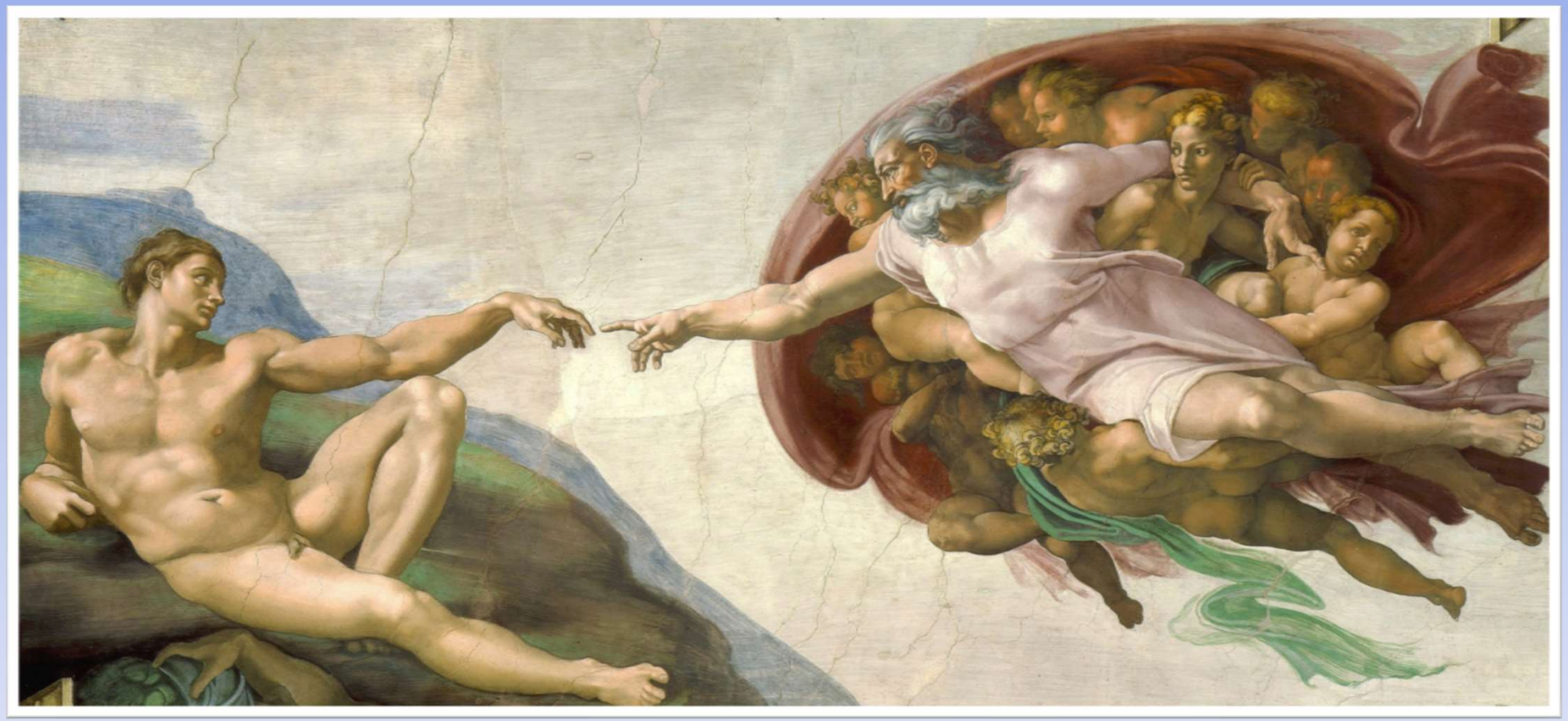
International frameworks for cyber resilience in the financial sector

