continuity and regularity in the performance of their regulated activities. Rules in the Rulebook set out high-level requirements of firms' governance and oversight, operational risk management, information security, business continuity, outsourcing, incident management and reporting and information sharing. This includes implementing cybersecurity controls, although these are not specifically detailed. The UK financial authorities have taken steps to put in place a programme of work to improve and test resilience to sophisticated cyber attacks, the CBEST testing framework. CBEST includes a threat intelligence phase during which the core threat intelligence deliverables are produced, threat scenarios are developed into a draft penetration test plan, threat intelligence capability is assessed and control is handed over to the penetration testers.

The third scheme, issued by the Financial Conduct Authority (FCA), covers **trading venues, banks, insurance companies, broker-dealers, asset managers, pension funds, financial advisers and consumer credit firms**. It addresses operational risk generally. The UK financial regulatory system operates a principles-based approach, and the FCA Handbook sets out that financial sector institutions in the UK should take reasonable steps to ensure continuity and regularity in the performance of their regulated activities. The Handbook requires regulated firms to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems. Firms are required to have effective processes and internal control mechanisms in respect to information processing systems. Firms must establish, implement and maintain an adequate business continuity policy. UK regulators recognise and have promoted information sharing as good practice amongst financial sector participants and interconnected companies outside of the financial sector, such as telecommunications and power providers.

Supervisory Practices: The UK reported three schemes of supervisory practices that address cybersecurity for the financial sector. The first, issued by BoE, covers **FMIs**. BoE's supervisory approach is designed to ensure that FMIs' rules, policies and practices are in line with the

CPMI-IOSCO Principles and compliant with all applicable regulatory requirements (for example, the European Market Infrastructure Regulation (EMIR) for central counterparties). The supervisory approach requires supervisors to make forward-looking judgments on the risks posed by FMIs to financial stability. BoE undertakes an assessment of each firm it supervises on an annual basis, which culminates in a number of risk mitigating actions it expects the firm to take. BoE also carries out a programme of structured reviews into FMIs' operations. These reviews are more in-depth than other supervisory activity and typically involve on-site inspections. Reviews of cyber resilience and outsourcing are among areas reviewed in this programme.

The second scheme, issued by the PRA, covers **banks, building societies, credit unions and investment firms**. The PRA does not differentiate supervisory practices based on the type of risk being addressed and general supervisory approaches apply to cyber risk as they do to all other risks. The PRA supervises firms to judge whether they meet its policies at the time of assessment and on a forward-looking basis, and will take action where needed to restore safety and soundness. Furthermore, BoE's CBEST framework provides for intelligence-led penetration and vulnerability testing of firms.

The third scheme, issued by the FCA, covers **trading venues, banks, insurance companies, broker-dealers, asset managers, pension funds, financial advisers and consumer credit firms**. The FCA's firm supervision is currently being supported through the use of a cyber questionnaire. The questionnaire is a self-assessment by firms as to their cybersecurity and resilience arrangements and capabilities. The FCA then conducts a desk-based review of the response. The FCA may then choose to undertake a more detailed examination of the firm's cyber resilience arrangements.

Future Plans: None reported.

Publicly Available Sources:

National Cyber Security Strategy 2016-21:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Standards for FMIs:
http://www.bankofengland.co.uk/financialstability/Pages/fmis/standards/requirements.aspx

PRA Rulebook: http://www.prarulebook.co.uk/rulebook/Home/Rulebook/27-04-2017

PRA Supervisory Statement on strengthening individual accountability in banking:
http://www.bankofengland.co.uk/pra/Documents/publications/ss/2015/ss2815.pdf

PRA Supervisory Statement on strengthening individual accountability in banking and insurance, amendments and optimisations:
http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3416split.pdf

PRA Supervisory Statement on internal governance:
http://www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss2115update.pdf

PRA Supervisory Statement on corporate governance: Board responsibilities:
http://www.bankofengland.co.uk/pra/Documents/publications/ss/2016/ss516.pdf

CBEST Implementation Guide:
http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestimplementationguide.pdf

CBEST, Understanding Cyber Threat Intelligence Operations:
http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestthreatintelligenceframework.pdf

CBEST Services Assessment Guide:
http://www.bankofengland.co.uk/financialstability/fsc/Documents/procuringpenetrationtestingservices.pdf

