

Understanding the FSSCC Cybersecurity Profile: For State Bank Regulators

December 11, 2019



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

Speakers Page: Introductions and Biographies



Denyette DePierro
VP & Senior Counsel
American Bankers Association

Denyette is the co-lead of the FSSCC Cybersecurity Profile initiative. Additionally, she serves as ABA's VP and Counsel where she focuses on the state, federal, and international regulation of technology, cybersecurity, privacy, and emerging trends, including fintech, blockchain, IoT, AI, and social media.

Prior to the ABA, Denyette was Legislative Counsel at the Independent Community Bankers of America (ICBA). She received her J.D. and M.D.R from the Pepperdine School of Law, where she was a fellow at the Straus Institute for Dispute Resolution.

She received a B.A. from the University of California, Santa Barbara, and was a EU Fellow at the University of Padua in Padua, Italy in Developmental Economics.

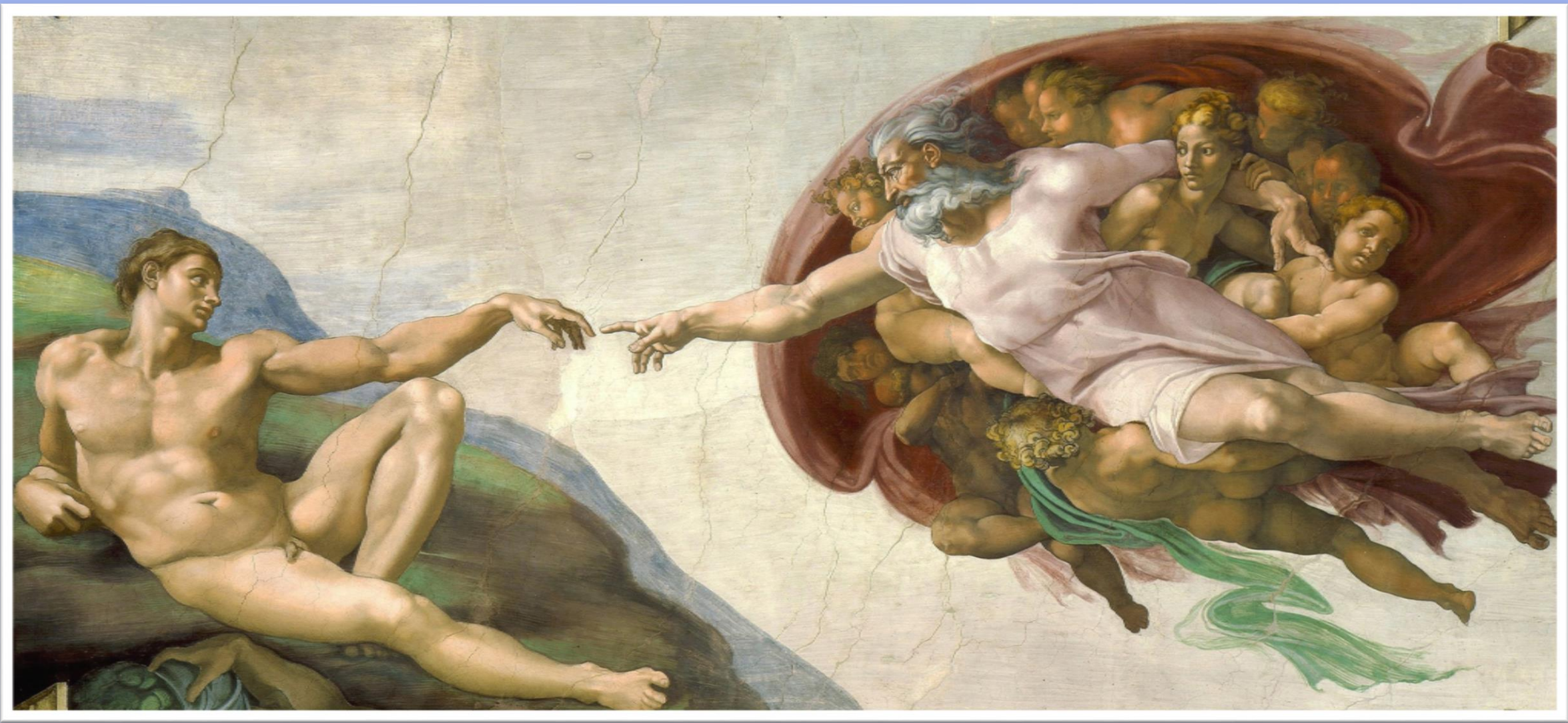


Josh Magri
SVP & Counsel
Bank Policy Institute - BITS

Josh is the principal architect and co-lead of the FSSCC Cybersecurity Profile initiative. Additionally, he serves as SVP and Counsel for BITS at the Bank Policy Institute. Previously, he served as Vice President and Counsel for Regulation and Developing Technologies at the Financial Services Roundtable/BITS.

