Cyber Task Force

Final Report

The Board
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR09/2019	**JUNE 2019**

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org

Contents

Executive Summary

This report, prepared by IOSCO's Cyber Task Force (CTF), compiles information from IOSCO member jurisdictions regarding their existing frameworks for Cyber[1] regulation. It is intended to serve as a resource for financial market regulators and firms to raise awareness of existing international Cyber guidance, and to encourage the adoption of good practices among the IOSCO community.

The report examines how IOSCO member jurisdictions are using three prominent and internationally recognised Cyber frameworks (as explained further below, the "Core Standards"). To avoid overlap or duplication, the report focuses on these existing Cyber frameworks instead of proposing a new framework or prescriptive guidance. The report also indicates how such existing Cyber frameworks could help address any gaps identified in members' current regimes. Lastly, the report provides a set of core questions that firms and regulators may use to promote awareness of Cyber good practices or enhance their existing practices.

The report findings and corresponding analysis are based on a survey of IOSCO member jurisdictions. Some of the key findings of this report are:

- **Rating Cyber Risk:** Many IOSCO member jurisdictions consider Cyber to be at least one of the most important risks faced by regulated firms in their jurisdiction. However, a significant percentage of survey respondents either consider Cyber to be a risk like any other or are unsure of its relative standing compared to other risks.

- **Consistency with the Core Standards:** A majority of survey respondents indicated that their domestic regulations, guidance, and/or supervisory practices were either "generally consistent" or "entirely consistent" with one of the Core Standards. While the principles underlying the Core, Standards have gained considerable influence in IOSCO jurisdictions, no one Core Standard predominates.

- **Express Reference to the Core Standards:** Almost half of the survey respondents indicated that they are flexible and not prescriptive as to which Cyber standards (Core Standards or otherwise) firms may utilise to comply with applicable domestic regulations.

- **Consistency across National Cyber Security Frameworks:** Despite jurisdictional differences, the Cyber frameworks of most survey respondents share certain common elements.

---

[1] This report uses terms and definitions as defined in the Cyber Lexicon of the Financial Stability Board (12 November 2018) (the Cyber Lexicon) available at: http://www.fsb.org/wp-content/uploads/P121118-1.pdf. In creating the Cyber Lexicon, the FSB relied on existing sources to develop the terminology drawing on the extensive work that has previously been done or is underway by other groups in developing lexicons and glossaries related to cyber security and cyber resilience, such as the terminology defined in the Core Standards (defined below) as well as other cyber frameworks and guidance. Cyber Lexicon terms are capitalised in the CTF report.

Cyber is defined to relate to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. *See* the Cyber Lexicon.

- **Updating and Improving Cyber Regimes:** Over one third of survey respondents reported that they have publicly declared plans to issue, within the next year, new regulations, guidance or supervisory practices that address Cyber Security[2] for all or part of their financial sector.

[2] Cyber Security is defined as the preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. Cyber Lexicon

1. Introduction

1.1 The Cyber Risk Landscape

Cyber Risk[3] is widely recognised as one the top threats to financial markets today. Examples of Cyber Incidents[4] abound from financial data breaches at large multinational public companies to high profile incidents on central banks and government systems. The potential economic costs of such events can be immense and the damage to public trust and confidence is significant as Cyber Incidents could potentially undermine the integrity of global financial markets.

As this risk grows, so too have domestic and international efforts to address it. Over the past five years, national authorities, standard setting bodies, and private sector organisations have launched initiatives to address Cyber Risk and increase the Cyber Resilience[5] of the financial markets and industry.[6]

IOSCO is actively engaged in these efforts. In 2013, IOSCO published a joint working paper with the World Federation of Exchanges, entitled *Cyber-Crime Securities Markets and Systemic Risk.*[7] In 2014, IOSCO and the Committee on Payments and Market Infrastructures (CPMI) set up a joint working group on Cyber resilience in financial market infrastructures (WGCR) which continues to monitor implementation issues associated with Cyber Resilience. This work led to publication in 2016 of the CPMI-IOSCO *Guidance on Cyber Resilience for Financial Market Infrastructures*[8] (CPMI-IOSCO Guidance), which provides an important framework for the financial services industry to address and implement Cyber resilience for financial market infrastructures. In 2016 IOSCO also published a report on

---

3 Cyber Risk is defined as the combination of the probability of Cyber Incidents occurring and their impact.

4 Cyber Incidents are defined as a Cyber event that either (i) jeopardises the Cyber Security of an Information System or the information the system processes, stores, or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. *See* the Cyber Lexicon.

5 Cyber Resilience is the ability of an organisation to continue to carry out its mission by anticipating and adapting to Cyber Threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from Cyber Incidents. *See* the Cyber Lexicon.

6 Prominent contributions include work by the FSB on the Cyber Lexicon, referenced above, and by the Financial Services Sector Coordinating Council (FSSC) on the Financial Services Sector Cybersecurity Profile (Profile). The Profile provides a framework for cyber risk management assessment by financial firms and to demonstrate regulatory compliance. Available at: https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile. Other notable work by the FSB includes the *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices* (October 13, 2017) (2017 FSB Stocktake), in which IOSCO submitted survey responses. Available at: https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/

7 http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

8 http://www.bis.org/cpmi/publ/d146.pdf

regulatory approaches to Cyber Security[9] entitled, *Cyber Security in Securities Markets – An International Perspective*.[10] IOSCO's Affiliate Member Consultative Committee (AMCC) is also very active in this area, assisting with IOSCO publications and separately coordinating with industry on Cyber Resilience issues.

1.2 Formation and Objective of the Cyber Task Force

While there has been significant progress in increasing global awareness and action to address Cyber Risk, Cyber Incidents continue to occur with greater frequency and greater sophistication. Preparation is important for financial entities and regulators alike.

To address these issues, IOSCO has undertaken work to raise awareness of existing international Cyber guidance and encourage the adoption of good practices among the IOSCO regulatory community. To carry out this work, the IOSCO Board established a Cyber Task Force (CTF) in October 2017.

In setting up the CTF, IOSCO determined that it would be more effective to build on existing expert work on Cyber guidance than to attempt to create a new framework or a new set of standards specifically for IOSCO members. Therefore, the CTF took as its starting point the wide body of existing industry-driven work created in consultation with public sector authorities. Among these, it identified three exemplars of well-received and widely used Cyber frameworks (referred to as the "Core Standards").[11]

The CTF's primary objective is to determine how IOSCO member jurisdictions have utilised the Core Standards and, where necessary, identify how such standards could be better applied to address any identified gaps among IOSCO member jurisdictions. By assessing the use of the Core Standards, the CTF also aims to identify and promote Cyber[12] sound practices for the IOSCO community.

