Seamless Security

Elevating Global Cyber Risk Management Through Interoperable Frameworks

February 2020

Seamless Security: Elevating Global Cyber Risk Management Through Interoperable Frameworks

Executive Summary

Global cyber threats are increasing in number and sophistication. For many organizations, addressing these threats requires effective cyber risk management and a web of partnerships across sectors and borders. Interconnectedness, including among global enterprises and small businesses integrated into global supply chains, intensifies the importance of more consistent or seamless approaches to security. In developing cybersecurity regulation and guidance documents, government policymakers can foster greater consistency, which has significant benefits not only for security operations but also for economic opportunity,[1] by leveraging internationally recognized cyber risk management frameworks and their standard taxonomies and terminology. Such frameworks, including ISO/IEC 27103, provide a foundational security baseline that facilitates interoperability and cross-sector and cross-border coordination.

This paper describes how international, national, and sectoral frameworks can leverage a common baseline, enabling consistency and interoperability while also building off that common baseline to address any unique concerns of their particular users. It also reflects the collective experience of Coalition to Reduce Cyber Risk (CR2) members that have worked with governments and internally to implement cyber risk management programs across dynamic global infrastructures and operations. We have learned that adoption of globally recognized frameworks, standards, and approaches helps companies manage and evaluate security at scale and focus on protecting their customers. Many of those cyber risk management approaches harness common security principles, desired outcomes, and controls through frameworks and sector-specific profiles.

The Challenge

In seeking to address the very real threats posed by malicious cyber actors, governments are implementing a range of cybersecurity policies and regulations at the national and sectoral levels, often resulting in inconsistent or disparate approaches. Currently, more than 80 countries have a national cyber law or strategy in place,[2] and many more are in development. While the intention to advance cybersecurity is commendable, and the need to respond to cyber threats is undeniable, a lack of international and cross-sector coordination is increasing the challenge of cyber risk management for organizations that operate across borders or integrate into global supply chains.

For companies, cybersecurity regulatory divergence undermines their ability to:

- Respond to multinational cyber incidents in a coordinated fashion;
- Implement best-in-class cybersecurity practices consistently across their supply chain;
- Track and analyze security telemetry at scale, enabling insights into threats and informing security capabilities that can better protect users;
- Share cyber threat information across borders;

[1] Cybersecurity Policy for Resilient Economies: A Global, Cross-Sector Approach, https://www.crx2.org/s/CR2_White_Paper-229x.pdf, at 7-8.
[2] Source: DataGuidance and UNIDIR Cyber Policy Portal.

- Combat online fraud; and
- Allocate resources toward security-enhancing investments rather than often duplicative compliance efforts.

Likewise, for governments, cybersecurity regulatory divergence impacts operations, national economic opportunity, and global security cooperation by:

- Increasing costs of developing and implementing new regulation;
- Delaying the implementation of new regulation;
- Driving up the costs of government services in which increased compliance costs are passed on to users;
- Impeding local companies from integrating into global supply chains;
- Interfering with local companies' ability to access emerging innovations and ideas that are brought to the global market; and
- Disrupting opportunities for dialogue and shared learning across governments.

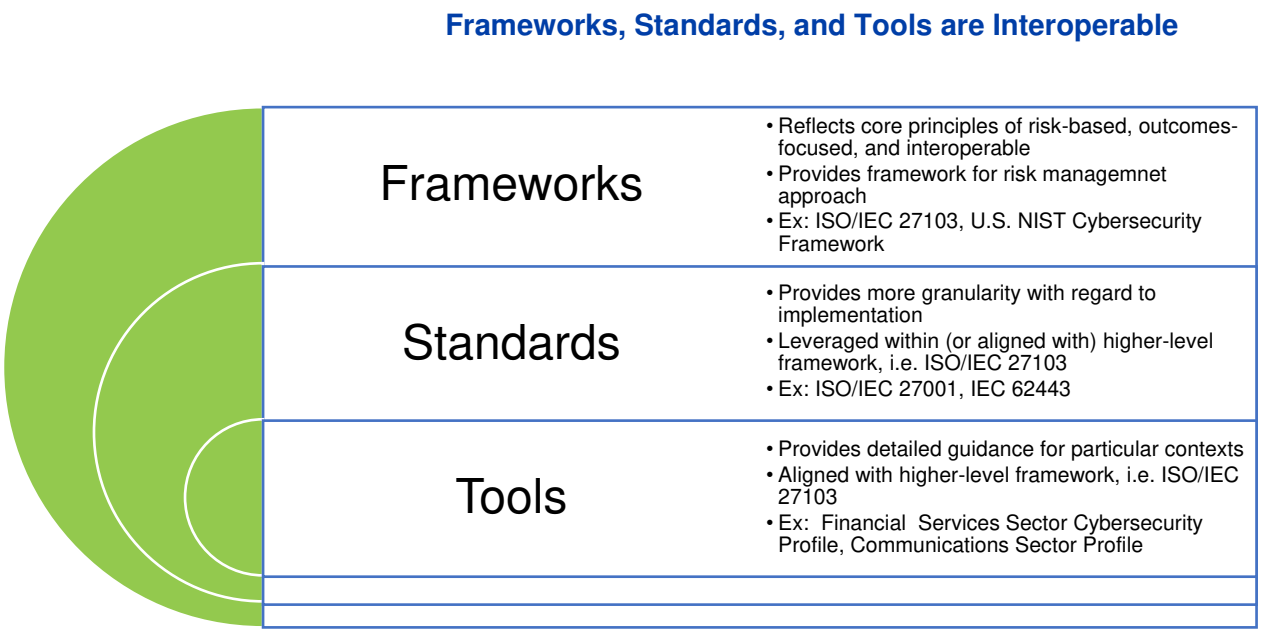
A Better Approach

In order to address shared cyber threats, countries and multilateral institutions should base their cybersecurity standards and policies on a globally recognized core framework for cybersecurity. This framework should prioritize risk management, focus on desired security outcomes, and reflect a consistent and aligned baseline, enabling organizations to interoperate efficiently across interconnected sectors and regions and ultimately, as a result, enhancing security.