In these roles, Josh has overseen regulatory, advocacy, and policy efforts on issues related to cybersecurity, data security and privacy, financial technology ("FinTech"), and developing technologies.

Josh received his J.D. from Boston College Law School and his undergraduate degree in Economics from Boston College.



The Creation of Adam by Michelangelo





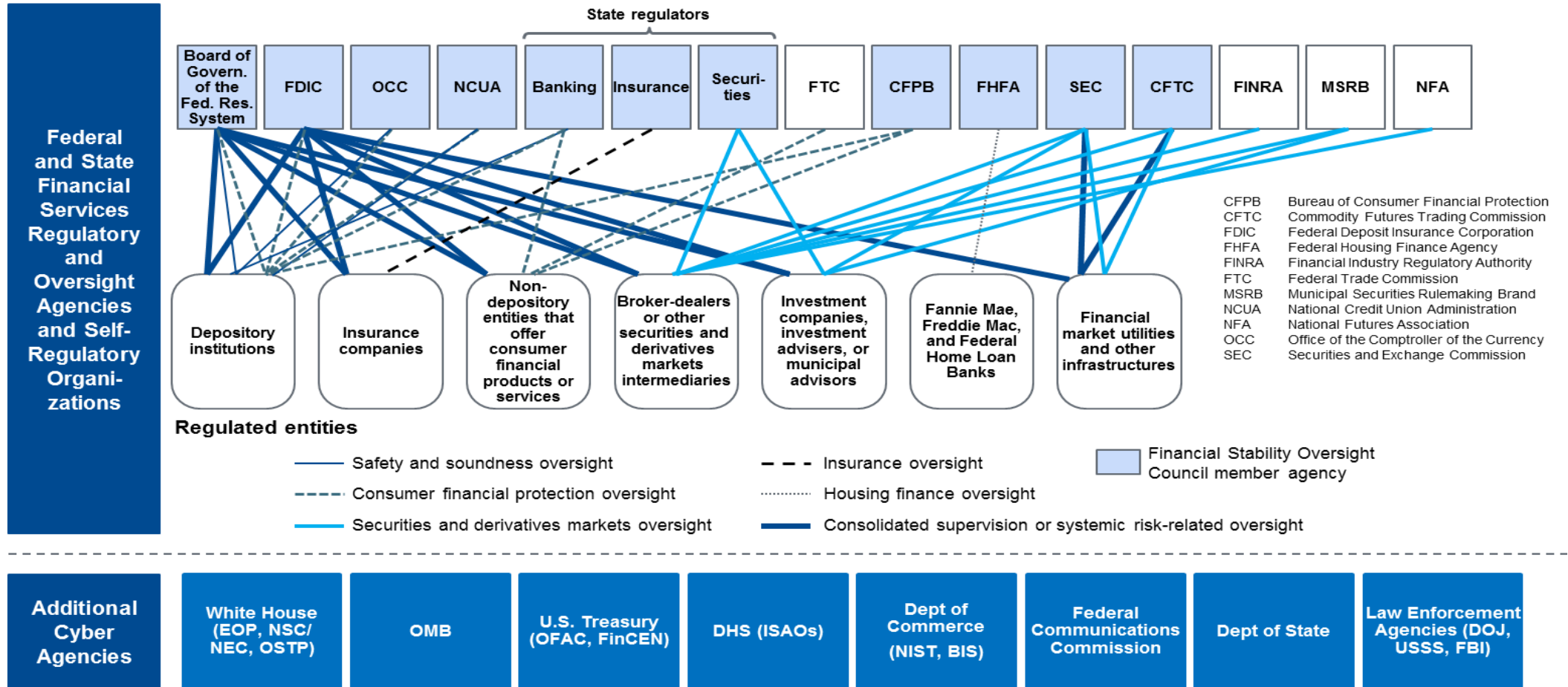
Genesis 3:1 -

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?