When the CTF began this work, there was no single source that described how IOSCO member jurisdictions were applying the Core Standards or that had identified where differences exist in their application. By highlighting the various applications of the Core Standards by IOSCO members, the CTF anticipates that members can review their own

---

9 Cyber Security is defined as preservation of Confidentiality, Integrity and Availability of information and/or Information Systems through the Cyber medium. In addition, other properties, such as Authenticity, Accountability, Non-Repudiation and Reliability can also be involved. *See* the Cyber Lexicon.

10 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.

11 While Cyber is a common risk, a myriad of diverse regimes could undermine cyber initiatives, confuse markets, and create inconsistencies where various approaches are conflicting or inconsistent, thereby making compliance with the different regimes difficult or impossible. In this regard, the Core Standards could be used as a reference to reduce the likelihood of inconsistent cyber standards being followed or applied across jurisdictions internationally.

12 Cyber is defined to relate to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. *See* the Cyber lexicon.

Cyber standards in relation to the practices provided by the Core Standards and, where relevant, use the Core Standards as a model to further enhance their Cyber regimes.

The CTF's report is organised into six parts: an introduction, review of the Core Standards, discussion of the survey issued by the CTF, analysis of IOSCO members' national Cyber Security frameworks, analysis of how the Core Standards are being used by IOSCO members, and, lastly, the conclusion and next steps.

1.3 Review of the Core Standards

The Core Standards are three prominent and widely respected Cyber frameworks that are being used in the financial sector worldwide.[13] They are often used not in isolation but in combination with other Cyber guidance, such as the COBIT 5 for Information Security.[14] The Core Standards are also generally consistent with each other and other notable Cyber principles,[15] such as the work of the G-7 Cyber Experts Group.[16]

The Core Standards are described in more detail below.

1.3.1 National Institute of Standards and Technology (NIST) Cybersecurity Framework

First published in 2014 and aimed at the operators of critical infrastructures, the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) is a voluntary, risk-based framework of industry standards and best practices designed to help organisations manage Cyber Security risks.[17] The framework enables organisations, regardless of size, degree of Cyber Security risk or Cyber Security sophistication, to apply the principles and best practices of risk management to improving the

---

13 The FSB's 2017 Stocktake found that the Core Standards were the most widely useful existing guidance on Cyber Security for FSB jurisdictions, and that such wide acceptance of these standards helps to promote a degree of international convergence with respect to Cyber Security regulation in the financial sector.

14 The Control Objectives for Information and Related Technology (COBIT) framework was created by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) to help organisations create, monitor, and maintain informational technology generally.

15 *See generally* Annex, *infra*.

16 The G-7 group was established in 2015 with the mandate of surveying member jurisdictions' approaches to financial sector cybersecurity and issuing recommendations to the G-7 finance ministers and central bank governors. In October of 2016, the G-7 published *Fundamental Elements of Cybersecurity for the Financial Sector.* Available at: https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf

17 U.S. National Institute of Standards and Technology (NIST) at, https://www.nist.gov/cyberframework/critical-infrastructure-resources,

security and resilience of critical infrastructure. The NIST Cybersecurity Framework is composed of three parts:

- **The Framework Core** is a set of Cyber Security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core consists of five Functions—Identify, Protect, Detect, Respond, Recover. Together these five functions and associated guidance aim to provide a high-level, strategic view of the lifecycle of an organisation's management of Cyber Security risk. The Framework Core then identifies key Categories and Subcategories for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- **The Framework Implementation Tiers** are designed to define how an organisation views Cyber Security risks and its processes to manage these risks. The Tiers describe the degree to which an organisation's Cyber Security risk management practices exhibit certain characteristics (e.g., risk and threat aware, repeatable, and adaptive) in order to define its place on a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers are intended to reflect a progression from informal, reactive responses to approaches that are agile and risk informed.

- **The Framework Profile** characterises the alignment of standards, guidelines, and practices to the Framework Core in a specific implementation scenario. Profiles can therefore be used to identify ways to improve Cyber Security by comparing a "Current" Profile with a "Target" Profile". The Current Profile can support prioritisation and measure progress towards the Target Profile. The Profiles can be used to conduct self-assessments and facilitate communication within an organisation or between organisations.

Following consultations, NIST released Version 1.1 of the NIST Cybersecurity Framework.[18] Version 1.1 is fully compatible with Version 1.0 and includes updates on:

- authentication and identity;
- self-assessing Cyber Security risk;
- managing Cyber Security within the supply chain; and
- vulnerability disclosure.

NIST plans to release an updated Roadmap for Improving Critical Infrastructure Cybersecurity, which describes key areas of development, alignment and collaboration.

[18] NIST in 2018 updated to Version 1.1 of its popular framework, commonly known at the NIST Cybersecurity Framework, including updates to authentication and identity; self-assessing cybersecurity risk; managing cybersecurity with supply chain; and vulnerability disclosure. Available at: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

1.3.2 CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance)

Published in 2016, the CPMI-IOSCO Guidance was developed for financial market infrastructure (FMIs) to enhance their Cyber resilience. Given the dynamic nature of Cyber threats the guidance is principles-based and is generally consistent with the other Cyber frameworks, including the other two Core Standards. While it is directed to FMIs, the guidance leaves open to the relevant authorities to apply it to other infrastructure.[19] The CPMI-IOSCO Guidance outlines five primary risk management categories and three overarching components that should be addressed across an FMI's Cyber resilience framework. The Five Primary Risk Management Categories are:

- **Governance:** Arrangements should be put in place to establish, implement and review the FMI's approach to managing Cyber risks. Effective governance should start with a clear and comprehensive Cyber resilience framework. Accordingly, guidance is provided on the basic elements of an FMI's Cyber resilience framework and how an FMI's governance arrangements should support that framework.

- **Identification:** It is crucial that FMIs identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. The CPMI-IOSCO Guidance outlines how an FMI should identify and classify business processes, information assets, system access and external dependencies.