A recent publication from International Standards Organization (ISO), ISO/IEC 27103, depicts how to leverage existing global standards in a cybersecurity framework and best exemplifies these core components. ISO/IEC 27103 also incorporates standards that are relevant in both information technology (IT) and operational technology (OT) or industrial control system (ICS) environments, making it relevant across industry verticals that often share many baseline goals and considerations in building out their cyber risk management approach. As such, ISO/IEC 27103 allows global and globally integrated companies from various sectors to implement flexible and extensible frameworks that deliver interoperable cyber risk management practices.

As Figure 1 demonstrates, cybersecurity policymakers and risk managers should draft their national policies or sectoral standards using a global cybersecurity framework like ISO/IEC 27103 as its core and, as necessary, draft derivative implementation guidelines to manage risks that are specific to a particular operating environment — either as a sovereign nation or from an industry-specific perspective. Because those derivative approaches rest on a common security baseline of practices as well as a common taxonomy and lexicon, organizations can build and maintain cyber risk management approaches that work across borders and industry verticals. Ultimately, unnecessary divergence is avoided while options for necessary customization are maintained.

FIGURE 1: ***Frameworks and Implementation Guidelines based on core principles and global cybersecurity risk management frameworks, i.e., ISO/IEC 27103, ensure interoperability and seamless security***



A Coordinated Solution

Numerous national governments and sectoral regulators have already adopted an approach that's consistent with using ISO/IEC 27103 as the core of their cyber framework, reducing barriers to coordination and enabling cross-border, cross-sector cooperation to address shared cyber threats.

We encourage government regulators from all countries and all sectors of the global economy to leverage ISO/IEC 27103 as the starting point for their approach to cybersecurity. The consistency that a common baseline, taxonomy, and lexicon provide will enable government and industry alike to better mitigate threats to their organizations and to our societies as a whole.

Interoperable Frameworks and Tools and Their Adoption

This section provides more information on an interoperable approach by delving into the frameworks and tools introduced in the text and table above. It starts with a review of ISO/IEC 27103, describing the internationally recognized functions, categories, and subcategories that it contains. Notably, the core concepts represented in ISO/IEC 27103 are also the basis of ongoing discussions that ISO/IEC Joint Technical Committee (JTC) 1 Subcommittee (SC) 27 is conducting to develop an international standard, currently referred to as ISO/IEC 27101: Cybersecurity framework development guidelines (DRAFT). As this standardization effort progresses, ISO/IEC 27101 has the potential to become another valuable resource for a risk-based, outcomes-focused, and interoperable approach to developing a cybersecurity framework.

ISO/IEC 27103 provides the initial framing for this section because it presents what CR2 considers to be a common baseline of cybersecurity risk management practices. Then, this section turns to the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") developed by the National Institute for Standards and Technology (NIST) in collaboration with many public and private sector stakeholders. While very similar to the ISO/IEC 27103, the Cybersecurity Framework Version 1.1. contains additional categories and subcategories focused on areas like supply chain risk management, digital identity proofing, and system resiliency. Finally, this section discusses "profiles" for the financial services and communications sectors. These sector-specific profiles include categories that are targeted at these highly regulated industries and capabilities that are specific to their needs (e.g., uptime, dependency management).

What Are Information Security and Risk Management?

Definitions of these key terms vary. The following definitions reflect approaches takes by international standards bodies and are specifically pulled from ISO/IEC 27000:2018.

Information Security
Preservation of confidentiality, integrity, and availability of information.

Risk Management Process
Systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.

ISO/IEC 27103

ISO/IEC 27013: "Cybersecurity and ISO and IEC Standards," published in February 2018,[3] defines and includes a cybersecurity framework and provides a mapping of existing international standards that contribute to the implementation of an effective cybersecurity program. It was developed by public and private sector organizations that are members of their national standards bodies and that participate in ISO/IEC JTC 1's SC 27.[4] According to ISO/IEC 27103, "[a] cybersecurity framework captures a set of desired cybersecurity outcomes that are common across all sectors and organizations" and "facilitates communication about implementation of these desired outcomes and associated cybersecurity activities across [an] organization, from the executive level to the implementation and operations levels"—using functions, categories, and subcategories.[5]

ISO/IEC explains that "[a] framework should consist of five functions, or high-level descriptions of desired outcomes…: Identify; Protect; Detect; Respond; Recover. When considered together, these functions provide a high-level, strategic view of an organization's management of cybersecurity risk. Within each function, there are also

[3] https://www.iso.org/standard/72437.html; https://webstore.iec.ch/publication/62742.
[4] https://www.iso.org/committee/45306/x/catalogue/. ISO/IEC JTC 1 SC 27 develops guidelines, techniques, requirements, and standards that are focused on the security and resiliency of information and communications technologies.
[5] ISO/IEC 27103 at 8.