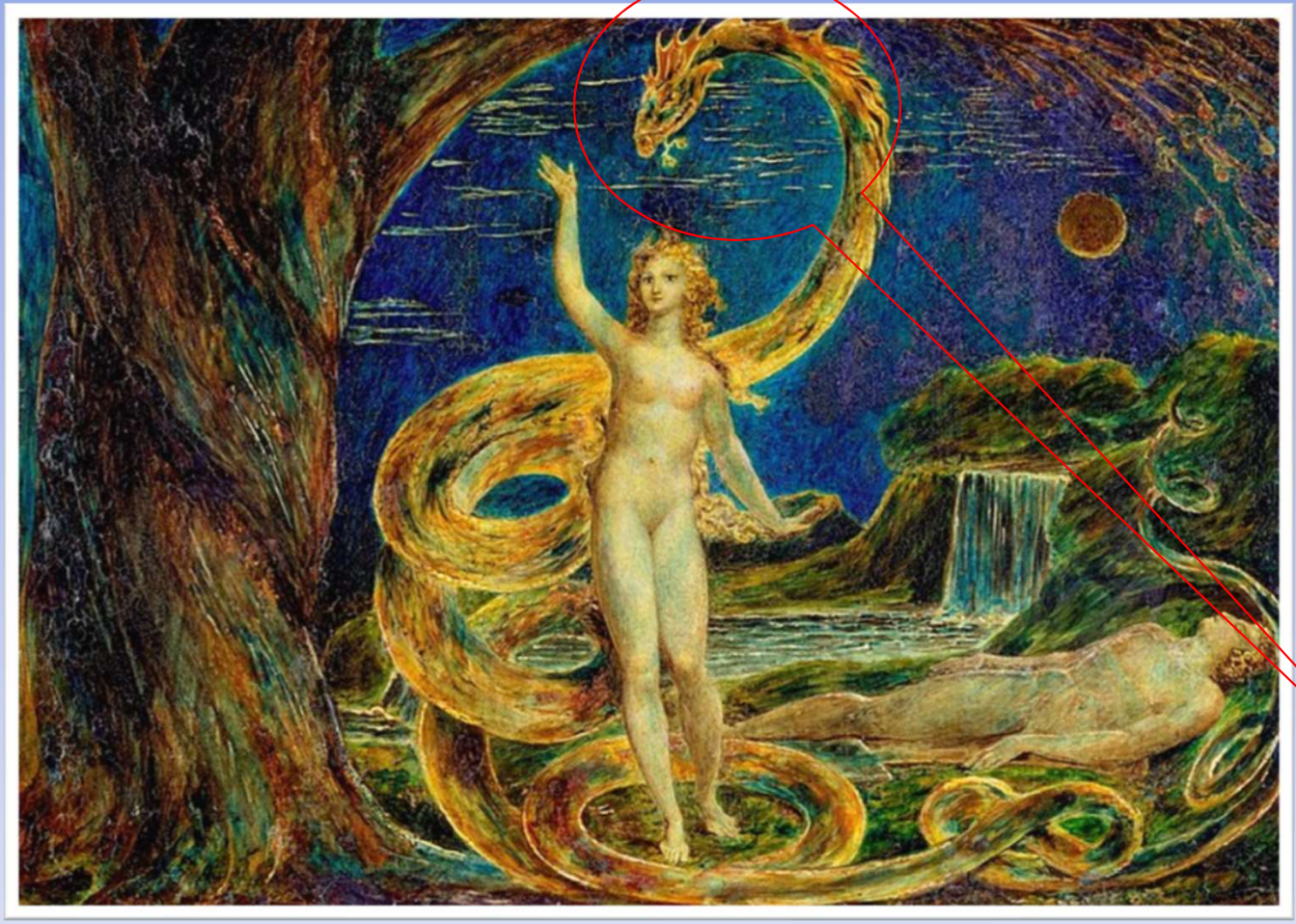
- Session I -

6 November 2019

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security



The Creation of Adam by Michelangelo



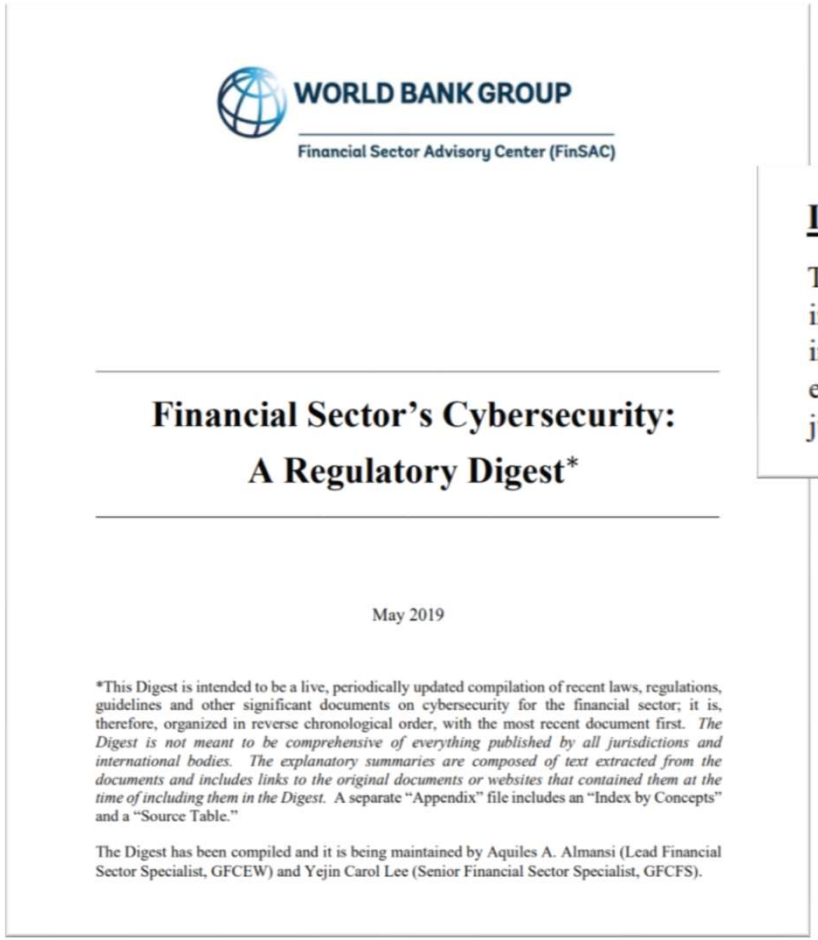
Eve Tempted by the Serpent by William Blake

Genesis 3:1 -

Now the serpent was more crafty than any of the wild animals the LORD God had made. He said to the woman, “Did God really say, ‘You must not eat from any tree in the garden’?

The first lawyer?

Cybersecurity Regulatory Landscape



WORLD BANK GROUP

Financial Sector Advisory Center (FinSAC)

Financial Sector's Cybersecurity: A Regulatory Digest*

May 2019

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

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

INTRODUCTION

This is the third edition of the World Bank's FinSAC Digest of Cybersecurity Regulations in the Financial Sector. It adds 40 cybersecurity related regulatory or supervisory initiatives (in 45 documents) to the 116 (in 128 documents) included in the previous edition, including cybersecurity related regulatory or supervisory initiatives of five jurisdictions previously not captured: Estonia; Ghana; Kenya; Nigeria; and Rwanda.

- 156 cybersecurity related regulatory or supervisory initiatives
- 173 documents