- **Protection**: Cyber resilience depends on effective security controls and systems and process design that protect the confidentiality, integrity and availability of an FMI's assets and services. The CPMI-IOSCO Guidance urges FMIs to implement appropriate and effective controls and design systems and processes in line with leading Cyber resilience and information security practices to prevent, limit and contain the impact of a potential Cyber incident.

- **Detection**: An FMI's ability to recognise signs of a potential Cyber incident, or detect that an actual breach has taken place, is essential to strong Cyber resilience. Given the stealthy and sophisticated nature of Cyber incidents and the multiple entry points through which a compromise could take place, advanced capabilities to extensively monitor for anomalous activities are needed. The chapter on detection in the CPMI-IOSCO Guidance outlines monitoring and process tools to be used by an FMI for the detection of Cyber incidents.

---

[19] As defined in the CPMI-IOSCO Guidance, and consistent with the CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMI), FMIs are systemically important payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories. Relevant authorities, however, may decide to apply the guidance to other types of infrastructure, such as non-systemically important entities, not specifically covered by the CPMI-IOSCO Guidance. The guidance supplements the international standards in the 2012 CPMI-IOSCO PFMI.

- **Response and recovery:** Financial stability may depend on an FMI's ability to settle obligations when due. Therefore, the CPMI-IOSCO Guidance states that an FMI's arrangements should be designed to enable it to resume critical operations rapidly, safely, and with accurate data to mitigate the potentially systemic risks of failure to meet such obligations.

The Three Overarching Components are:

- **Testing:** All elements of a Cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter.

- **Situational awareness:** Refers to an FMI's understanding of the Cyber threat environment within which it operates, and the implications of being in that environment for its business and the adequacy of its Cyber risk mitigation measures.

- **Learning and evolving:** An FMI's Cyber resilience framework needs to achieve continuous Cyber resilience given the ever-changing threat environment. An FMI should aim to instil a culture of Cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

The CPMI-IOSCO Guidance does not establish additional standards for FMIs beyond those set out in the CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMI).[20] Instead, the guidance supplements the PFMI, in particular, 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).

1.3.3 International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

ISO and the IEC developed and published the 27000 family of standards on information security management systems to help organisations keep secure information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. The ISO series comprises a set of standards which have been developed since the 1990s and is widely used by multinational corporations. The most recent version was published in 2013.[21] Under the ISO system, a company that has implemented a standard such as ISO 27001 can be certified (or registered) if it successfully completes an audit carried out by a certification body that has been accredited by ISO.

---

20 Available at: https://www.bis.org/cpmi/publ/d101a.pdf

21 For example, one part of the ISO series was updated in 2018. *See*: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

The most relevant ISO Cyber standards include ISO 27001, which lays out the framework to create a comprehensive IT security program, and ISO 27002, which then contains the "best practices" to construct it.

- **ISO/IEC 27001** defines a suite of activities for managing information risks (Information Security Management System or "ISMS"). The ISMS is an overarching management framework through which the organisation identifies analyses and addresses information risks. The standard covers all types of organisations of all sizes in all industries or markets, public and private.

  Given the range of entities that can use it, ISO/IEC 27001 does not take a one-size-fits-all approach or mandate particular controls. The information security controls set out in Annex A to ISO/IEC 27001 act as a menu from which organisations can choose the most applicable controls given the risks they face. Consequently, it prompts organisations to undertake a comprehensive assessment of their information risks, which is one of the most important steps in information security and a vital part of the ISMS. The standard also gives organisations the option to avoid or transfer information risks, rather than mitigate them through controls.

- **ISO/IEC 27002** sets out a code of good practice for information security. It is an advisory document and not a formal specification like ISO/IEC 27001. It recommends good practices addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organisations must assess their information risks, clarify their control objectives, and apply suitable controls using the standard for guidance.

While the Core Standards share many of the same objectives, each offers a different approach in both scope and detail.

Figure 1
Comparison of the Key Characteristics of the Core Standards

	NIST	CPMI-IOSCO	ISO
Developed by	U.S. non-regulatory agency	International standard setting bodies	Independent, non-governmental, worldwide federation of national standards bodies
Designed for	Originally aimed at operators of critical infrastructure	Financial market infrastructure	All sectors, public and private
Cost	Free	Free	Charges apply to most standards
Approach	Framework	Principles/Guidance	Framework, Menu of Controls, and Guidance
Updates	Updated April 2018	Not currently planned	Periodic updates
Single or Multiple Standards	Framework referencing variety of standards	Single set of guidance supplementing PFMI	Framework and Set of standards

2. CTF Survey and Gap Analysis

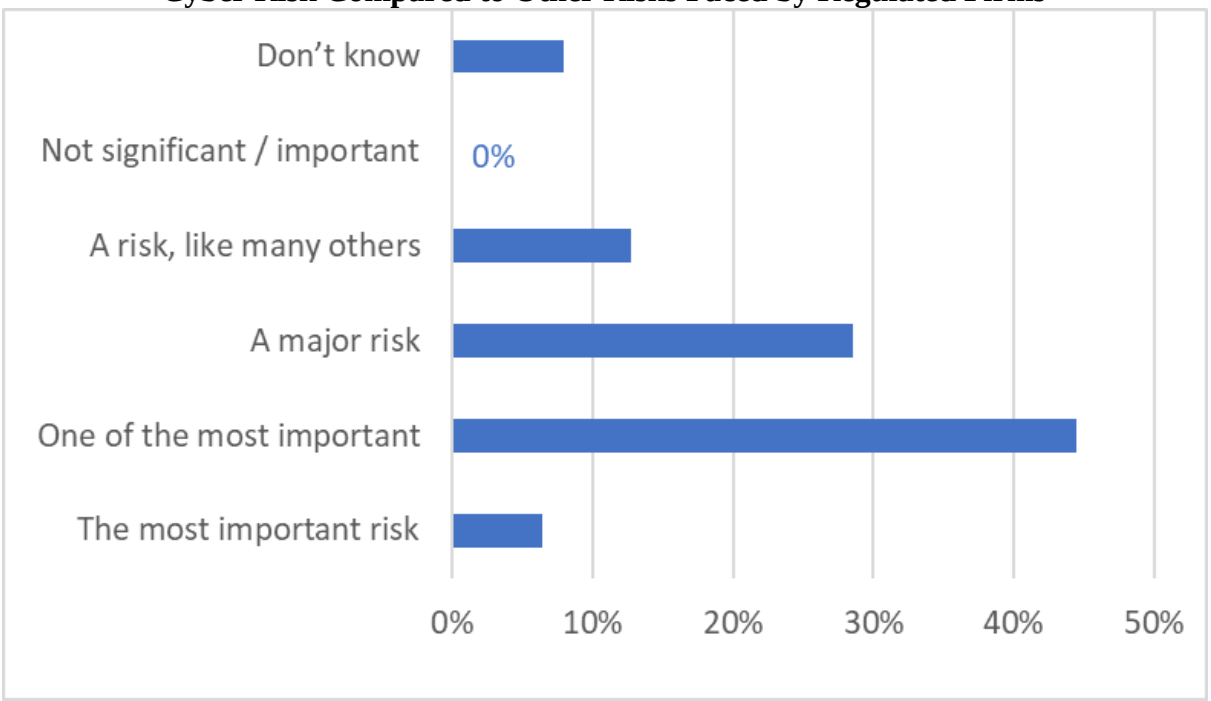
The CTF conducted a survey of IOSCO members to obtain information on how the Core Standards are being applied to financial firms in IOSCO jurisdictions and to identify any potential gaps in the application of the Core Standards.