categories and subcategories, a prioritized set of activities that are important for achieving the specified outcomes."[6] Moreover, ISO/IEC defines its 22 categories as "the subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities" and 88 subcategories as representing the further division of a category "into specific outcomes of technical and/or management activities."[7] Ultimately, according to ISO/IEC 27103, "[o]rganizing a cybersecurity framework into multiple levels, such as functions, categories, and subcategories, helps to enable communication across boundaries."[8] Functions are appropriate for engaging executives, and managers and practitioners can use categories and subcategories; having high-level and more specific descriptions of desired cybersecurity outcomes organized within a single document facilitates communication between executives and practitioners, supporting strategic planning.[9]

ISO/IEC also includes five tables—one for each function—that organize and describe categories that fit within each function as well as "references," or ISO and IEC standards that support the implementation of an effective cybersecurity program.[10] References are intended to go one step further than subcategories, providing more prescriptive guidance that organizations can use as needed. ISO/IEC 27103 integrates international standards developed in collaboration with ISO/IEC JTC 1 SC 27 and other ISO and IEC subcommittees, leveraging broader risk management and security guidance and supporting cross-sector relevancy (e.g., ISO/IEC 20243, ISO/IEC 27002, ISO/IEC 27035, ISO 31000, ISO/IEC 38054, and IEC 62443 among others).[11] An example layout of a function table is included below in Table 1. The first line of the Protect function table, i.e., the category of Access Control, is included as an example; additional categories, descriptions, and references are included in the full table within ISO/IEC 27103.

Table 1: Layout for function/category tables (e.g., Protect function)

Category	Description	References
Access Control	Limiting access to facilities and assets to only authorized entities and associated activities. Included in access management is entity authentication.	ISO/IEC 27002: 2013, Clause 9 ISO/IEC 29146 SIO/IEC 29115 IEC 62443-2-1:2010, 4.3.3.5

There are also two annexes within ISO/IEC 27103. Annex A organizes and describes subcategories that fit within each introduced category and provides a mapping of ISO and IEC standards that support the implementation of each subcategory.[12] Annex B articulates three principles and ten essentials that are particularly relevant for top

[6] *Id.*
[7] *Id.* The 22 categories are: Business Environment, Risk Assessment, Risk Management Strategy, Governance, and Asset Management (within the Identify function); Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology (within the Protect function); Anomalies and Events, Security Continuous Monitoring, and Detection Processes (within the Detect function); Response Planning, Communications, Analysis, Mitigation, and Improvements (within the Respond function); and Recovery Planning, Communications, and Improvements (within the Recover function). The 88 subcategories include activities such as: the organization's role in the supply chain is identified and communicated (within Business Environment category, Identify function); information security policy for the organization is established (within Governance category, Identify function); identities and credentials are managed for authorized devices and users (within Access Control category, Protect function); monitoring for unauthorized personnel connections, devices, and software is performed (within Security Continuous Monitoring category, Detect function); coordination with stakeholders occurs consistent with response plans (within Communications category, Respond function); recovery strategies incorporate lessons learned (within Improvements category, Recover function).
[8] *Id.*
[9] *Id.*
[10] *Id* at 9-13.
[11] *Id.*
[12] *Id* at 14-24.

management, also providing a mapping to ISO and IEC standards that support their implementation.[13] Below, Tables 2 and 3 provide examples of Annex A and B tables. For Annex A (Table 2), the first line of the Access Control category table, i.e., one subcategory within the Access Control category, is included as an example; additional sub-categories and mapped standards are included in the full table within ISO/IEC 27103. Likewise, for Annex B, the first line of the table of standards supporting the three principles is included as an example; additional principles, essentials, and supportive standards are included in the full table within ISO/IEC 27103.

Table 2: Layout for category/subcategory tables (e.g., Access Control category)

Description of Subcategory	Standards Mapping
Identities and credentials are managed for authorized devices and users	ISO/IEC 27002:2013, 9.2.1, 9.2.2, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.2, 9.4.3 IEC 62443-2-1:2010, 4.3.3.5.1 ISO/IEC 27019:2013, 11.1.1, 11.3.1, 11.5.2

Table 3: Layout for principles/supporting standards table (e.g., Principle 1)

Principle	ISO/IEC standard/s
(1) Top management is required to drive cybersecurity measures considering possible risks that accompany wider utilization of IT	ISO/IEC 27104: Information technology—Security technique—Governance of information security ISO/IEC 27001: Information technology—Security techniques—Information security management systems—Requirements

Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework")

The *Framework for Improving Critical Infrastructure Cybersecurity*, also known as the "Cybersecurity Framework," was first published in 2014 and then updated in April 2018.[14] The Cybersecurity Framework was developed by NIST in coordination with public and private sector stakeholders from around the world. NIST has organized open workshops and multiple public comment opportunities to engage with those stakeholders and receive their input on the Cybersecurity Framework and ongoing efforts to improve it.[15] Many global and cross-sector organizations have contributed their expertise by submitting public comments, including the American Petroleum Institute, British Standards Institution (BSI) Group, Center for Internet Security, European Central Bank, Financial Services Sector Coordinating Council, Healthcare Information and Management Systems Society, Information Technology Industry Council, Internet Security Alliance, Kaiser Permanente, National Australia Bank, NTT Corporation, the Open Group, Pricewaterhouse Coopers (PwC) Cybersecurity, Siemens, and US Telecom, among others.

The NIST Cybersecurity Framework has three main components: the Core, Implementation Tiers, and Profiles, each of which is described in detail below. First, the *Core*, which is similar to ISO/IEC 27103, "is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors." It

[13] *Id* at 25-27.
[14] https://www.nist.gov/cyberframework.
[15] https://www.nist.gov/node/1310901/archived-documents

"consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover," and for each Function, there are also underlying Categories and Subcategories that describe discrete outcomes (Version 1.1 has 23 Categories[16] and 108 Subcategories[17]).