FSSCC

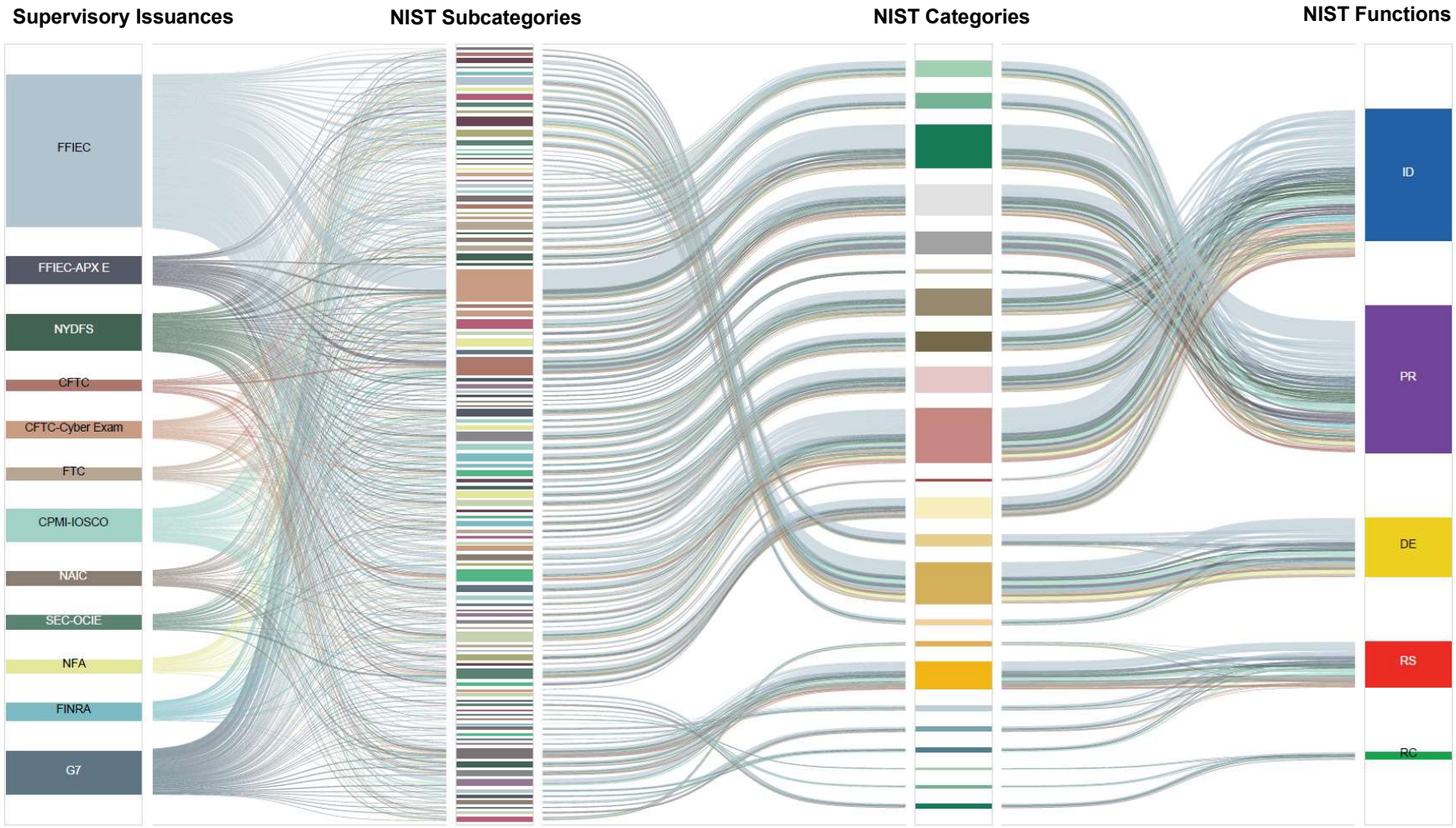
The Standards Landscape

	NIST	CPMI-IOSCO	ISO	NIS	G7	COBIT
Developed by	U.S. non-regulatory agency	International standard setting bodies	Independent, nongovernmental, worldwide federation of national standards bodies	Adopted by the European Parliament	G7 Finance Ministers	IT Governance Institute and the Information Systems Audit and Control Association (ISACA),
Designed for	Usable by all, but originally created for critical infrastructure operators	Financial market infrastructure (FMI)	All sectors, public and private	EU Member States and essential services and digital services providers	Financial sector private and public entities	Usable by private sector firms (the enterprise), but originally the financial audit community
Cost	Free	Free	Charges apply	Free	Free	Charges apply
Approach	Framework	Principles/Guidance	Framework, Menu of Controls, and Guidance	Legislative Framework	Principles/ Fundamental Elements for Framework Building	Framework
Key Components	**Functions:** 1. Identify, 2. Protect, 3. Detect, 4. Respond, 5. Recover	**Risk Management Categories:** 1. Governance, 2. Identification, 3. Protection, 4. Detection, 5. Response and Recovery **Overarching Components:** 1. Testing, 2. Situational Awareness, 3. Learning and Evolving	**27001:** Defines a suite (menu) of activities for managing information risks **27002:** Code of good practices recommended to meet security control objectives	**27 Articles:** ***1–6*** - scope and main definitions; ***7–10*** - describe the national frameworks for adoption; ***11–13*** - describe cooperation mechanisms; ***14–18*** - define the security requirements and incident notification for operators of essential services and digital service providers, respectively; ***19-20*** - The adoption of standards and the process of voluntary notification are dealt with in articles; ***21–27*** - Misc	**The elements include:** 1. Cybersecurity Strategy and Framework, 2. Governance, 3. Risk and Control Assessment, 4. Monitoring, 5. Response, 6. Recovery, 7. Information sharing, and 8. Continuous learning	Defines generic processes for the management of IT, with each process defined together with – • process inputs and outputs, • key process-activities, • process objectives, performance measures, and • an elementary maturity model
Updates	Periodic, Version 1.1	N/A	Periodic	N/A	N/A	Periodic, COBIT 2019

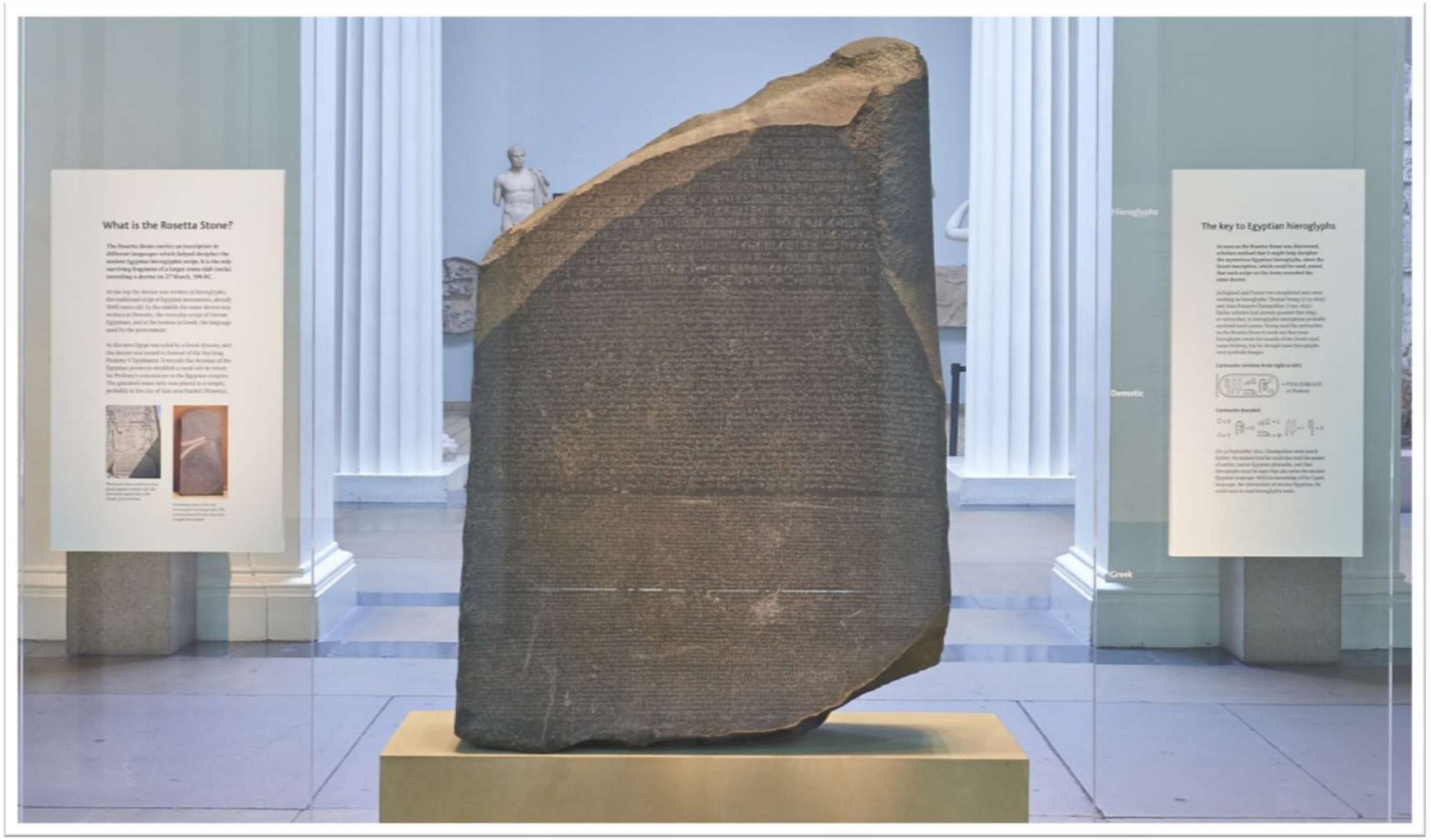
* Developed from multiple sources, including the Financial Stability Board “Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices” and OICV-IOSCO “Cyber Task Force: Final Report”