The survey is divided into three broad categories of questions: (i) general background information; (ii) regulatory and supervisory approaches with respect to Cyber; and (iii) consistency with, or reliance upon, the Core Standards. The CTF received 59 survey responses from a total of 128 member jurisdictions – or just slightly under a 50% response rate. Set forth below is a summary of the gap analysis from the survey responses. Key findings are in bold text.

2.1 Rating Cyber Risk

With respect to estimating the importance of Cyber Risk to financial firms operating in IOSCO jurisdictions, **most survey respondents (81%) consider Cyber Risk to be at least one of the most important risks, the most important risk, or a major risk faced by regulated firms in their jurisdiction. Meanwhile, a minority of respondents (19%) either consider Cyber Risk to be a risk like any other or are unsure of its relative standing compared to other risks.** This data is reflected in Figure 2, below.

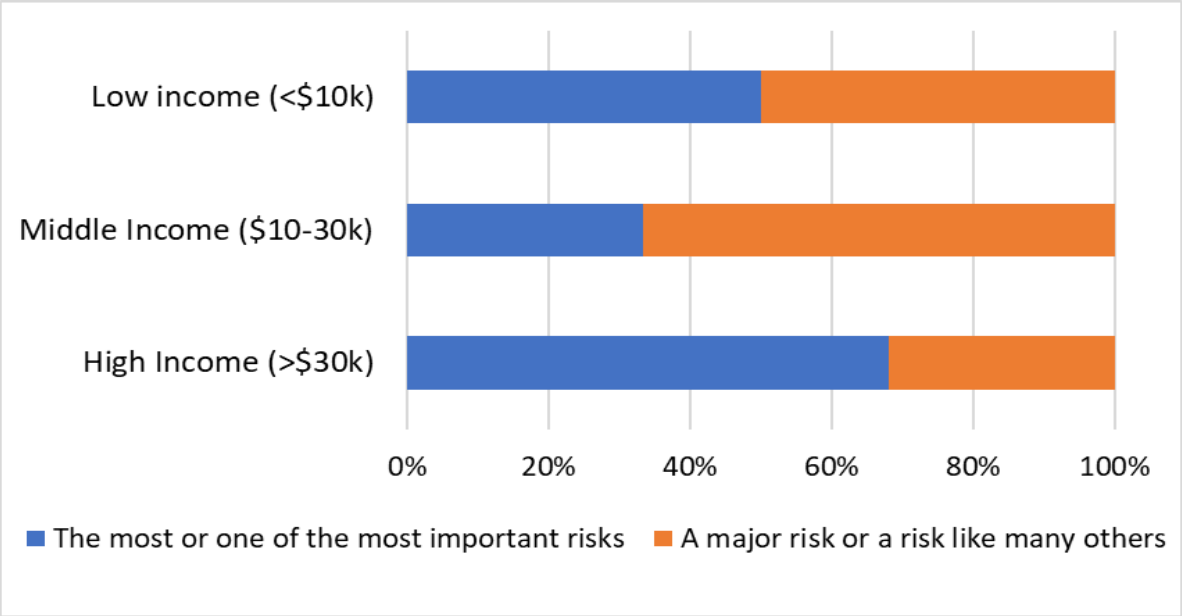
Figure 2
Cyber Risk Compared to Other Risks Faced by Regulated Firms



The survey responses also illustrate that **that Cyber Risk is perceived as a greater risk in jurisdictions with higher GDP per capita (GDP per capita over $30,000).** However, the relationship is U-shaped, with jurisdictions with mid-range GDP per capita (GDP per capita

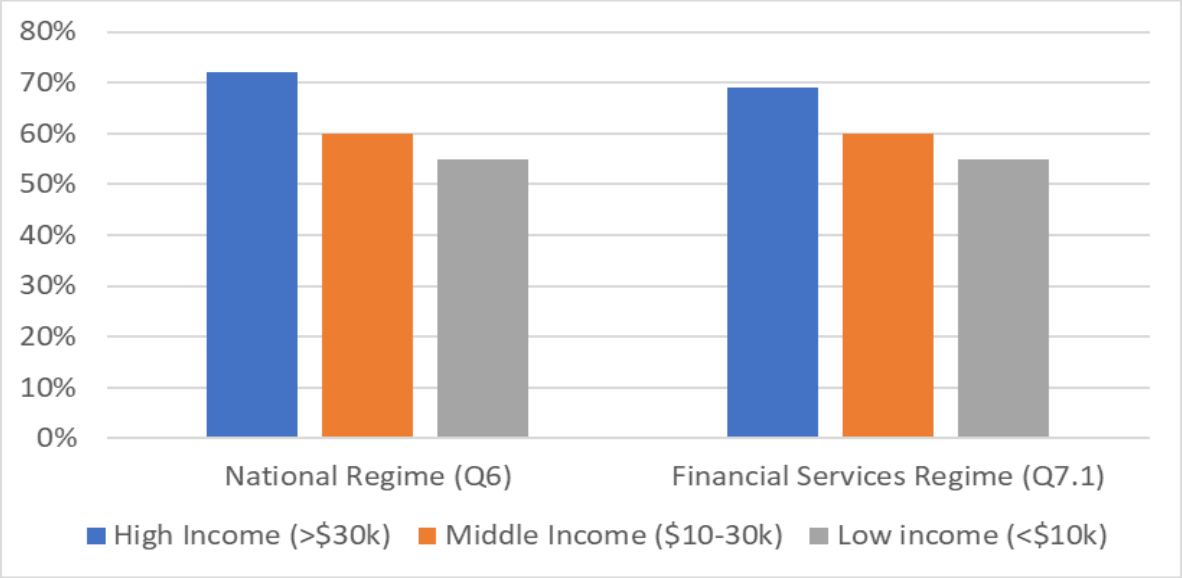
of $10,000-$30,000) perceiving Cyber Risk as lowest while lower GDP per capita jurisdictions (GDP per capita of less than $10,000) perceive Cyber Risk as only a slightly less of a risk than high income countries. This data is reflected in Figure 3, below.