The Subcategories are also matched with "example Informative References such as existing standards, guidelines, and practices," providing implementation options and details for practitioners.[18] Leading international, national, and nonprofit resources are included as Informative References (e.g., ISO/IEC 27001, NIST SP 800-53, COBIT, ISA 62443, and the Center for Internet Security's Critical Security Controls). The full Core, including the Functions, Categories, Subcategories, and Informative References, is included in Appendix A of the Cybersecurity Framework.[19] Below, Table 4 outlines the Functions and Categories.

Table 4: Cybersecurity Framework Functions and Categories

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technologies
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

[16] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf at 23.The 23 Categories are included in Table 4.
[17] *Id* at 24-44. The 108 Subcategories include activities such as: physical devices and systems within the organization are inventoried (within the Asset Management Category of the Identify Function); suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process (within the Supply Chain Risk Management Category of the Identify Function); data at rest is protected (within the Data Security Category of the Protect Function); the network is monitored to detect potential cybersecurity events (within the Security Continuous Monitoring Category of the Detect Function); personnel know their roles and order of operations when a response is needed (within Response Planning Category of Respond Function); recovery activities are communicated to internal and external stakeholders as well as executive and management teams (within Communications Category of Recover Function).
[18] *Id*. at 3.
[19] *Id* at 23-44.

Second, *Implementation Tiers* "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk." Tiers can be applied across the Core's Functions, Categories, or Subcategories to provide a high-level or more detailed characterization of an organization's capabilities and investments in cyber risk management processes and practices. Using the Tiers, which range from Partial (Tier 1) to Adaptive (Tier 4), organizations can assess to what extent their processes and practices reflect "informal, reactive responses" to cyber risk or more "agile," coordinated, and "risk-informed" responses to cyber risk.[20] Below, Table 5 introduces the four Tiers; further detail to help organizations assess which Tier best describes their current or target risk management processes is in the NIST Cybersecurity Framework.[21]

Table 5: Cybersecurity Framework Implementation Tiers

Tiers	Descriptions
1	Partial
2	Risk Informed
3	Repeatable
4	Adaptive

Third, *Profiles* can be used "to identify opportunities for improving cybersecurity posture by comparing a 'Current' Profile (the 'as is' state) with a 'Target' Profile (the 'to be' state).... The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can [also] be used to conduct self-assessments and communicate" about cyber risk management capabilities and investments. Within Profiles, Tiers can provide a quantitative metric across relevant Core Functions, Categories, and Subcategories.[22] Below, Table 6 outlines an example method by which organizations may use Current and Target Profiles.

Table 6: Example tables for Current and Target Profiles

Function, Category, or Subcategory	Current	Evidence	Target
Identify	2 (Risk Informed)	Category and/or Subcategory information	3 (Repeatable)
Identify – Risk assessment	2	Subcategory and/or Informative Reference information	3
Identify – Risk assessment – Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	2	Informative Reference or other internal information	3

[20] *Id*. at 3-4.
[21] *Id*. at 8-11.
[22] *Id.* at 4.

Financial Services Sector Cybersecurity Profile

The Financial Services Sector Cybersecurity Profile[23] ("Financial Services Profile") was developed by the financial services industry via the U.S.-based Financial Services Sector Coordinating Council (FSSCC). The Profile was developed in response to a proliferation of international cybersecurity regulatory guidance, examination questionnaires, etc., which topically overlapped but used bespoke organizational structures and semantically different phrases and terms. The process to reconcile these differences with a singular cybersecurity program was diverting available cybersecurity professionals from security-related activity.

The need for a solution became even more pronounced upon the publication of the Financial Stability Board's (FSB) 2017 "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices."[24] The FSB reported that, among its 25 member jurisdictions, there were 56 different sets of cybersecurity regulations and 35 schemes for cybersecurity supervision, none of which was adequately harmonized. Of those 25 member jurisdictions, 72 percent reported that they also planned to issue "new regulations, guidance or supervisory practices that address cybersecurity for the financial sector" in calendar year 2018 alone.

To develop the Profile, starting in late 2016, a coalition of trade associations gathered under FSSCC and began an effort that would ultimately lead to over 50 working sessions. Over 300 individual experts, representing over 150 financial institutions — ranging from community banks and credit unions to large multinational banking, investment, and insurance organizations — participated in and contributed to the sessions.

During the initial sessions, the coalition of experts mapped various financial services regulatory organizations' supervisory expectations against the NIST Cybersecurity Framework, Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO),[25] and relevant ISO standards. With multiple mappings complete, a pattern emerged: Over 80 percent of the mappings were topically identical but semantically different. To reduce the time in reconciling these differences, the experts group began developing a unifying architecture/organizational structure and coding system based on the NIST Cybersecurity Framework and its five Functions, Categories, and Subcategories. The five Function architecture was then extended to include two new functions for the financial services sector – Governance and Supply/Dependency Management – as the mapping revealed that these subjects were distinct areas of appropriate financial services regulatory focus and were items highlighted in the 2016 CPMI-IOSCO "Guidance on cyber resilience for financial market infrastructures."[26] Additionally, the group leveraged the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool, adding a series of Diagnostic Statements that synthesize overlapping expectations from multiple regulatory organizations into a singular, more standardized set of assessment-ready diagnostics and coding them by Function, Category, Subcategory, and associated numbering against the CPMI-IOSCO and NIST Cybersecurity Framework.[27]