FCA Handbook: https://www.handbook.fca.org.uk/handbook

BoE's Approach to the Supervision of FMIs:
http://www.bankofengland.co.uk/financialstability/Documents/fmi/fmisupervision.pdf

BoE's Supervision of FMIs, Annual Report (2016):
http://www.bankofengland.co.uk/publications/Documents/fmi/annualreport2016.pdf

PRA's Approach to Banking Supervision:
http://www.bankofengland.co.uk/publications/Documents/praapproach/bankingappr1603.pdf

PRA's Approach to Insurance Supervision:
http://www.bankofengland.co.uk/publications/Documents/praapproach/insuranceappr1603.pdf

Recent FCA speeches articulating supervisory practices:
https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms; and https://www.fca.org.uk/news/speeches/expect-unexpected-cyber-security-2017-and-beyond

FCA guidance on outsourcing of cloud-based solutions:
https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it

United States

National Strategy: Established in 2003, the National Strategy to Secure Cyberspace is part of the overall effort to protect the nation and helped shape the strategic approach taken by the United States (US) Government. Over time, the strategic framework has evolved based on Executive Orders, Homeland Security Presidential Directives, Presidential Policy Directives, and other official guidance that outline strategic goals and objectives for the US, inclusive of government, industry, and civil society. This framework is also complemented by Congressional legislation.

Regulations/Guidance:[18] The US reported 10 schemes of regulations/guidance that address cybersecurity for the financial sector. The US regulates financial institutions on a functional basis under which separate agencies regulate different types of financial institutions, and in certain areas their regulations are required by legislative mandate to be consistent and comparable.

The first scheme, issued by the Federal Financial Institution Examination Council (FFIEC), covers **banks and credit unions**. The FFIEC focuses on exam uniformity, with outputs including IT risk. The scheme covers a number of matters, including the role of the board of directors, senior management and the chief information security officer; independence of the chief information security officer; obtaining, analysing, responding to, and maintaining repository of threat and vulnerability information; risk assessment; inventory of IT assets; maintenance of network and connectivity diagrams and data flow charts; secure storage of sensitive information, including physical controls, logical controls and environmental controls, as well as logging and monitoring controls; training to support security awareness; patch management, vulnerability scanning and penetration testing and secure software development; audits; incident response, including containment, coordination with law enforcement and third parties, restoring systems, preserving data and evidence and assisting customers; insurance policies as part of a mitigation strategy; sharing of attack data to benefit industry at large; due diligence in selecting and monitoring third-party service providers; authorities' access to information and supervisory and enforcement actions; and IT risk ratings.

The second scheme covers cybersecurity risk management at **FMIs that are subject to the supervision of the Federal Reserve Board (FRB)**. The scheme builds on the first scheme described above. In addition to the FFIEC materials, FRB uses the CPMI-IOSCO Guidance, Regulation HH and Part I of the Payment System Risk Policy to inform supervisory practices and assessments.

The third scheme, issued by the US Securities and Exchange Commission (SEC) staff, covers certain **asset managers and investment companies**. It is targeted to cybersecurity and/or IT risk. The guidance addresses a number of matters, including the creation of a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include: (i) controlling access to various systems and data via management of user credentials, authentication and authorisation methods, firewalls and/or perimeter defences, tiered access to sensitive information and network resources, network segregation and system hardening; (ii) data encryption; (iii) protecting against the loss or exfiltration of sensitive data by restricting

[18] The descriptions below do not include information regarding rules and guidance issued by self-regulatory organisations in the United States.

the use of removable storage media and deploying software that monitors technology systems for unauthorised intrusions, the loss or exfiltration of sensitive data or other unusual events; (iv) data backup and retrieval; and (v) the development of an incident response plan. The guidance also stated that routine testing of strategies could also enhance the effectiveness of any strategy. The guidance also addresses staff training, business continuity plans, and issues surrounding critical service providers, including backup processes and contingency plans.