Tower of Babel by Pieter Bruegel the Elder

A Graphical Depiction of the Reconciliation Process: Topical Overlap, Difference in Phrasing



The Rosetta Stone: The Inspiration for the Profile

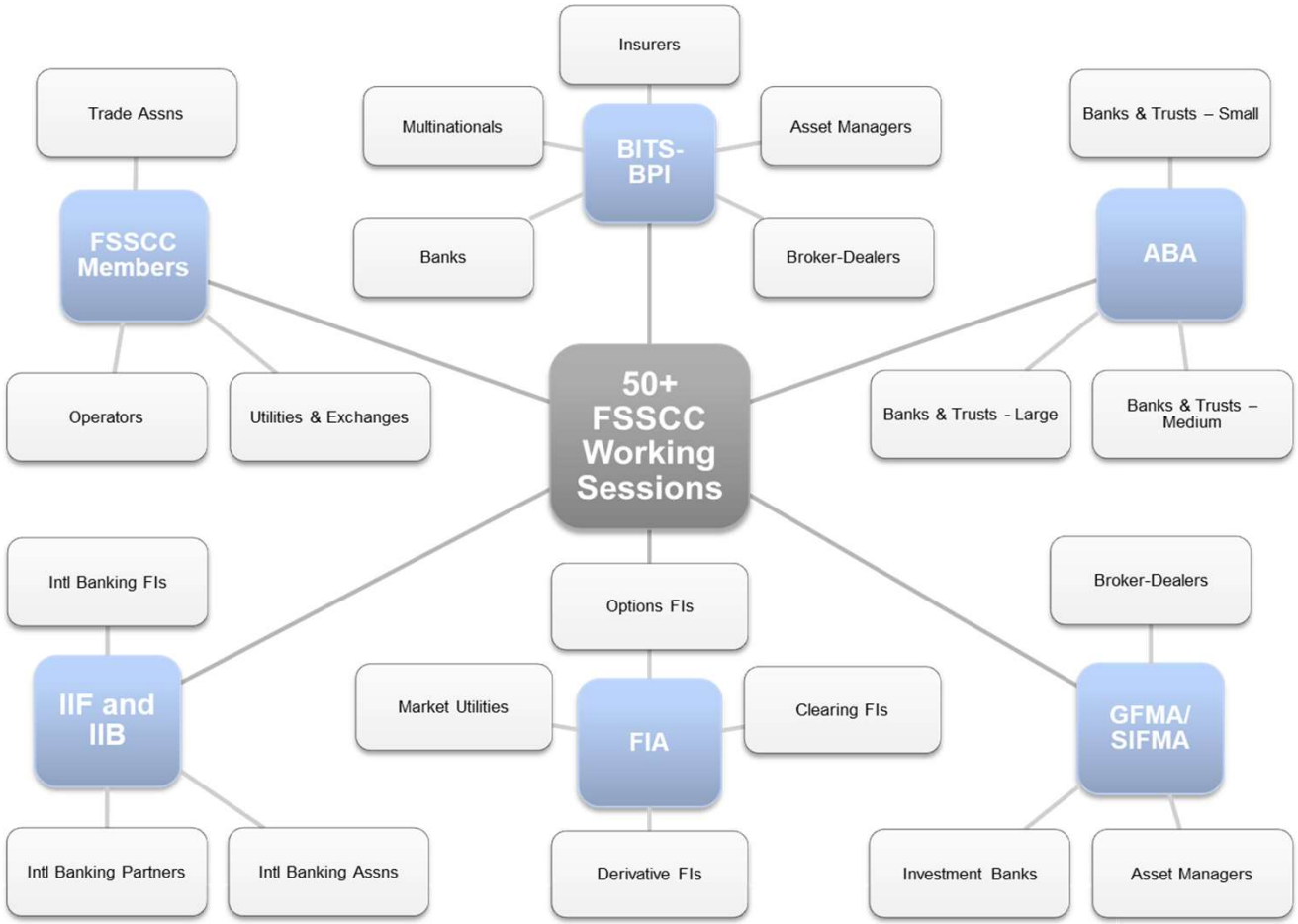


Developing the Profile: The Process and Main Participants

Starting in Q3 2016, a coalition of trade associations under FSSCC led between 50+ working sessions with over 300 individual experts, representing over 150 financial institutions ranging from community banks and credit unions to large multi-national banking, investment and insurance organizations.

The inputs were discussed, debated, and adjudicated based on a consensus process.