In April 2018, NIST hosted an open workshop to further develop a scaling system for the Profile. Over 100 individuals attended, with representation from firms and the regulatory community. From that workshop and the working sessions, the scaling system evolved into the current "Impact Tiering" overlay. Through an associated questionnaire based on regulatory issuances and direction, the Impact Tiering overlay segments financial

[23] https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
[24] https://www.fsb.org/wp-content/uploads/P131017-2.pdf
[25] https://www.iosco.org/about/?subsection=cpmi_iosco
[26] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
[27] https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf

institutions into one of four different Impact levels based on a given institution's complexity, criticality, and interconnectedness, i.e., its impact on the global economy. These "Impact Tiers" are as follows:

Tier 1: National/Super-National Impact – Designated most critical by one or more regulatory agencies and/or bodies (e.g., Globally Systemically Important Bank, also known as G-SIB designation). Implies the gross cyber risk exposure of an organization or service has the most potential adverse impact to overall economic stability.

Tier 2: Subnational Impact – Providers of mission critical services; providers of a high number of services with customer counts rising into the millions. Implies the gross cyber risk exposure of an organization or service has substantial potential adverse impact to the financial services sector and regions of a nation.

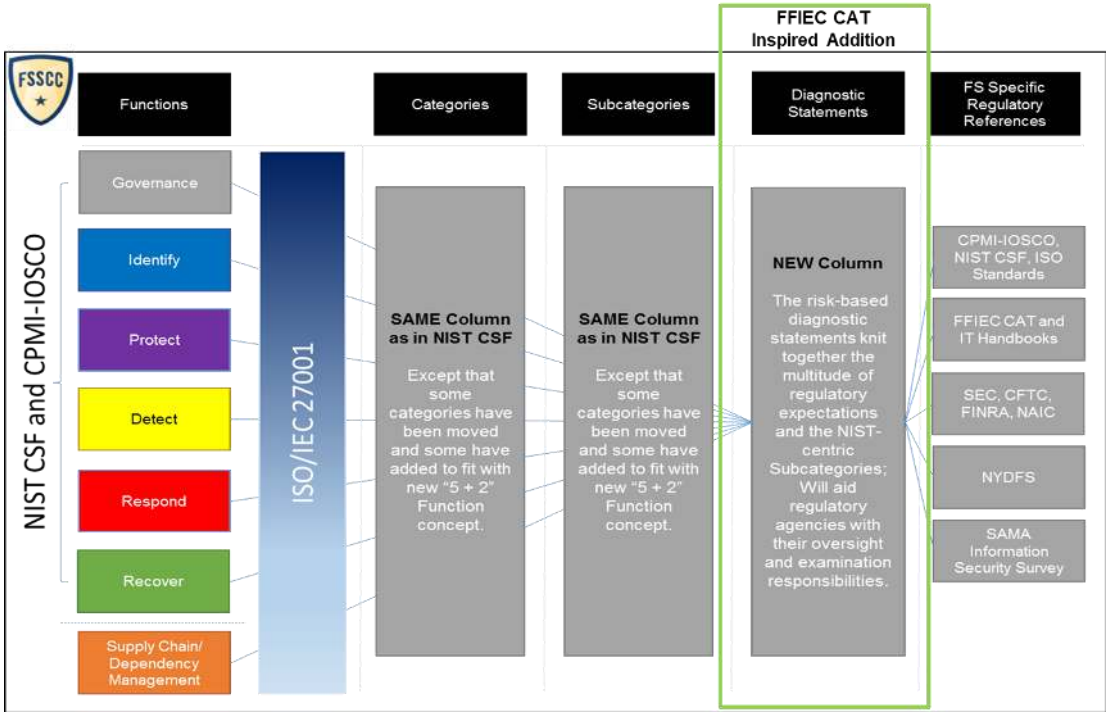
Tier 3: Sector Impact – Institutions with a high degree of interconnectedness, with certain institutions acting as key nodes within and for the sector. The nature of services that these firms provide to others in the sector plays a significant role in determining those firms' criticality.

Tier 4: Localized Impact – Institutions at this level have a limited impact on the financial services sector or more broadly. Typical characteristics include: (a) institutions with a localized presence (e.g., community banks, state banks); and (b) providers of services that do not impact the ability of other institutions to provide services.

Once an Impact Tier is determined, firms then answer Diagnostic Statements that correspond to that particular tier, scaling according to impact (i.e., for Tier 1, 277 Diagnostics; for Tier 2, 262 Diagnostics; for Tier 3, 188 Diagnostics; and for Tier 4, 136 Diagnostics).

Because of this flexibility, financial institutions from across the globe can use the Profile as the baseline assessment with their regulators and even extend the functionality to evaluate partners, vendors, and service providers.

Figure 2: The Financial Services Profile Underlying Organization and Architecture



Communications Sector Profile

The Communications sector similarly undertook efforts to draft a Communications Sector Profile following the release of the NIST Cybersecurity Framework Version 1.0 in 2014. The profile was developed by the Communications Security, Reliability and Interoperability Council (CSRIC)[28] IV Working Group 4 (WG4)—a public-private partnership collaboration with the Federal Communications Commission (FCC). WG4 was tasked with: 1) developing voluntary mechanisms that give the FCC and the public assurance that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise; and 2) providing implementation guidance to help communications providers use and adapt the NIST Cybersecurity Framework in their own operational contexts. WG4 included over 100 industry volunteers from across the five major industry segments (Broadcast, Cable, Satellite, Wireless, and Wireline); stakeholders from other sectors, including academia and government; a Leadership Team of approximately 20 individuals; and a Technical and Policy Advisory Board that included senior representatives from NIST, the White House National Security Council, and the FCC.