Figure 3
Cyber Risk in Relation to Other Risks



Jurisdictions with higher GDP per capita were more likely to have already adopted a Cyber security framework at both a national or financial services sector level than jurisdictions with a mid-range or lower GDP per capita. Figure 4 below reflects this disparity.

Figure 4
Whether a Cyber Framework Has Been Adopted



Overall, the survey results suggest that, of the IOSCO members that responded to the survey, a majority are acutely aware of Cyber Risks and have implemented Cyber approaches (regulations, polices, frameworks, etc.) that are entirely or generally consistent with one or more of the Core Standards

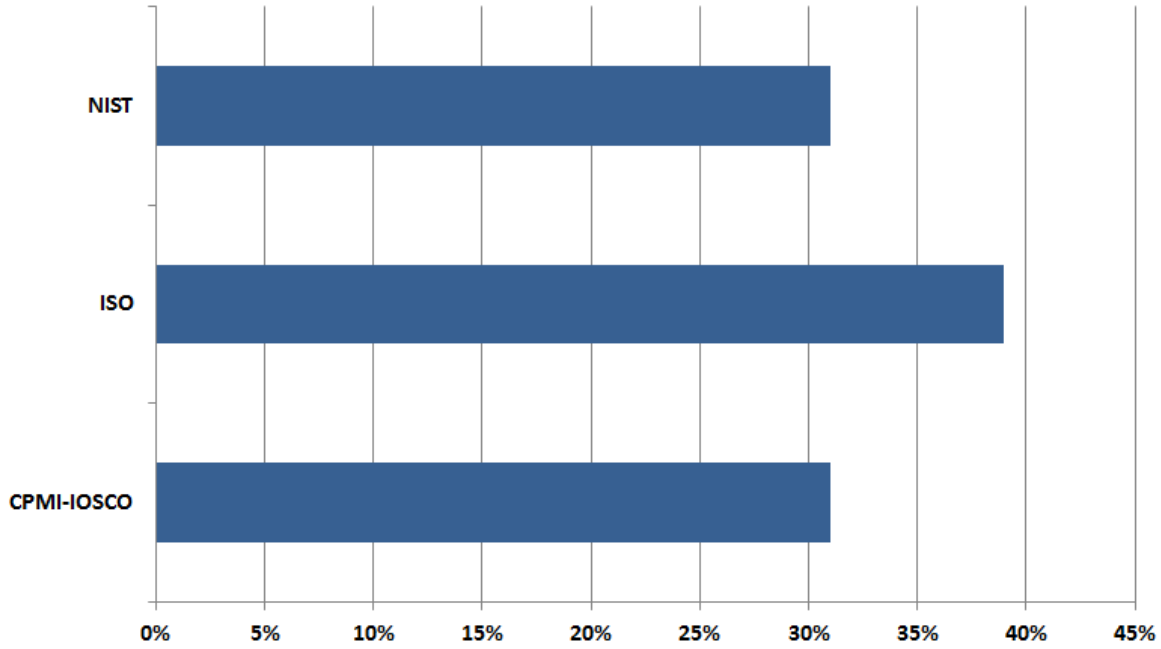
2.2 Consistency with the Core Standards

The survey responses confirm that the Core Standards have gained significant influence with regulators worldwide and across different sectors of the securities markets. Notably, a substantial majority of IOSCO jurisdictions reported that their approaches to Cyber Security regulation are consistent with the Core Standards. Many IOSCO jurisdictions also reported that their Cyber approaches are also consistent with the high-level principles in the G7 Fundamental Elements.

A majority of survey respondents (59%) indicated that their domestic regulations, guidance, and/or supervisory practices were either "generally consistent" or "entirely consistent" with one of the Core Standards.

The survey data also suggest that authorities are influenced by a variety of standards, rather than any single one. As Figure 5, below shows, 31% of survey respondents reported that their Cyber approaches are generally consistent with NIST, 39% reported that their Cyber approaches are generally consistent with ISO, and 31% reported their Cyber approaches were generally consistent with CPMI-IOSCO. These results suggest that, **although the principles underlying the Core Standards have gained considerable influence in IOSCO jurisdictions, no one Core Standard predominates**.