Eve Tempted by the Serpent by William Blake

The U.S. Financial Services Regulatory Structure (2019)



Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure

Source: GAO; GAO-16-175





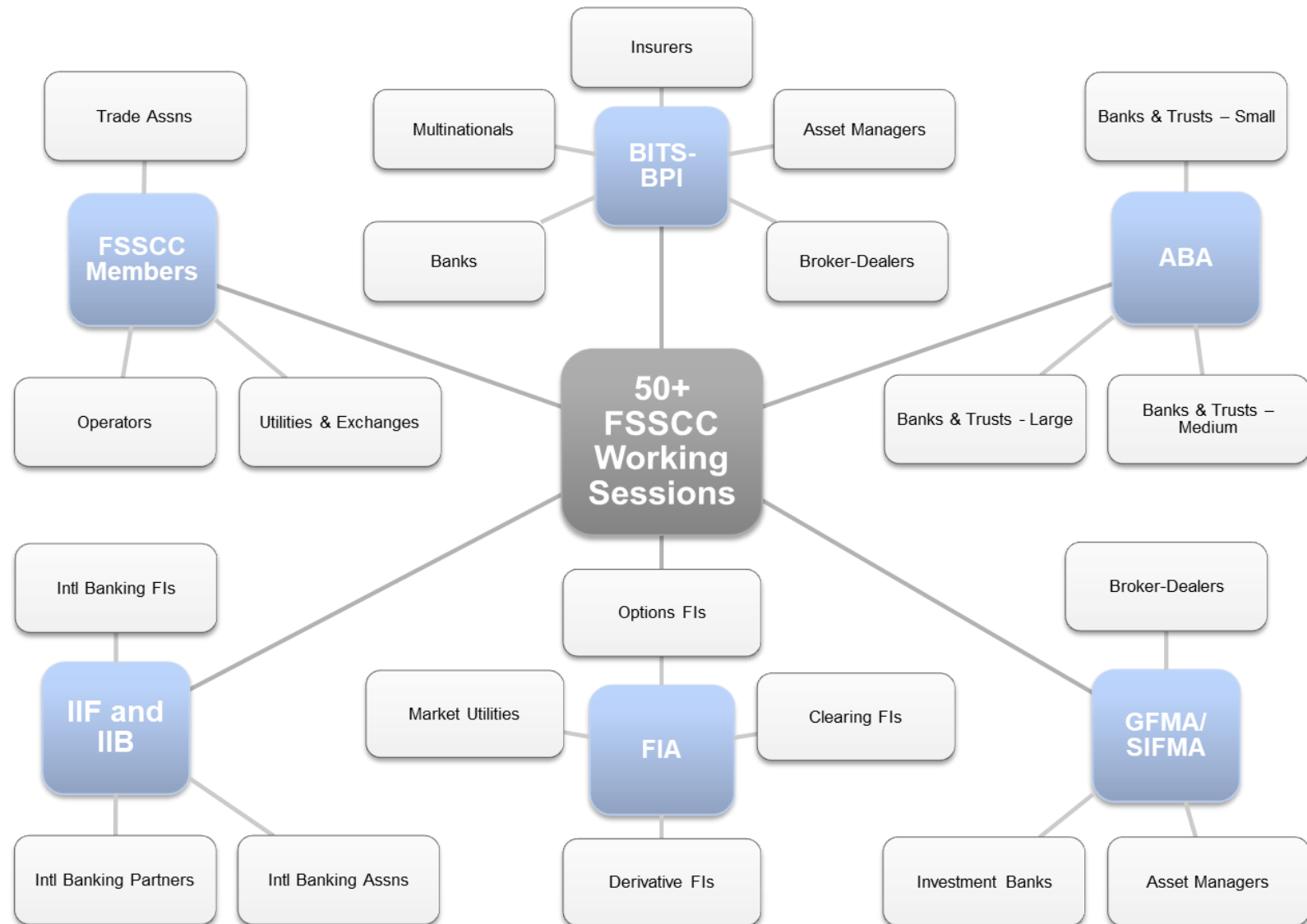
Tower of Babel by Pieter Bruegel the Elder