The fourth scheme, issued by the SEC, covers **FMIs, trading venues, certain broker-dealers, clearing agencies, the Financial Industry Regulatory Authority, the Municipal Securities Rulemaking Board and plan processors**. It is targeted to cybersecurity and/or IT risk. The scheme is aimed at strengthening the technology infrastructure of the US securities markets and is broadly focused on issues relating to automated systems of key market participants, including their capacity, integrity, resilience, availability and security. The regulations apply to the systems of covered entities that directly support any one of six key securities market functions – trading, clearance and settlement, order routing, market data, market regulation and market surveillance. In addition, the regulations specify that "indirect systems" – systems that, if breached, are reasonably likely to pose a security threat to the enumerated systems – are subject to certain provisions of the regulation regulating to security standards and systems intrusions. The regulation requires covered entities to adopt policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain operational capability and promote fair and orderly markets. When a system intrusion occurs, covered entities are required to take appropriate corrective action, notify the SEC and disseminate information about the incident to members/participants. The regulation also requires: (i) regular reviews and testing of automated systems to identify vulnerabilities; (ii) periodic reviews of the effectiveness of policies and procedures and prompt action to remedy deficiencies; (iii) annual objective reviews for compliance with the regulations; (iv) business continuity and disaster recovery plans with recovery time objectives reasonably designed to achieve resumption for critical systems of two hours and for other systems of next business day; and (v) penetration testing at least every three years.

The fifth scheme, issued by the SEC, covers **FMIs**. It addresses operational risk generally. Each "covered" clearing agency shall establish, implement, maintain and enforce written policies and procedures reasonably designed to manage its operational risks by: (i) identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls; (ii) ensuring that systems have a high degree of security, resiliency, operational reliability and adequate, scalable capacity; and (iii) establishing and maintaining a business continuity plan that addresses events posing a significant risk of disrupting operations. Similar, but not identical, requirements apply to other registered clearing agencies. In addition, every security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities, shall establish, maintain and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability and security.

The sixth scheme, issued by the SEC, covers **broker-dealers, asset managers, investment companies, certain investment advisers, and transfer agents**. It is targeted to cybersecurity and/or IT risk. Under Regulation S-ID, each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft

Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Each financial institution's or creditor's Program must include reasonable policies and procedures to: (i) identify relevant red flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into its Program; (ii) detect red flags that have been incorporated into the Program of the financial institution or creditor; (iii) respond appropriately to any red flags detected in (ii) to prevent and mitigate identity theft; and (iv) ensure the Program (including the red flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft. A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. Regulation S-P provides that brokers, dealers, investment companies, and investment advisers registered with the SEC must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorised access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. In addition, Regulation S-P provides that brokers, dealers, investment companies, investment advisers, and transfer agents registered with the SEC that maintain or otherwise possesses consumer report information for a business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorised access to or use of the information in connection with its disposal.

The seventh scheme, issued by the SEC staff, covers **FMIs, trading venues, broker-dealers, asset managers, pension funds, self-regulatory organisations (including clearing agencies) and transfer agents**. It is targeted to cybersecurity and/or IT risk. The scheme consists of staff-issued guidance that focuses on practices and issues that regulated entities may want to consider in light of staff's observations from examinations of regulated entities. The guidance covers a number of matters, including the use of published standards, such as NIST, ISO and FFIEC; the roles of chief information security and chief technology officers; written information security policies; risk assessment; inventory of technology resources and network resources, connections and data flows; encryption; information security training for vendors and business partners; penetration testing and vulnerability scans; incident response, mitigation and recovery; business continuity plans; cyber insurance; information sharing regarding best practices; system maintenance and software patches; cybersecurity requirements in vendor and business partner contracts; and customer education.

The eighth scheme, issued by the US Commodity Futures Trading Commission (CFTC), covers **entities registered with the CFTC, including: (i) FMIs registered with the CFTC as derivatives clearing organisations; (ii) futures and swap markets registered with the CFTC as designated contract markets or swap execution facilities; and (iii) data repositories registered with the CFTC as swap data repositories.**. The programme focuses on cyber and information security and operational risk, including business continuity and disaster recovery preparedness and reflects statutory and regulatory requirements. The regulations require a programme of risk analysis and oversight to identify and minimise sources of operational risk through the development of appropriate controls and procedures. Automated

systems must be reliable, secure, and have adequate scalable capacity. These entities must have emergency procedures, backup facilities, and a plan for disaster recovery that allows for the timely recovery and resumption of operations, and must periodically test such procedures to ensure continuity of operations. The regulations require the programme of risk analysis and oversight to comply with industry best practices for each required element of the programme, which includes a cyber resilience framework. The scheme covers other matters, including, but not limited to, vulnerability management and vulnerability testing, external and internal penetration testing, identification of key controls and testing of all controls, security incident response planning and testing of the plan, completion of an enterprise technology risk assessment, physical security and environmental controls, and systems and data access controls.