Figure 5
Cyber approaches are generally consistent with Core Standards

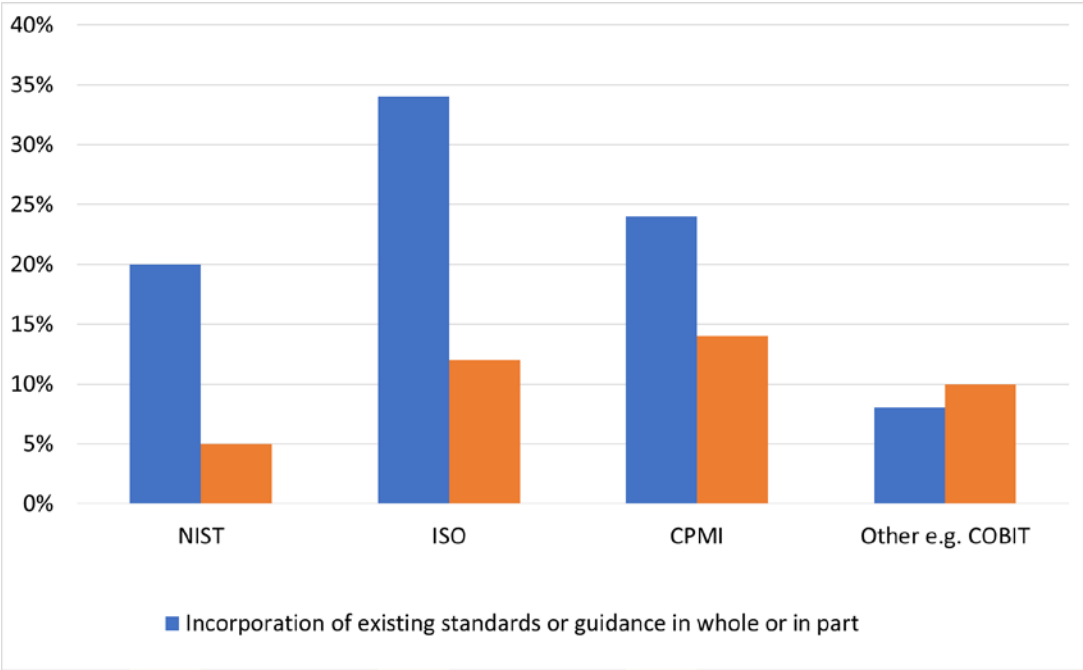


Among the 37% of survey respondents who did not identify their Cyber standards as consistent with the Core Standards, some explained why this is the case. For example, one survey respondent noted that the CPMI-IOSCO Guidance was inapplicable to its regulatory framework, because market participants in its jurisdiction typically use market infrastructures in neighbouring countries.

2.3 Express Reference to the Core Standards

A majority of survey respondents (58%) reported that their domestic regulations and guidance expressly refers to elements of the Core Standards or other prominent standards. Figure 6 illustrates the breakdown of the type of standard that is referenced. The results suggest that ISO is referenced slightly more often in domestic regulations or guidance than any other prominent standard.

Figure 6
Express Reference to Core Standards or Other Prominent Standards



These results may be viewed in a wider context. Notably, **half of the survey respondents (49%) indicated that they are flexible and not prescriptive with respect to which Cyber standards (Core Standards or otherwise) firms may utilise to comply with applicable regulations.** In fact, if a respondent answered "yes" to any part of the question asking about express reference or reliance on a Core Standard, the survey respondent almost inevitably also indicated that its jurisdiction took a flexible approach. This data suggests that among the respondent jurisdictions, most seem to acknowledge there is no one-size-fits-all approach to Cyber Security regulation and instead adopt a principles-based approach. As one IOSCO member noted, regulated firms under its jurisdiction may reference any of the Core Standards to comply with applicable legal requirements. Another IOSCO member noted that one of its key Cyber regulations does not mandate that specific security standards be adopted or followed. Moreover, in a related guidance document, its staff provided examples of standards that a regulated financial entity could look to in developing reasonable policies and procedures to comply with the relevant Cyber regulation.

2.4 Consistency across National Cyber Security Frameworks

The survey analysis highlights several common elements among the national Cyber Security strategies, policies or frameworks across respondent jurisdictions.

Despite jurisdictional differences, common elements exist across the Cyber regimes of most respondents. These common Cyber Security strategies, policies or frameworks elements are:

- The institutionalisation of a national agency that promoted Cyber Security policies and initiatives and had the capability to deliver support to critical infrastructure through, typically, a national Computer Emergency Response Team (CERT).
    - Of those that had Cyber Security strategies, policies or frameworks, about 30% included policies and initiatives for critical infrastructure protection.
- Enhancing Cyber Resilience of government agencies, critical infrastructure and investing in research to build Cyber Security capabilities.
- Establishing and/or adopting Cyber Security standards and implementing certification and accreditation schemes for Cyber Security professionals and service providers, respectively.
- Collaboration between government and industry on Cyber Security initiatives and ecosystem development, in particular treating Cyber Security as an enabler to economic growth.
- Encouraging organisations to establish risk management frameworks of their own with Cyber Security policies along with action plans to monitor implementation of Cyber Security measures such as Cyber Incident management.
- Educating the public on Cyber safe practices and raising the awareness of the public on Cyber Security threats.
- International cooperation between governments to fight Cyber-crime.

About 39% of survey respondents reported that they have public plans to issue, within the next year, new regulations, guidance or supervisory practices that address Cyber Security for all or part of the financial sector. Of that 39%, about 75% have already issued regulations, guidance or supervisory practices. This may be attributed to the need for updated guidance in light of the rapid pace of technological developments and the growing sophistication of Cyber Security threats.

2.5 Potential Gaps in the Application of the Core Standards

Potential gaps the CTF has identified from the survey results are as follows:

- A minority of survey respondents either do not view cyber risk as a major risk or are unsure of its severity. This could mean that these survey respondents do not yet fully appreciate the serious nature of Cyber Risks.
- A minority of survey respondents indicated that their Cyber regimes are not at least "generally consistent" with the Core Standards. As the Core Standards have been

widely adopted, jurisdictions that have regimes which differ significantly from the Core Standards such that their approach is not generally consistent with the Core Standards may find it useful to ascertain where there are material gaps between their Cyber regimes and the Core Standards.

The CTF suggests further exploration of these potential gaps as follow-up considerations.

3. Industry Initiatives

The CTF consulted with the IOSCO Affiliate Members Consultative Committee (AMCC) to understand how industry and firms in various financial sectors (asset management, intermediaries, and exchanges) are addressing Cyber issues. Below is AMCC's high-level summary of private sector initiatives to increase Cyber awareness.

Asset Management:[22] The AMCC Cyber Resilience Task Force Working Group on Investment Management Cyber Security conducted an annual survey to benchmark the Cyber Security posture of the asset management industry globally (AMCC Survey).

The AMCC Survey results show that around one third of respondents fail to achieve even the most rudimentary and fundamental security practices. For example, 35% claim to have not modelled their information security program against any known framework (such as ISO, COBIT, etc.). While small- and even some medium-sized firms may find these and other Cyber Security frameworks overwhelming, some basic implementation of simple, actionable, Cyber Security practice is critical.

The Center for Internet Security (https://www.cisecurity.org/controls/), which details 20 security controls, is another valuable resource for firms whose information security programs are not consistent with one or more established frameworks.

Intermediaries:[23] National Futures Association (NFA), Financial Industry Regulatory Authority (FINRA), Investment Industry Regulatory Organization (IIROC) and The Brazilian Financial and Capital Markets Association (ANBIMA) are self-regulatory organisations that oversee a diverse population of intermediaries. Although these four SROs do not mandate the use of a particular Cyber Security standard, their regulatory programs cover these issues. For example, the NFA requires its Members to adopt a written information systems security program (ISSP), while ANBIMA requires members to implement Cyber Security rules, procedures and controls that should be consistent with the size, risk profile, business model, and complexity of the activities performed by the institution. IIROC requires its dealer members to conduct mandatory self-assessment surveys.