Developing the Profile: The Process and Main Participants

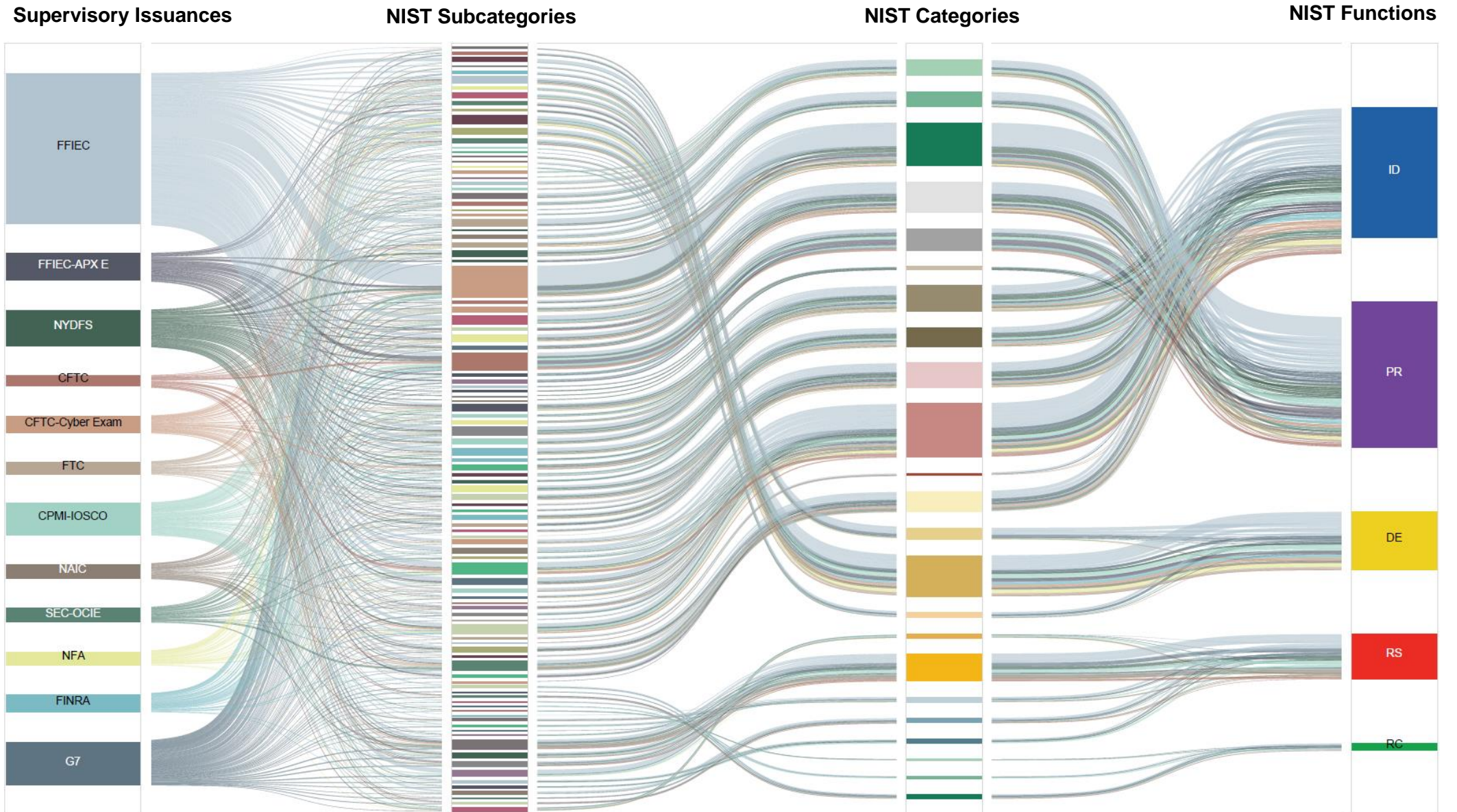
Starting in Q3 2016, a coalition of trade associations under FSSCC led between 50+ working sessions with over 300 individual experts, representing over 150 financial institutions ranging from community banks and credit unions to large multi-national banking, investment and insurance organizations.