The ninth scheme, issued by the CFTC, covers **swap dealers, futures commission merchants and other intermediaries.** It addresses operational risk generally. CFTC regulations require certain futures commission merchants and swap dealers to adopt risk management programmes that take into account technical and operational risks, which would generally include cybersecurity risks. For example, operational risk policies and procedures are required to take into account: (i) secure and reliable operating information systems with adequate, scalable capacity and independence from the business trading unit; (ii) safeguards to detect, identify and promptly correct deficiencies in operating and information systems; and (iii) reconciliation of all data and information in operating and information systems.

The tenth scheme, issued by the National Association of Insurance Commissioners (NAIC), covers **insurers** and other entities required to be licensed by state departments of insurance. It is targeted to cybersecurity and/or IT risk. The NAIC is in the process of adopting a draft model law that establishes risk-based standards for data security and standards for investigation of, and notification to the commissioner of, a cybersecurity event. The draft model law requires implementation of an information security programme, which addresses the following issues: designation of an employee responsible for the information security programme; risk assessment; protection against environmental hazards; restriction of access privileges; employee training; use of multi-factor authentication; encryption of non-public information; monitoring and testing; use of audit trails; development of an incident response plan; oversight by the board of directors; and oversight of third-party service provider arrangements. The model law requires prompt investigation of a cybersecurity event and notice to the commissioner within 72 hours. Furthermore, the model law provides the commissioner with authority to investigate and examine licensees for compliance with the law.

Supervisory Practices: The US reported five schemes of supervisory practices that address cybersecurity for the financial sector. The first scheme, issued by FFIEC, covers **banks and credit unions**. Supervisory frequency and scope are determined annually, with strategies risk-based and tailored for each institution. The scheme covers a number of matters, including review of board and management IT oversight; institution's IT risk; institution's risk identification process; effectiveness of IT controls; whether management develops satisfactory measures for defining and monitoring metrics, performance benchmarks, service level agreements, compliance with policies, effectiveness of controls and quality assurance and control; whether institution has necessary resources, training and testing; threat monitoring and incident response processes; business continuity planning; and third-party service providers.

The second scheme **covers FMIs that are subject to the FRB supervision**. Its content is identical to the first scheme, described above.

The third scheme, issued by SEC staff, **covers FMIs, trading venues, broker-dealers, asset managers, pension funds, self-regulatory organisations (including clearing agencies) and transfer agents**. Cybersecurity has been publicly identified by SEC staff as an examination priority in 2015, 2016 and 2017. The scheme describes information that SEC staff may review, and areas on which staff may focus, when conducting initiatives focused on cybersecurity. This may include documents relating to a firm's cybersecurity framework, governance structure and risk assessments. It also may include policies and procedures relating to inventory of physical devices and systems; enterprise data loss prevention, data security and backup systems; and penetration testing and vulnerability scans. Staff also may review information relating to training, business continuity of operations plan, incident response planning and actual cybersecurity incidents. Staff also may review documents relating to cybersecurity risk assessments of vendors; policies and procedures that address the supervision, monitoring and tracking of, and access controls for, vendors; and information regarding third-party access to the firm's network or data. Staff examinations may result in a deficiency letter requesting corrective action or a referral for possible enforcement action.

The fourth scheme, issued by the CFTC, covers entities registered with the CFTC, including: (i) **FMIs registered with the CFTC as derivatives clearing organisations;** (ii) futures and swap markets registered with the CFTC as **designated contract markets or swap execution facilities; and (iii) swap data repositories**. The CFTC conducts formal structured reviews of all these registered entities' cybersecurity programmes to assess ongoing compliance with statutory and regulatory mandates.

The CFTC conducts risk assessments to determine the frequency and scope of examinations of these registered entities. The risk assessment will include many different sources of information such as: notifications submitted by the entities concerning hardware or software malfunctions, trading halts, cybersecurity incidents or targeted threats that actually or potentially jeopardise automated system reliability, security, or capacity; information from other public and governmental resources; previous examination results; and emerging cybersecurity and information security risks.