These working sessions were largely co-led by BITS, ABA, and the team of framework and standards experts at Boston Consulting Group-Platinion, led by Nadya Bartol.



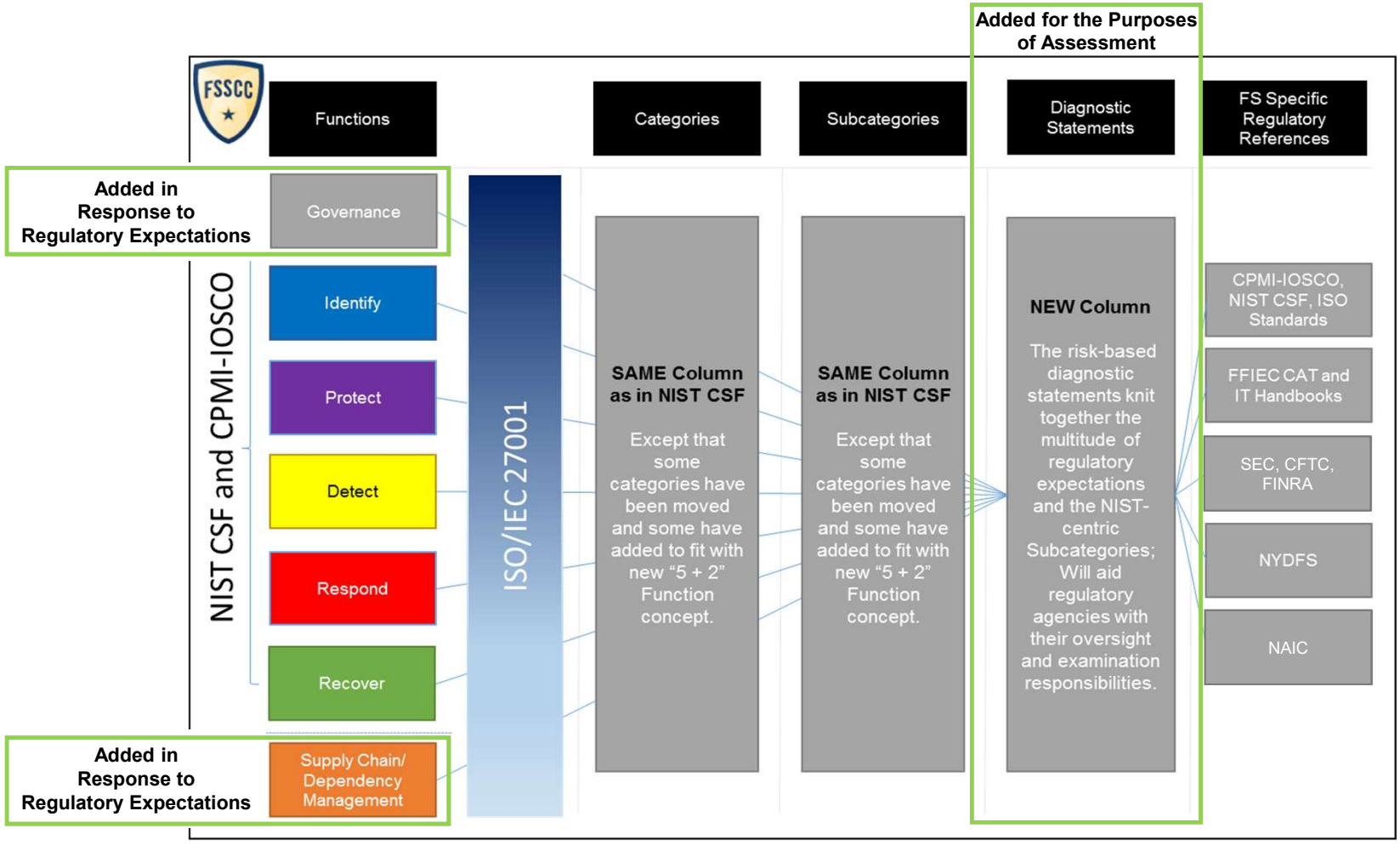
1) Part I: Impact Assessment (9 questions)

2) Part II: The Architecture, Diagnostic Statements, and Underlying Regulations

Profile and materials available at no cost:

- https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
- https://www.fsscc.org/The-Profile-FAQs

Part 2: Architecture, Diagnostic Statements, and Example Regulations (Part 1 is Next Slide)



Part 1: Sector-wide Scaling through an Impact Assessment (Part 2 is Prior Slide)

Impact Questionnaire

- ***9 Questions***.
- Scaled according to an institution's impact on the global, national, and local economies.
- Questions based on global methodologies, such as Basel Committee determinations for G-SIBs, transaction volume, and interconnectedness.

National or Global Impact – Tier 1

- Applies to systemically important and/or multinational firms.
- Examples: GSIBs, GSIFIs, systemically important market utilities.

277 Diagnostics

Subnational (Regional) Impact – Tier 2

- Applies to firms offering mission critical services or having more than 5m customer accounts.
- Examples: Super-regional banks, large insurance firms.

262 Diagnostics

- Industry-wide scaling achieved through government and industry collaboration.

- ~ 70 firms implementing the Profile or actively exploring implementation for 2019/2020.

188 Diagnostics

- Applies to firms with a high degree of interconnectedness and between 1-5 customer accounts.
- Examples: Regional banks, large credit unions.

Sector Only Impact – Tier 3

136 Diagnostics

- Applies to firms with a smaller number of customers.
- Examples: Community banks, small broker dealers/investment advisors.

Customer/3rd Party Impact Only – Tier 4

Benefits of the Profile Approach

In excess of 2300 regulatory provisions reduced to 9 tiering questions and 277 Diagnostic Statement questions, an approximately 88% overall reduction

Financial Institutions

- ✓ ***Optimization of cyber staff' time*** "at the keyboard," defending against attacks – ***complete once per cycle, report out multiple times***.
- ✓ ***Improved Boardroom and Executive engagement***, understanding and prioritization.
- ✓ Enhanced, ***efficient third-party vendor management***.

Supervisory Community

- ✓ ***Examinations tailored to institutional complexity, enabling scrutiny*** in areas of greater interest.
- ✓ ***Enables supervisory agencies to better understand the sector's systemic risk***, with more time for testing and validation.
- ✓ Enhanced ***visibility of non-sector and third-party cyber risks***.