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

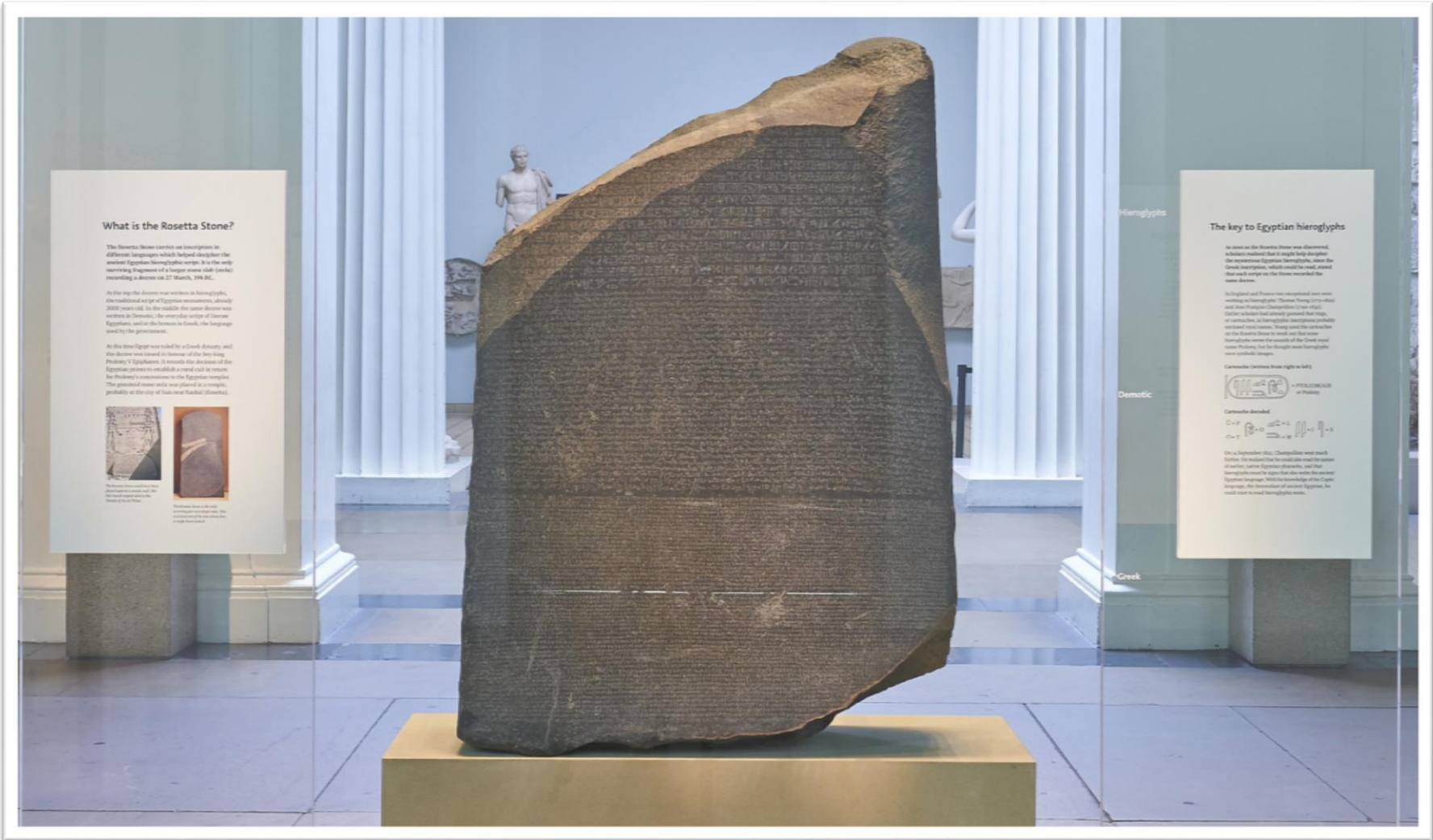
These working sessions were largely co-led by BITS, ABA, and the team of framework and standards experts at Boston Consulting Group-Platinion, led by Nadya Bartol.