WG4 organized itself into five subgroups representing the five key segments of the communication industry (Broadcast, Cable, Satellite, Wireless, and Wireline). Each subgroup had strong industry representation, including representation from small and mid-sized entities. Their representatives were encouraged to pursue independent evaluations of the CSRIC WG4 charge based on their own operating environments. Each segment made its own determination as to what critical infrastructure should be categorized as "in-scope" or "out-of-scope" and which of the NIST Cybersecurity Framework Categories and Subcategories were most critical to protecting that infrastructure. Each subgroup also chose criteria to prioritize the risk management processes. The analyses were intended to be illustrative examples of how individual companies in each segment could go about assessing and prioritizing NIST Cybersecurity Framework components.

WG4 also established five "feeder" subgroups to engage in a deeper, more focused analysis of subject matter areas that would help the communications sector segments evaluate their cybersecurity risk environment, posture, and tolerance. To ensure that the voluntary mechanisms and sector guidance were grounded in accurate information and thoughtful judgments and were practical in their design, the following "feeder" topics were examined: Cyber Ecosystem and Dependencies; Top Threats and Vectors; Cybersecurity Framework Requirements and Barriers; Small and Medium Businesses; and Measurements. Each of the segment subgroups, informed by the findings of the topical feeder subgroups, evaluated the applicability of the NIST Cybersecurity Framework Version 1.0's 98 Subcategories to their segment, prioritized the applicable Subcategories on an illustrative basis, and assessed the challenges of implementation and effectiveness for each applicable Subcategory.

[28] CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. CSRIC's members focus on a range of public safety and Homeland Security-related communications matters, including: (1) the reliability and security of communications systems and infrastructure, particularly mobile systems; (2) 911, Enhanced 911 (E911), and Next Generation 911 (NG911); and (3) emergency alerting.

WG4 produced a final report in March 2015 for communications providers of all sizes and scopes that may use the material to evaluate and improve their cybersecurity posture and communicate needs and expectations both internally and with external stakeholders. The following recommendations are organized around the five key areas of WG4:

1. provide macro-level assurances that communications providers are taking necessary corporate and operational measures to manage cybersecurity;
2. identify voluntary mechanisms that provide assurances that cybersecurity best practices are being adopted;
3. use the NIST Cybersecurity Framework or an equivalent construct;
4. adopt meaningful indicators of successful cyber risk management; and
5. provide communications sector implementation guidance for using the NIST Cybersecurity Framework.

The report also included the individual segment subgroup reports in the appendices to provide concrete guidance on how to use the NIST Cybersecurity Framework to bolster cyber readiness in the communications sector. Each WG4 segment subgroup report surveys infrastructure core assets and critical services and also employs use cases, all with the aim of offering guidance on how to incorporate the risk management protocols and practices referenced in the NIST Cybersecurity Framework with the operating environment of the respective industry segment.

Baseline Comparison

ISO/IEC 27103, the Cybersecurity Framework, the Financial Services Sector Cybersecurity Profile, and the Communications Sector Profile have a number of important similarities: They leverage a common baseline; prioritize risk management; and focus on desired security outcomes. They also have a number of differences, such as the scope of their guidance and the resources from which they draw for references to support implementation. While such differences help each framework and tool address particular concerns or needs of their users, their similarities mean that they have significant interoperability, driving security advancements as well as economic opportunity across the globally connected and sectorally interdependent digital ecosystem.

A common baseline — a set of desired security outcomes and associated cybersecurity activities across at least five common functions, 22 or more similarly scoped categories, and 88 or more similarly scoped subcategories — makes all four frameworks/profiles interoperable, supporting increased focus on security and enabling organizations to operate or integrate more seamlessly across jurisdictions or in the context of different sectors. Additionally, building off a common baseline has enabled shared learning across coordinating organizations and efforts. For instance, as a result of the financial services-specific effort, NIST is now leveraging the Governance Function of the Financial Services Profile to build interoperability into other related but separate frameworks, such as the NIST Privacy Framework, which is currently under development. This use of a common baseline also bridges the gap between NIST's more recent privacy effort and previous related efforts, like the development of the Financial Services Profile.

Moreover, while the NIST Cybersecurity Framework Core, the Financial Services Profile, and the Communications Sector Profile add functions, categories, and/or subcategories beyond what's included in ISO/IEC 27103, the broadly common baseline means that organizations can use all four approaches efficiently. In practice, if an organization chooses or is required to use multiple approaches, it could, for example, directly leverage any existing efforts to implement ISO/IEC 27103 while focusing new resources on implementing the activities that go beyond the common baseline, such as additional categories or subcategories. Alternatively, if an organization is required to use multiple frameworks that do not leverage a common baseline, then it will have to undertake mapping exercises and redundant efforts, diverting organizational resources away from security and toward compliance. Worse still, if an organization is required to use multiple frameworks with conflicting guidance or requirements, then it will have to choose among them and potentially among jurisdictions in which to operate or integrate.

ISO/IEC 27103, the NIST Cybersecurity Framework, the Financial Services Profile, and the Communications Sector Profile also share common, foundational principles. Each framework and tool prioritizes risk management; rather than functioning solely as a compliance exercise in which a binary "yes" or "no" suffices, a risk-based approach allows senior management to understand security posture, engage on risk prioritization, and commit to investments needed to continuously improve. Cyber risk management is a relatively new and technical topic for many company boards and directors, but executive engagement is critical. The organizing logic of ISO/IEC 27103, the NIST Cybersecurity Framework Core, the Financial Services Profile, and the Communications Sector Profile is fundamental to their effectiveness in this regard. As each approach describes security outcomes and cyber risk management activities at various levels of detail (i.e., functions provide a high-level framing, whereas categories, subcategories, and references provide more detail and implementation guidance), they can be used to communicate consistently, both horizontally and vertically, across an organization's executives, business groups, managers, and security practitioners—all of whom require differing levels of detail. Establishing a common language and communicating consistently can bridge risk management understanding across important audiences, such as executives and security practitioners. Moreover, with context on desired security outcomes and cyber risk management activities, executives and managers

can make more informed decisions, resulting in effective prioritization of resources and continuity in security strategy, planning, and investments.