---

22 Response provided by the Investment Company Institute.

23 Response provided by ANBIMA, FINRA, IIROC and NFA.

The four SROs all recognise the need to develop assistance for small and medium sized firms with limited resources to develop effective Cyber Security programs. ANBIMA, FINRA, IIROC and NFA also provide Cyber Security educational initiatives and a number of these resources are customised for small and medium sized entities. For example, FINRA has created a checklist (primarily derived from NIST and FINRA's Report on Cyber Security Practices) to assist small firms in establishing a Cyber Security program. FINRA has also delivered a webinar, entitled "How to Build an Effective Cyber Program with Limited Resources."

Exchanges/Market Infrastructure:[24] In 2017, the World Federation of Exchanges (WFE) published a set of Cyber Resilience standards to ensure alignment and common minimum standards across the global system. In 2018, WFE published a set of best practice guidelines on the behavioural aspects and preventative methods for encouraging employees to comply with Cyber protocols.

WFE established the Global Exchange Cyber Security Working Group (GLEX) in December 2013, to act as an information sharing channel to connect Information Security leadership (i.e., CISOs) amongst the world's leading financial exchanges and CCPs. The primary purpose of the GLEX is to facilitate information sharing. In addition, a more specialised intelligence and incident response sub-group (The GLEX.SECOPS sub-group) was created to share information and track potential adversaries who might have an interest in targeting exchanges.

4. Promoting Sound Cyber Practices

As described in Section 1.2, one of the CTF's primary objectives was to consider how to use the Core Standards to help promote sound Cyber Security practices in IOSCO member jurisdictions. The financial securities sector is interconnected, and therefore Cyber Security practices in one jurisdiction may have potential consequences for the capital markets sector in other jurisdictions. To meet this goal, the CTF, in consultation with the AMCC and other industry stakeholders, created a sample set of 15 questions intended to assist financial sector entities operating in IOSCO jurisdictions in understanding certain key structural components commonly found in the Core Standards.

These questions are not intended to be a shortcut or substitute for the comprehensive Cyber schema found in the Core Standards or the relevant existing regulatory framework.[25] Rather,

---

[24] Response provided by the World Federation of Exchanges.

[25] Nor do they supplant sophisticated mappings that track the relationship between the Core Standards, such as the analysis embedded into the Financial Services Sector Cybersecurity Profile (FSSCP), Version 1.0. Available at https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile .

The FSSCP is a customisation of the NIST Cybersecurity Framework that financial institutions can use for internal and external cyber risk management assessment and as evidence for compliance, encompassing relations between Cyber frameworks, including the Core Standards. Further, the

these questions could be used to promote awareness of sound Cyber Security practices in the financial sector. Specifically, the questions are meant to suggest lines of inquiry by financial sector entities while they review their own practices and are not intended to endorse any regulatory or supervisory framework. Finally, the questions are designed to be consistent with certain common categories found both in the Core Standards and in other Cyber frameworks, guidance and standards, as follows:

- **Identification and protection practices:** identification and protection against Cyber Incidents, such as user authentication; secure network infrastructure; testing (including penetration testing); and password and session timeout controls.

- **Detection practices:** detection of hacking and other risks, and alerting institutions, clients and authorities to mitigate their impact and reduce financial losses.

- **Response and Recovery practices:** developing and managing incident response plans as well as backup and contingency plans that include incident reporting and management of third-party service providers.

The set of 15 questions is as follows:

A. INDUSTRY STANDARD FRAMEWORK:

1. *Does the organisation use an industry standard to develop a Cyber Risk management strategy and framework (e.g., ISO, NIST Cyber Security Framework, and/or others)? Please identify the standard(s).*

B. IDENTIFY AND PROTECT:

2. *Does the organisation maintain an inventory of its software, hardware, applications, and vendors?*
3. *Does the organisation identify Cyber Risks and Vulnerabilities[26] that may impact business operations?*
4. *Does the organisation have an Identify[27] and access management program designed to limit access to and remove access from its users in a timely manner?*
5. *Does the organisation have a Security Awareness and Training Program that allows for individuals to understand their roles within Cyber Security and learn more about emerging threats?*

FSSCC's Cybersecurity Profile tool encompasses all three of the Core Standards of this report, as well as others, detailing how different subsections of each of the three Core Standards (the NIST Cybersecurity Framework, ISO, and the CPMI-IOSCO Guidance), as well as other frameworks may overlap with or be functionally equivalent to each other.

26 Vulnerabilities are defined as a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. *See* the Cyber Lexicon.

27 Identify is defined as to develop the organizational understanding to manage cyber risk to assets and capabilities. See the Cyber Lexicon

6. *Does the organisation employ a Patch Management[28] program to address known software vulnerabilities? Does the organisation employ hardware (e.g., firewalls, network intrusion detection systems) and software (e.g., anti-malware, host intrusion detection systems) to protect its information systems?*
7. *Does the organisation have written procedures to ensure that backups of information are conducted, maintained, and tested periodically?*

C. DETECT:

8. *Does the organisation detect and analyse potential Cyber Events to understand the nature, scope and methods of a Threat Actor?[29]*
9. *Does the organisation implement email protection mechanisms to automatically scan, detect, and block malware or malicious links in email?*
10. *Does the organisation have a testing program to validate the effectiveness of the organisation's incident detection processes and controls?*

D. RESPOND/RECOVER:

11. *Does the organisation have an incident response plan to contain Cyber Incidents and applications and processes to ensure the alert and activation of the plan?*
12. *Does the organisation's incident response plan address information sharing, including managing vulnerability disclosures and other communication, and reporting about Cyber Incidents to internal and external stakeholders, third-parties, regulators, and law enforcement, as appropriate?*
13. *Does the organisation test its incident response plan regularly and update it as needed based on Cyber Incidents that have occurred and Threat Intelligence?[30]*
14. *Does the organisation have a recovery plan to ensure a timely recovery from Cyber Incidents?*
15. *Does the organisation periodically review and update your recovery plan?*

---

28 Patch Management is defined as the systemic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. *See* the Cyber Lexicon.

29 Threat Actor is defined as an individual, a group or an organisation believed to be operating with malicious intent. *See* the Cyber Lexicon.