Topics included in the examination plan may include: (i) systems risk management and governance relating to system safeguards or cybersecurity; (ii) information security; (iii) business continuity and disaster recovery planning and resources; (iv) capacity and performance planning; (v) systems operations; (vi) systems development and quality assurance; and (vii) physical security and environmental controls. The information security aspects of the examination may include: a review of the governance surrounding the process and/or the results of the process under review, including any review by committees of the entity's board of directors; procedures and results of those procedures as pertains to vulnerability scans, external or internal penetration tests, controls testing, incident response testing, and business continuity and disaster recovery testing; controls related to access to systems and data including least privilege, separation of duties, and account monitoring and control; user and device identification and authentication; system and information integrity, including malware defences and software integrity monitoring; and any other element of information security included in best practices.

CFTC staff will issue a confidential examination report, including findings and recommendations regarding any areas of concern; additionally, staff will require a remediation

plan to address such concerns by a specified date, and ultimately may refer an issue for possible enforcement action.

The fifth scheme, issued by NAIC, covers **insurance companies**. The supervisory practices include both broad and specific guidance providing direction for use in evaluating how a company identifies, assesses and mitigates cybersecurity exposures. Specific topics include cybersecurity; data confidentiality, integrity and backup; information sharing practices; system and network access controls; network monitoring; threat assessment and detection, including penetration testing and vulnerability scans; incident recovery; corporate governance; and IT controls and policies.

Future Plans: The US reported that members of the FFIEC routinely update the FFIEC IT Handbook, which includes new or clarifying expectations with regard to cybersecurity and operational risk guidance. Additionally, the NAIC routinely updates its Financial Condition Examiners Handbook. Furthermore, the Office of the Comptroller of the Currency, FRB and the Federal Deposit Insurance Corporation jointly released an Advanced Notice of Public Rulemaking regarding enhanced cyber risk management standards. The agencies are currently reviewing the public feedback in consideration of a formal rulemaking.

Publicly Available Sources:

Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Presidential Policy Directive 63 - Critical Infrastructure Protection: https://clinton.presidentiallibraries.us/items/show/12762

The National Infrastructure Protection Plan (NIPP): https://www.dhs.gov/national-infrastructure-protection-plan

NIPP including financial services: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf

Executive Order 13636 - Improving Critical Infrastructure Cybersecurity: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Presidential Policy Directive 41 - United States Cyber Incident Coordination: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

US International Strategy for Cyberspace: https://www.state.gov/documents/organization/255732.pdf

FFIEC IT Handbook: http://ithandbook.ffiec.gov/

FFIEC Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm

FFIEC Cybersecurity Awareness Page: https://www.ffiec.gov/cybersecurity.htm

Regulation HH (financial market utilities): https://www.gpo.gov/fdsys/pkg/FR-2014-11-05/pdf/2014-26090.pdf

Payment System Risk Policy (Part I) https://www.gpo.gov/fdsys/pkg/FR-2014-11-13/pdf/2014-26791.pdf

SEC's Covered Clearing Agency Standards: https://www.gpo.gov/fdsys/pkg/FR-2016-10-13/pdf/2016-23891.pdf

SEC's Clearing Agency Standards: http://www.gpo.gov/fdsys/pkg/CFR-2013-title17-vol3/pdf/CFR-2013-title17-vol3-sec240-17Ad-22.pdf; and https://www.gpo.gov/fdsys/pkg/FR-2012-11-02/pdf/2012-26407.pdf

Rule 38a-1 under the Investment Company Act of 1940: https://www.gpo.gov/fdsys/pkg/CFR-2016-title17-vol4/pdf/CFR-2016-title17-vol4-sec270-38a-1.pdf

Rule 206(4)-7 under the Investment Advisers Act of 1940: https://www.gpo.gov/fdsys/pkg/CFR-2016-title17-vol4/pdf/CFR-2016-title17-vol4-sec275-2064-7.pdf.