An outcomes-focused approach is also critical to the effectiveness of ISO/IEC 27103, the NIST Cybersecurity Framework, the Financial Services Profile, and the Communications Sector Profile. Whereas a prescriptive approach, framed in terms of compliance-focused security, may be useful to security practitioners at some organizations for specific periods of time, an outcomes-focused approach, framed in terms of what security outcomes need to be achieved, has relevance across organizations and sectors and is more flexible over time. Technology capabilities, including those used for security, are dynamic, and malicious cyber actors are also continuously evolving their techniques and tactics, making adaptability essential for effective cyber risk management. An outcomes-focused approach enables organizations to be adaptable, determining the processes and technologies that most effectively manage risks in their environments today and evolving those processes and technologies along with the changing ecosystem and threat environment. An outcomes-focused approach also encourages organizations to continuously improve their cyber risk management rather than being constrained by a static, prescriptive approach, though it can incorporate more prescriptive guidance that can be leveraged as necessary by practitioners.

The differences between ISO/IEC 27103, the NIST Cybersecurity Framework, the Financial Services Profile, and the Communications Sector Profile do not undermine their interoperability or risk-based and outcomes-focused approaches but rather enhance their utility for their primary users. For example, each of the documents draws from different reference documents. ISO/IEC 27103 (and the forthcoming standard, ISO/IEC 27101) includes only ISO/IEC standards as references and pulls from ISO/IEC standards developed for various sectors, making it especially relevant globally and across sectors. The Cybersecurity Framework includes not only international standards and nonprofit resources but also NIST standards, making it relevant for organizations operating globally as well as for those operating only in the United States. The Financial Services Profile includes sector-specific regulations as references, making it particularly useful for financial organizations that must demonstrate compliance with numerous regulations while seeking to integrate those requirements into a holistic cyber risk management program. The Communications Sector Profile provides surveys of core assets and critical services, as well as employee surveys, to help guide risk management approaches to implementing the NIST Cybersecurity Framework Core.

Ultimately, as an international reference point that integrates existing international standards with demonstrated effectiveness and relevance across sectors, ISO/IEC 27103 is especially useful as a global, cross-sector baseline that can drive continuous improvement in cyber risk management while also facilitating alignment across interdependent sectors and regions (see Figure 1). Governments may also look to the Cybersecurity Framework as a useful model, leveraging a common baseline and international standards and adding categories or subcategories to address particular risk scenarios as well as references to support implementation (i.e., maintaining global standards that are critical for organizations operating across or integrating two or more jurisdictions and adding other standards or guidance that may be more relevant for local organizations). In addition, for sector-specific efforts, governments may consider the Financial Services Profile and the Communications Sector Profile as models, again leveraging a common baseline consistent with international standards but adding to it as necessary to address specific risks and integrate existing sectoral requirements or resources.

Industry Utilization

One of the most important aspects of recognizing and standardizing around a common baseline of internationally recognized cyber risk management practices is the interoperability of those practices across borders and industries. CR2 member companies have enterprises and IT environments that span the globe and multiple sectors and have built cyber risk management programs reflecting that scope. Below are some vignettes that highlight the importance of standardizing around interoperable risk management practices. They are written and submitted by the individual companies in their voice. In addition to these vignettes, CR2 recognizes that many international companies use both the NIST Cybersecurity Framework and relevant ISO/IEC standards to inform their cyber risk management programs.[29]

JP Morgan Chase (JPMC)

JPMC's North American team supports the NIST Cybersecurity Framework and ISO/IEC 27103 through the application of the Financial Sector Profile. Externally, we strongly support the growth and maturation of the Financial Sector Profile. JPMC believes that the comprehensive adoption of the Financial Sector Profile as an accepted standard across our industry would bring significant boosts to efficiency and productivity as it relates to international compliance efforts.

As it stands, JPMC must employ compliance specialists in regions around the world in order to work with local regulators on the unique aspects of their respective regimes. While we acknowledge that every international regulatory regime, and its associated regulatory bodies, will always have unique perspectives and requirements, JPMC believes the formal widespread adoption of the Financial Sector Profile would decrease the amount of effort and resources spent by financial sector organizations on duplicative compliance by 20 percent to 30 percent.

Furthermore, JPMC anticipates the benefits of a more uniformly adopted Financial Sector Profile to increase as it matures and becomes mapped to more regulatory regimes. To help drive adoption, JPMC has joined with other financial institutions to create a Financial Sector Profile implementation guide while supporting the Cyber Risk Institute's stewardship of the profile itself.

AT&T

Network and information security is a business imperative for AT&T. We firmly believe that ubiquitous adoption of risk management approaches to security consistent with the core elements of the NIST Cybersecurity Framework and ISO/IEC 27103, for example, would lead to dramatic gains in industry productiveness by streamlining burdensome regulatory processes. AT&T supports the development of flexible and interoperable frameworks and standards like the NIST Cybersecurity Framework and ISO/IEC 27103. The common adoption of globally recognized industry standards, which are market driven and based on the consensus of industry experts, would be a meaningful step toward reducing the strain that compliance puts on industry.