The Ecosystem

- ✓ ***Based on NIST and ISO, it allows for greater intra-sector, cross-sector and international cybersecurity collaboration and understanding***.
- ✓ Enables ***collective action to better address collective risks***.
- ✓ ***Greater innovation as technology companies, including FinTech's, are able to demonstrate compliance to accepted cybersecurity standards.***

Appendix: A Conceptual View of Our Approach

Annex A:
Additional Tables

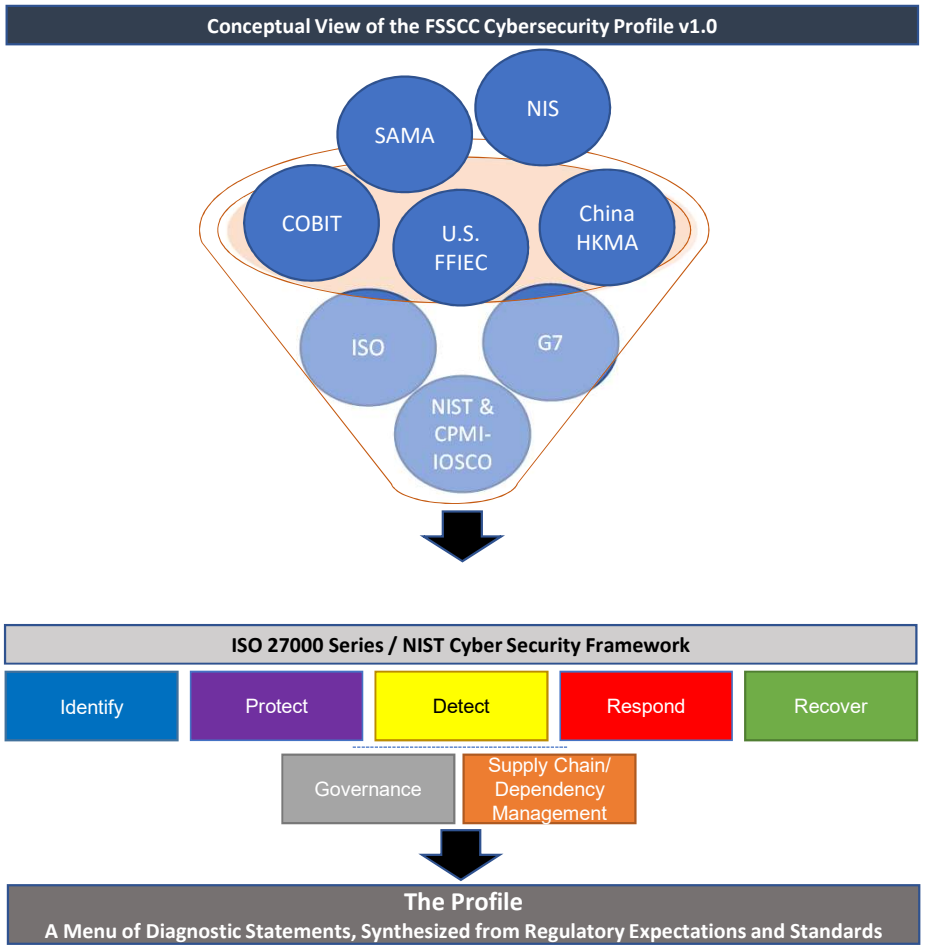
Table 6: Number of Jurisdictions Reporting Use of Existing National or International Guidance or Standards in their Regulatory and/or Supervisory Practices Schemes

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

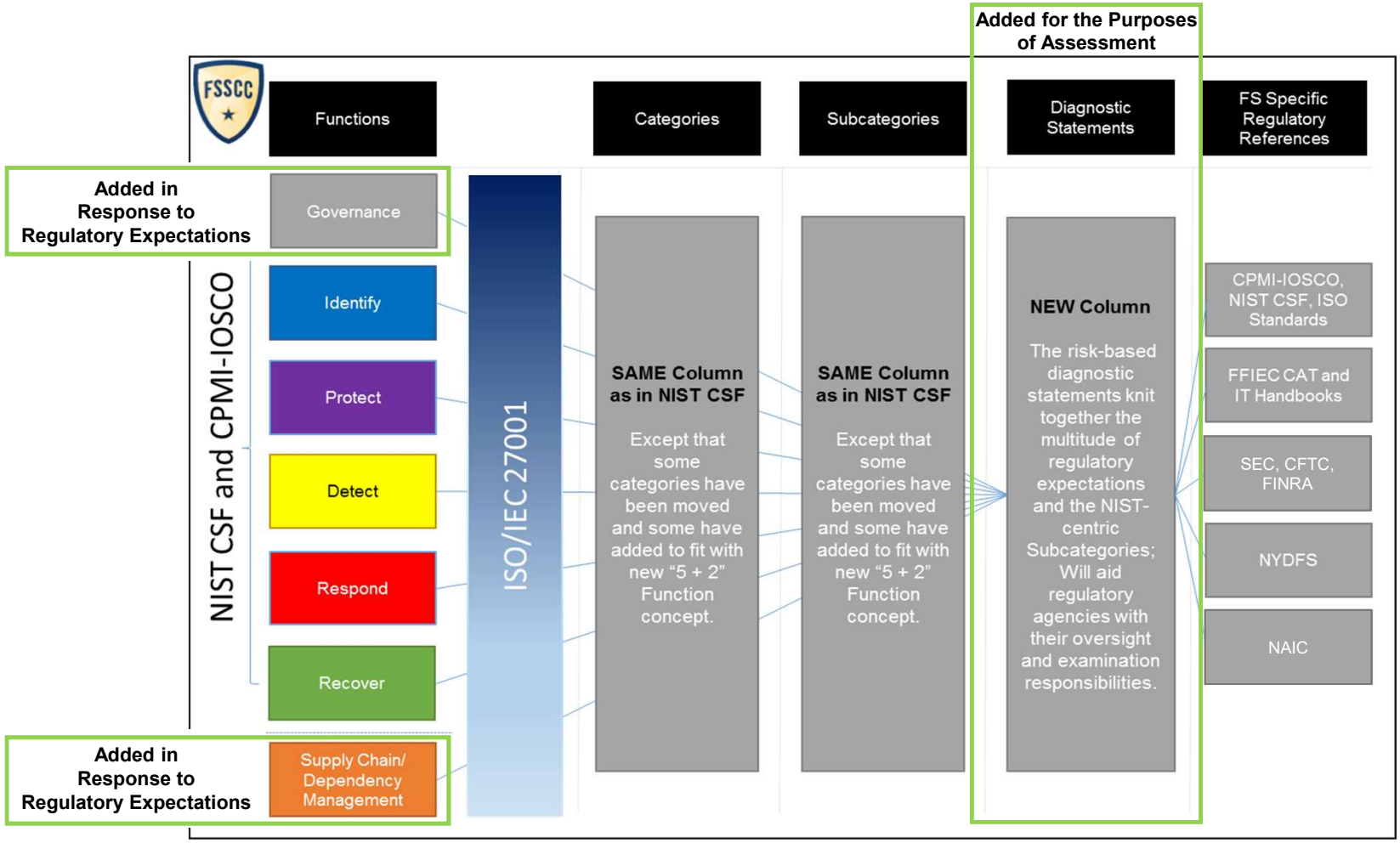
* Financial Stability Board "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices"