The 2003 adopting release for both rule 38a-1 and rule 206(4)-7 is available at: https://www.gpo.gov/fdsys/pkg/FR-2003-12-24/pdf/03-31544.pdf

SEC Cybersecurity Guidance, Investment Management Staff Guidance Update: https://www.sec.gov/investment/im-guidance-2015-02.pdf

Business Continuity Planning for Registered Investment Companies, Investment Management Staff Guidance Update (BCP Guidance): https://www.sec.gov/investment/im-guidance-2016-04.pdf

Regulation Systems Compliance and Integrity (Regulation SCI): https://www.gpo.gov/fdsys/pkg/FR-2014-12-05/pdf/2014-27767.pdf

SEC Staff Guidance on Current SCI Industry Standards: http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf

Rules and guidance contained in Regulation S-ID are published in the Code of Federal Regulations: https://www.gpo.gov/fdsys/pkg/CFR-2016-title17-vol4/pdf/CFR-2016-title17-vol4-part248-subpartC.pdf. Additional guidance is provided in the Federal Register: https://www.gpo.gov/fdsys/pkg/FR-2013-04-19/pdf/2013-08830.pdf

Rules and guidance contained in Regulation S-P are published in the Code of Federal Regulations, Title 17, Part 248, Subpart A, and Appendix A to Subpart A: https://www.gpo.gov/fdsys/pkg/CFR-2016-title17-vol4/pdf/CFR-2016-title17-vol4-part248-subpartA.pdf. Additional guidance is provided in the Federal Register: https://www.gpo.gov/fdsys/pkg/FR-2000-06-29/pdf/00-16269.pdf; and https://www.gpo.gov/fdsys/pkg/FR-2004-12-08/pdf/04-26878.pdf.

OCIE Risk Alert, OCIE Cybersecurity Examination Sweep Summary: https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (only involving examinations of broker-dealers and investment advisers).

OCIE Risk Alert, OCIE's Cybersecurity, Ransomware Alert: https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf

OCIE Risk Alert, Observations from Cybersecurity Examinations, August 7, 2017: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

Regulation SDR (17 C.F.R. § 240.13n-6): https://www.gpo.gov/fdsys/pkg/CFR-2016-title17-vol4/pdf/CFR-2016-title17-vol4-sec240-13n-6.pdf; and https://www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-03127.pdf

System Safeguards Testing Requirements for Derivatives Clearing Organizations: https://www.ecfr.gov/cgi-bin/text-idx?SID=43e5200caf6d23c05c5b1a5464421075&mc=true&node=se17.1.39_118&rgn=div8; and https://www.ecfr.gov/cgi-bin/text-idx?SID=4a29dcdede5c031eee54c3d9121b983a&mc=true&node=se17.1.39_134&rgn=div8

System Safeguards Testing Requirements for Designated Contract Markets (futures markets): https://www.ecfr.gov/cgi-bin/text-idx?SID=b2ac4aa8ed882350142a5ec4453209e2&mc=true&node=sp17.1.38.u&rgn=div6

System Safeguards Testing Requirements for Swap Execution Facilities: https://www.ecfr.gov/cgi-bin/text-idx?SID=b2ac4aa8ed882350142a5ec4453209e2&mc=true&node=sp17.1.37.o&rgn=div6

System Safeguards Testing Requirements for Swap Data Repositories: https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=2d432480912088546a7ee9ad16fb612b&ty=HTML&h=L&mc=true&r=SECTION&n=se17.2.49_124

Risk Management Program for futures commission merchants: https://www.ecfr.gov/cgi-bin/textidx?SID=593f2af71175611e2336d8860da5c3bb&mc=true&node=se17.1.1_111&rgn=div8

Risk Management Program for swap dealers and major swap participants: https://www.ecfr.gov/cgibin/textidx?SID=593f2af71175611e2336d8860da5c3bb&mc=true&tpl=/ecfrbrowse/Title17/17cfr23_main_02.tpl

NAIC Draft Model Law: http://www.naic.org/documents/cmte_ex_cswg_170509_model_law_v4_clean.pdf

New York State Department of Financial Services regulation on Cybersecurity Requirements Required for Financial Services Companies: http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

FFIEC IT Handbook, IT Booklets: http://ithandbook.ffiec.gov/it-booklets.aspx

OCIE Examination Priorities: https://www.sec.gov/page/ocie-section-landing

OCIE Risk Alert, Cybersecurity Preparedness Initiative: https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

OCIE Risk Alert, Cybersecurity Examination Initiative: https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

Enhanced Cyber Risk Management Standards: https://www.federalregister.gov/documents/2017/01/24/2017-01539/enhanced-cyber-risk-management-standards

CFTC System Safeguards Testing Requirements for Derivatives Clearing Organizations: http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816b.pdf

CFTC System Safeguards Testing Requirements:
http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816c.pdf