Microsoft

Since 2014, Microsoft has used the NIST Cybersecurity Framework to assess the company's security capability. We regularly conduct assessments, covering a broad mix of customer-facing and internal infrastructure services across

[29] NIST's website includes several perspectives from various companies that have utilized some or all of its framework. These perspectives can be found at the following URL: https://www.nist.gov/cyberframework/perspectives

the enterprise, and the assessments are the foundation for comprehensive, internal business discussions about security that extend from operational levels to senior leadership and the company's Board of Directors. The Cybersecurity Framework serves as a vehicle to enable such discussions about Microsoft's security profile across organizational silos and subcultures and to bring leaders together to talk about critical capability as well as aspirations and future investments in a risk-based format.

The Cybersecurity Framework's interoperability and strong alignment with global best practices and reference points, including ISO/IEC 27103 and ISO/IEC 27001, also provide security benefits. Microsoft uses the Cybersecurity Framework to develop a unified view of security capability using an external standard and to reconcile multiple security approaches and compliance requirements.

While maintaining strict alignment with the Cybersecurity Framework structure, Microsoft appreciates the Framework's flexibility to integrate with multiple informative references (e.g., ISO 27001) and global approaches (i.e., ISO/IEC 27103). Because of its flexibility and interoperability, Microsoft has been able to adopt and benefit from the Framework in a way that limits operational disruption and results in minimal duplication of efforts. Our investment in the Framework is tailored to existing operational approaches and focused on security capability. For example, we group assessed services into self-defined pillars to enable aggregation and comparison, thus acknowledging and enabling differentiation between types of services.

Microsoft also actively uses the NIST Cybersecurity Framework concept of a Target Profile. This allows for a focused measure of security capability and enables us to discuss priorities and track gaps as well as progress over time, thereby supporting a continuous improvement culture.

HSBC

HSBC's U.S. team approaches cybersecurity risk management through the use of the common core of accepted cybersecurity functions, categories, and subcategories as defined in ISO/IEC 27103 and the NIST Cybersecurity Framework. However, HSBC has found that using this framework appropriately requires implementation and review of security controls by smart, talented practitioners as well as a robust review and challenge process from an independent third party, which in their case is the Second (Resilience Risk) and Third (Internal Audit) Lines of Defense. It also requires an ongoing monitoring process to ensure such reviews and challenges processes do not reflect a "once and done" assessment but rather one that is modified based on internal or external trigger events, such as a change in a technical control.

HSBC believes this approach to cybersecurity risk management — i.e., using the common core of accepted cybersecurity functions, categories, and subcategories as mentioned above or within the Financial Services Profile — should be adopted widely by the industry sector. To do so helps drive consistency between industry sector organizations' cybersecurity risk management programs and what our regulators understand to be acceptable risk management practices. This mutual understanding, exemplified by a common understanding of how to use the agreed-upon framework and what constitutes evidence of compliance, and harmonized terminology could eventually result in a significant decrease in the amount of time and resources that an organization must allocate to understand and become compliant with various international regulatory regimes.

Additionally, HSBC believes that use of a common, interoperable cybersecurity risk management framework would satisfy a significant majority of the international cybersecurity regulatory requirements. As HSBC begins to scale the approach used by the U.S. team, the company anticipates reductions in the time and effort that an organization's security and IT personnel spend mapping and implementing unique solutions for each new regulatory environment.

The time and effort saved will allow these teams in institutions of any size to remain engaged in their primary responsibilities of implementing security tools and controls needed to keep customers' information and finances safe and secure, thus increasing the level of security within the industry.

The overall effect will also be to make compliance more efficient and effective, which in turn will reduce demand for a skill set that is already in short supply. HSBC hires personnel with specific security skills and then asks them to spend their time on compliance rather than protecting the bank. By doing so, we may also reduce the talent available to smaller banks that are not able to compete with large global companies for resources.

Conclusion

As companies and governments have grown more reliant on IT infrastructure to support modern delivery of services to customers and citizens, securing that infrastructure has also grown increasingly important. At the same time, global supply chains and trade have enabled companies to integrate with and manage efforts to provide goods and services in multiple countries around the world. As threats to the IT ecosystem that supports global e-commerce continue to accelerate and adapt new techniques, government and industry must work together to develop and agree upon an interoperable, risk-based approach to meet that evolving threat landscape.

Many countries and companies have identified key practices that underpin cyber risk management and are using those practices as the baseline to build out their cyber risk management policies and programs. These programs often support organizations that span the globe and share information across numerous borders. Many nations have also embraced these core risk management practices as the basis of the cybersecurity policies that support their own IT infrastructure. This common approach to cyber risk management allows for interoperable approaches to deal with the constantly evolving threat landscape, helping to secure interactions between the nation states and the companies that help drive economic development for their citizens. Ultimately, while cybersecurity policies that are inconsistent across jurisdictions or sectors risk weakening global cybersecurity and undercutting economic advancement, aligned approaches support global exchange of information, enable greater visibility into global threats, increase access to best-in-class products and services, and promote economic advancement.

As governments initiate a range of efforts intended to address cybersecurity challenges, we encourage them to consider not only appropriate policy processes and principles but also how their efforts contribute to security across our global, interconnected ecosystem. Specifically, as governments and industry sectors focus on cyber risk management, we strongly encourage the leveraging of a common core of accepted cybersecurity functions, categories, and subcategories, such as those outlined in ISO/IEC 27103.

CR²

COALITION TO REDUCE
CYBER RISK