30 Threat Intelligence is defined as threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. *See* the Cyber Lexicon.

5. Mappings to the Core Standards

Mappings between the Core Standards and Cyber regulatory frameworks may also promote sound Cyber or enhance existing Cyber practices by providing examples of how to incorporate the Core Standards into different types of national Cyber regimes

The survey respondents were asked to provide a "map" between their regulatory or supervisory approach and the Core Standards, such that they are able to illustrate which of their rules, guidance, and practices are consistent with the various subcomponents of the Core Standards. Eighteen IOSCO jurisdictions provided "mappings" which are available to IOSCO members through the Cyber Portal established on the members only section of the IOSCO website.

6. Conclusion and Next Steps

This report endeavours to provide a perspective on the landscape of Cyber regulations among IOSCO member authorities. It examines how members are using the Core Standards and other prominent Cyber guidance in their respective regulatory regimes and identifies potential gaps in the application of these standards that may need to be addressed. It further provides a set of questions that could be used to promote awareness of sound Cyber Security practices within the IOSCO community.

By focusing on the Core Standards and identifying possible regulatory gaps in relation to these already established frameworks, the report underscores first, that IOSCO is not proposing new Cyber standards or guidance in this report. Instead, the optimal path forward, given the reliance by many IOSCO members on the Core Standards, is to continue to draw from existing, prominent Cyber frameworks developed by experts in this space. This approach ensures consistency and avoids overlap, duplication, and conflict between Cyber frameworks, all of which can impede progress in this area.

Second, the report underscores that, because of the high degree of interconnectivity between securities markets, infrastructures, and firms, the global financial markets are only as strong as their weakest link. Thus, while the report finds that IOSCO members have made good progress in establishing appropriate Cyber regimes, there is still work to be done in key areas.

In this regard, the CTF recommends that further work be considered in order to explore this report's findings. In particular, with respect to the potential gaps identified in Section 2.5. we recommend that the CTF consider exploring the use of sector-wide organisational surveys as part of the next phase of its work to gain a better understanding of where the gaps lie.

Annex

Additional Prominent Cyber Standards, Guidance and Frameworks

Of the jurisdictions that have adopted a national Cyber Security strategy, policy or framework, many also reference or expressly follow the tools and good practices in other Cyber frameworks or guidance as well. These other Cyber standards include:

- G7 Fundamental Elements of Cybersecurity for the Financial Sector.[31]
- Guidance and standards provided by jurisdictions' local government agencies and industry associations.
- Center for Internet Security (CIS) Critical Security Controls (CSC).[32]
- U.S. Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool.[33]
- Financial Services Sector Cybersecurity Profile (FSSCP), Version 1.0.[34]
- Global Financial Markets Association's Key Principles for a Commonly Accepted Cybersecurity Penetration Testing Framework.[35]

In addition, there are several general information technology frameworks which including, within them, substantial guidance on Cyber Security and Cyber Resilience. These include:

- COBIT 5 for Information Security.[36]
- Information Technology Infrastructure Library (ITIL).[37]

---

31 *Fundamental Elements of Cybersecurity for the Financial Sector*. Available at: https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf (October 2016). *See* n.14.

32 The CSC is a recommended set of actions in identifying, protecting against, and responding to Cyber Threats and Cyber Incidents. https://www.cisecurity.org/controls/. These controls are consistent with the NIST Cybersecurity Framework but prioritise and focus on a smaller number of actionable controls with "high payoff," identifying key priorities for Cyber Security and Cyber Resilience.

33 https://www.ffiec.gov/cyberassessmenttool.htm (designed to help financial institutions identify risks and determine Cyber Security and Cyber Resilience preparedness) (updated 2017).

34 https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile. *See* n. 5.

35 http://gfma.org/uploadedFiles/News/GFMA_in_the_News/2017/GFMA-Penetration-Testing-Principles.pdf (December 2017). Consistent with this report's focus on existing frameworks, this GFMA publication specifically notes the risks posed by public sector involvement in penetration testing, including the risk of "duplicative and prescriptive penetration testing methods and frameworks" that demand "increased resources within the industry to respond appropriately to each and every test," resources that "could be used more efficiently to protect firms and their clients." *Id*. at 2.

36 The Control Objectives for Information and Related Technology (COBIT) framework was created by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) to help organisations create, monitor, and maintain informational technology generally.

- TOGAF[38]

Moreover, there are substantial online resources to support these various Cyber frameworks and guidance. Examples include:

- NIST Cybersecurity Framework Critical Infrastructure Resources page, Cybersecurity Framework Critical Infrastructure Resources webpage.[39]
- NIST Special Publication 800-series and Special Publication 1800-series.[40]
- Information Security Forum (ISF)'s Research Library.[41]

For jurisdictions that intend to create or improve national Cyber standards and would like guidance in addition to the Core Standards, they may wish to consider reviewing these additional Cyber standards.

Background References

Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience" OFR Viewpoint, February.

ITU, Global Cyber Security Index (2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Securities and Exchange Commission, 2018, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures"

World Bank Group Financial Sector Advisory Committee, Financial Sector's Cybersecurity: A Regulatory Digest World Bank (2017), http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf

Sultan Almuhammadi and Majeed Alsaleh "Information Security Maturity Model for NIST Cyber Security Framework" (2015)

---

37 ITIL is a set of detailed practices for information technology management, including but not limited to Cyber issues. It is owed by AXELOS as a jointly owned venture between Capita and the United Kingdom Cabinet Office. It researched its most recent ITIL 4 Foundation Book in February of 2019.

38 The Open Group Architecture Framework (TOGAF) is a popular framework for enterprise architecture, including a set of supporting tools. https://www.isaca.org/JOURNAL/ARCHIVES/2017/VOLUME-4/Pages/enterprise-security-architecture-a-top-down-approach.aspx?utm_referrer=

39 https://www.nist.gov/cyberframework/critical-infrastructure-resources,

40 NIST publishes a series of guidelines, recommendations, and specifications of general interest to the computer security community. https://www.nist.gov/itl/nist-special-publication-800-series-general-information

41 https://www.securityforum.org/research/

Marsh and Mcllean – Cyber Threats: A Perfect Storm about to hit Europe 2017

Marsh Global Cyber Risk Perception Survey February 2018 “By the Numbers: Global Cyber Risk Perception Survey”

WEF The Global Risks Report 2018 13th Edition

Financial Stability Board, Cyber Lexicon (November 12, 2018), http://www.fsb.org/wp-content/uploads/P121118-1.pdf