■ Jurisdictions with coverage

Blank cell indicates no coverage



Appendix: Architecture, Diagnostic Statements, and Example Regulations



Appendix: The Additions of Governance and Supply Chain/Dependency Management

Identify

ID.AM	Asset Management
ID.BE	Business Environment
ID.GV	Governance
ID.RA	Risk Assessment
ID.RM	Risk Management
ID.SC	Supply Chain

Governance

GV.SF	Strategy and Framework
GV.RM	Risk Management
GV.PL	Policy
GV.RR	Roles and Responsibilities
GV.SP	Security Program
GV.IR	Independent Risk Management Function
GV.AU	Audit
GV.TE	Technology

Supply Chain / Dependency Management

DM.IM	Internal Dependencies
DM.ED	External Dependencies
DM.RS	Resilience
DM.BE	Business Environment

Appendix: A Visual Example of the Impact Tiering, the Diagnostics, and Potential Responses

A More Granular View The Profile identifies key attributes of a cybersecurity program and articulates them in a consistent manner through suggested diagnostic statements and references to recognized standards and best practices. The Profile can be leveraged to respond consistently to multiple supervisory requests.

Functions	Categories	Subcategories	NIST CSF v1.1 Ref	FS Profile Diagnostic Statements	Diagnostic Statement Reponses	Tier 1: National+	Tier 2: Sub-National	Tier 3: Sector	Tier 4: Localized	FS References	Informative References from NIST CSF v1.1
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	ID.RA-5	ID.RA-5.2: The organization considers threat intelligence received from the organization's participants, service and utility providers and other industry organizations.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					NYDFS/500.02, NYDFS/500.03, NYDFS/500.09, NFA/Security Risk Analysis, CFTC-Cyber Exam/A, CPMI-IOSCO/Situational awareness, FFIEC/1, FFIEC/2, FFIEC-APX E/Mobile Financial Services Work Program, CFTC/E, FFIEC IT Booklet/Information Security/II.C, FFIEC IT Booklet/Operations	• CIS CSC 4 • COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
				ID.RA-5.3: The organization has established threat modeling capabilities to identify how and why critical assets might be compromised by a threat actor, what level of protection is needed for those critical assets, and what the impact would be if that protection failed.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					NYDFS/500.02, NYDFS/500.03, NYDFS/500.09, NFA/Security Risk Analysis, CFTC-Cyber Exam/A, CPMI-IOSCO/Situational awareness, FFIEC/1, FFIEC/2, FFIEC-APX E/Mobile Financial Services Work Program, CFTC/E, FFIEC IT Booklet/Information Security/II.C, FFIEC IT Booklet/Operations	
				ID.RA-5.4: The organization's business units assess, on an ongoing basis, the cyber risks associated with the activities of the business unit.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					G7/3, NYDFS/500.03, NYDFS/500.09, NAIC/4, FFIEC/5, NFA/Security Risk Analysis, CFTC-Cyber Exam/A, CPMI-IOSCO/Situational awareness, FFIEC/1, FFIEC/2, FFIEC-APX E/Mobile Financial Services Work Program, CFTC/E, FFIEC IT Booklet/Information Security/II.A, FFIEC IT Booklet/Management/III, FFIEC IT Booklet/Operations	

The **'Diagnostic Statements'** column defines authoritative, common language for multiple regulatory requirements, enabling Firms to comply with largely the same but distinct requirements from different supervisors

The **'FS References'** and **'Informative References'** columns detail specific mapping of distinct requirements to the single Profile requirement

Appendix: Sector-wide Scaling through an Impact Assessment

Impact Questionnaire

- ***9 Questions***.
- Scaled according to an institution's impact on the global, national, and local economies.
- Questions based on global methodologies, such as Basel Committee determinations for G-SIBs, transaction volume, and interconnectedness.

National or Global Impact – Tier 1

- Applies to systemically important and/or multinational firms.
- Examples: GSIBs, GSIFIs, systemically important market utilities.

277 Diagnostics

Subnational (Regional) Impact – Tier 2

- Applies to firms offering mission critical services or having more than 5m customer accounts.
- Examples: Super-regional banks, large insurance firms.

262 Diagnostics

- Industry-wide scaling achieved through government and industry collaboration.

- ~ 70 firms implementing the Profile or actively exploring implementation for 2019/2020.

188 Diagnostics

- Applies to firms with a high degree of interconnectedness and between 1-5 customer accounts.
- Examples: Regional banks, large credit unions.

Sector Only Impact – Tier 3

136 Diagnostics

- Applies to firms with a smaller number of customers.
- Examples: Community banks, small broker dealers/investment advisors.

Customer/3rd Party Impact Only – Tier 4

Appendix: Impact Tiering Questionnaire – An Example

Example Off-Ramp for Impact Tier 1

Q1.2 – Does your organization consistently participate in (e.g., clear or settle) at least five percent of the value of transactions in a critical market? Check all that apply.

- ❑ A. Federal Funds
- ❑ B. Foreign Exchange
- ❑ C. Commercial Paper
- ❑ D. U.S. Government Securities
- ❑ E. U.S. Agency Securities
- ❑ F. Corporate Debt
- ❑ G. Corporate Equity Securities
- ❑ H. Derivatives

If No to <u>all</u>: Proceed to **Criticality Level 2: Subnational Impact** and its questions.

If Yes to <u>any</u>: Our organization is designated a **Level 1: National/Super-National** impact.

Legend

National+ - 1	Subnational - 2	Sector - 3	Localized - 4

Based on the responses selected, the survey will either off-ramp (once an organization is deemed ***Level 1: National/Super-National Impact*** no more questions will need to be answered) <u>OR</u> it will continue until a determination of the impact tier has been reached.

For all tiers outside of ***Level 1*** additional questions will be required to determine the impact tier.

Appendix: Regulatory Complexity Example with Respect to Third Party Oversight

	To assess compliance with a requirement defined in multiple sources…	*…each regulator asks for information in a different way…*	*…to which a financial institution provides a different response.*
EXAMPLE 1 Requirement that the organization will have a formal **third party due diligence and monitoring program.**	OCC 2013-29, FRSR 13-19, ANPR/4, NYDFS/500.11, FFIEC/4, COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013, NIST SP 800-53	**OCC:** "Provide a description of outsourced application development arrangements."	A listing of approved application development suppliers
		FRB: "Provide documentation on third party relationship lifecycle"	Third Party Oversight Policy, Standards, other materials
		NFA: "Provide documentation on due diligence on critical service providers"	Overview of Firmwide Critical Supplier function
		FINRA: "Provide information on ongoing due diligence on existing vendors"	Overview of Third Party Oversight function
		NFA: "Provide information on measures to conduct due diligence on third party providers with access to the firm's data or information systems."	Overview of Third Party Control Assessment process
EXAMPLE 2 Requirement that the organization will conduct **risk assessment** to define, implement and monitor controls to address the risks presented by each third party.	OCC 2013-29, FRSR 13-19, ANPR/4, NYDFS/500.11, FFIEC/4	**OCC:** "Provide a detail of Third party Risk Assessment process"	Overview of Inherent Risk Rating, Control Assessment Questionnaire, Contracting process
		FINRA: "Provide understanding of vendor relationships, outsourced systems and processes as part of the firm's risk assessment process"	Overview of Third Party Oversight function and control assessment process
		CFTC: "Provide cybersecurity risk assessments of vendors and business partners"	Overview of Third Party Oversight function and risk assessments
		OCC: "Provide the most recently completed supplier risk assessment"	Supplier risk and control assessment results for specified suppliers
		NFA: "Describe how the bank assesses threats posed through any third party"	Overview of Third Party Oversight function, Inherent Risk Rating and Control Assessments
EXAMPLE 3 Requirement that the organization has established **policies**, plans and procedures to identify and manage risks associated with third parties.	OCC 2013-29, FRSR 13-19, ANPR/4, NYDFS/500.02, FFIEC/4	**Taiwan Financial Supervisory Commission:** "Please describe the review process for Third Party Risk Management Policy"	Overview of Policy review process and frequency
		Reserve Bank of India: "Describe outsourcing and vendor management process controls"	Third Party Oversight Policy, Standards, assessment process, Minimum Control Requirements for suppliers
		Central Bank of Philippines (BSP): "Describe how the bank considers strategic and business objectives prior to outsourcing"	Overview of Third Party Oversight function, including engagement initiation and approvals requirements

Appendix: The Profile as a Tool for Public/Private Collaboration

Globally

- ✓ **CPMI-IOSCO** lists the Profile as a cyber framework to follow.
- ✓ **Financial Stability Board (FSB)** harmonizing around key cyber terms and definitions, drawing from the Profile sources (NIST and ISO).

U.S. Federal

- ✓ **Federal Reserve (FRB)** mentioning the Profile's use as an acceptable assessment methodology in upcoming First Day examination letters with plans to train examiners.
- ✓ **SEC Office of Compliance Inspections and Examinations (OCIE)** training its staff on Profile usage in Nov 2018.

U.S. States

- ✓ **New York Department of Financial Services (NYDFS)** modifying its final regulation in favor of an assessment based approach.
- ✓ **National Association of Insurance Examiners (NAIC)** exploring voluntary use of the Profile for exam purposes.

Standards Bodies

- ✓ **International Standards Organisation (ISO)** developing a standard on standards development, adopting the Profile development process.
- ✓ **NIST and ISO** drafting, with FSSCC, a joint white paper describing the complementary nature of each.

Appendix: Documented Agency Statements of Support

- **CPMI-IOSCO:** "The [FSSCC's Cybersecurity Profile] 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 FSSCC's Cybersecurity Profile tool encompasses all three of the Core Standards of this report, as well as others…."

- **NIST:** "…[O]ne of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date."

- **FFIEC:** The FFIEC "emphasized the benefits of using a standardized approach to assess and improve cybersecurity preparedness," and named the Profile along with NIST, CAT, and the CIS 20 (formerly SANS 20) as those standardized assessment approaches.

- **Federal Reserve:** "… we'll welcome any financial institution to provide information to us using the structure and taxonomy of the profile, we see that as a boon for harmonization."

- **OCC:** "If the industry moves to use this cybersecurity profile, that is what we will base our assessments on…."

- **FDIC:** "That was one of the things, at the FDIC, that we were most interested in is looking at the tiering."

- **SEC:** "…to the extent that we can rationalize and cut down on that duplication, allowing those scarce resources to start driving toward protecting the enterprise, I think we're in a good space."

Appendix: Issue, Solution, Benefits, and Supporters

The Issue: Domestic and international regulatory agencies asking the same question in different ways, stretching limited cybersecurity talent and resources**.**

The Profile as a Solution: The Profile provides a common methodology and standardized approach for cybersecurity oversight**.**

Voluntary with Many Benefits, Including:

- Provides consistent and efficient processing of examination material for financial services and regulators.
- Allows regulators and financial companies to focus on systemic risk to the financial sector and economy.
- Establishes industry best practices.

Supporting Associations:

FSSCC Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

American Bankers Association

bpi Business Innovation Technology Security BITS

FIA

gfma

iib Institute of International Bankers Advancing the interests of the International Banking Community in the United States www.iib.org

IIF Institute of International Finance

Appendix: Other Takeaways and Key Points

- BPI and BITS Member CEOs, FSF Member CEOs support, understand, and are willing to finance Cybersecurity Profile and caretaker organization forward.
- Developed by 150 financial institutions, 300 subject matter experts, incorporating financial services regulatory agency feedback.
- Based on widely used and effective risk-based frameworks to manage cyber risks and enhance resiliency, including US, IOSCO, NIST, ISO, COBIT, and others.
- Scaled to cover financial institutions from across the sector based on the impact that institution might have to the overall economy if affected by an event.
- Saves resources for both regulators and financial institutions allowing increased focus on most important risks and investment to mitigate those risks.
- Profile is freely available and freely downloadable in the widely used Microsoft Excel format.