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



The Rosetta Stone: The Inspiration for the Profile



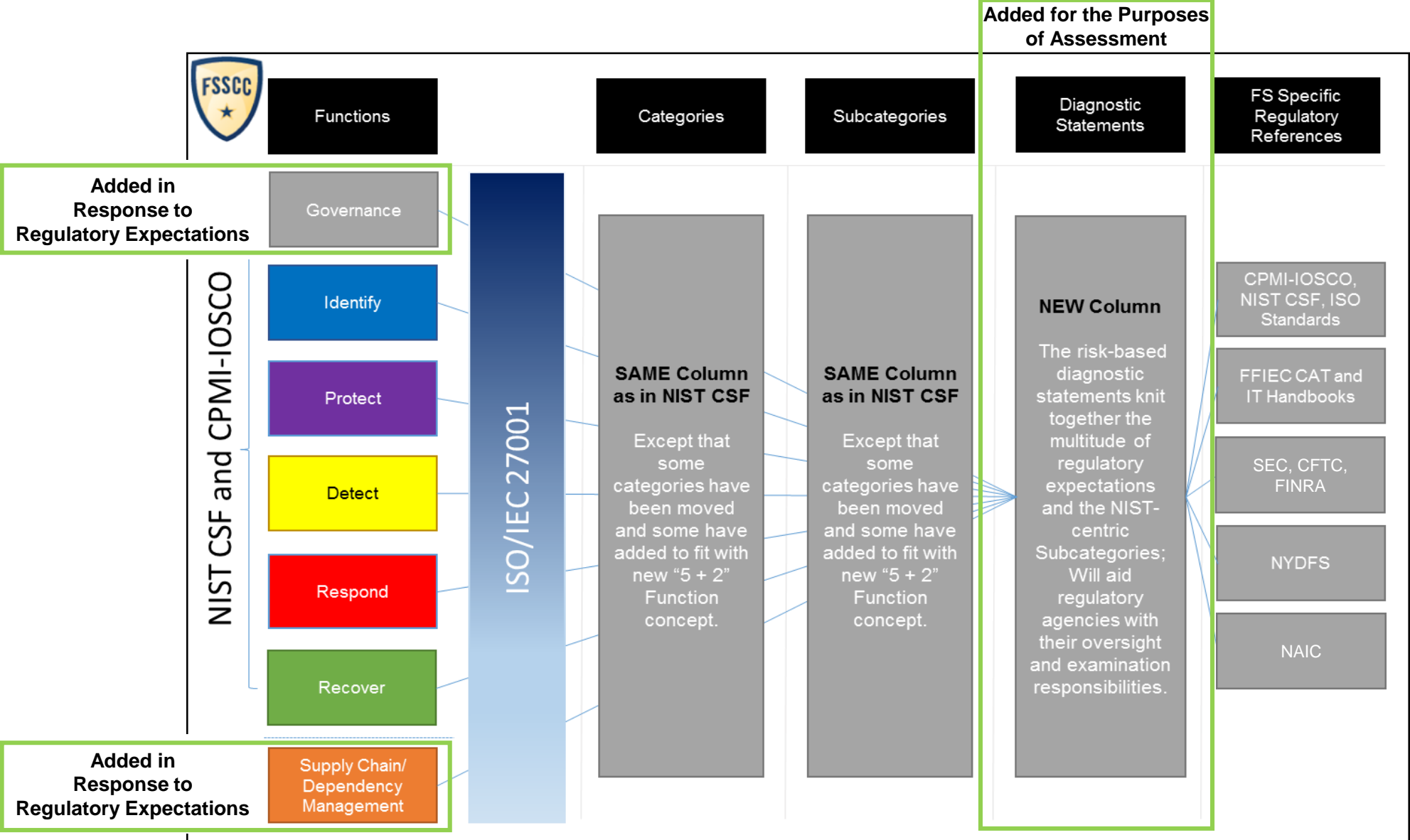
- 1) Part I: Impact Assessment (9 questions)
- 2) Part II: The Architecture, Diagnostic Statements, and Underlying Regulations

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

188 Diagnostics

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

Sector Only Impact – Tier 3

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

136 Diagnostics

- Examples: Community banks, small broker dealers/investment advisors.

Customer/3rd Party Impact Only – Tier 4

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

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



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.***

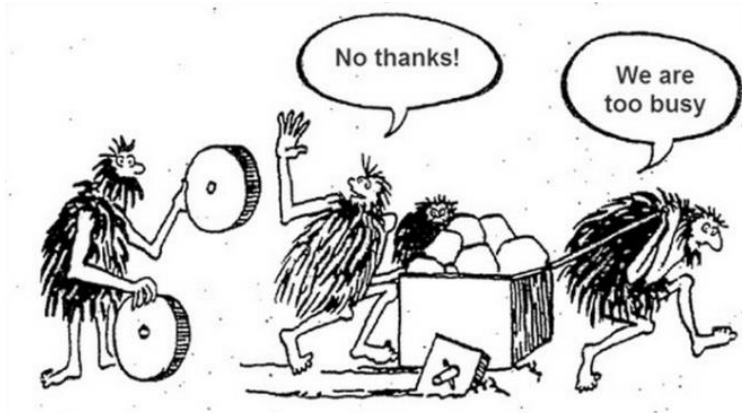


Documented Agency Statements of Support

- **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.”



A Sustained Organization with Four Areas of Focus: The Three Year Plan



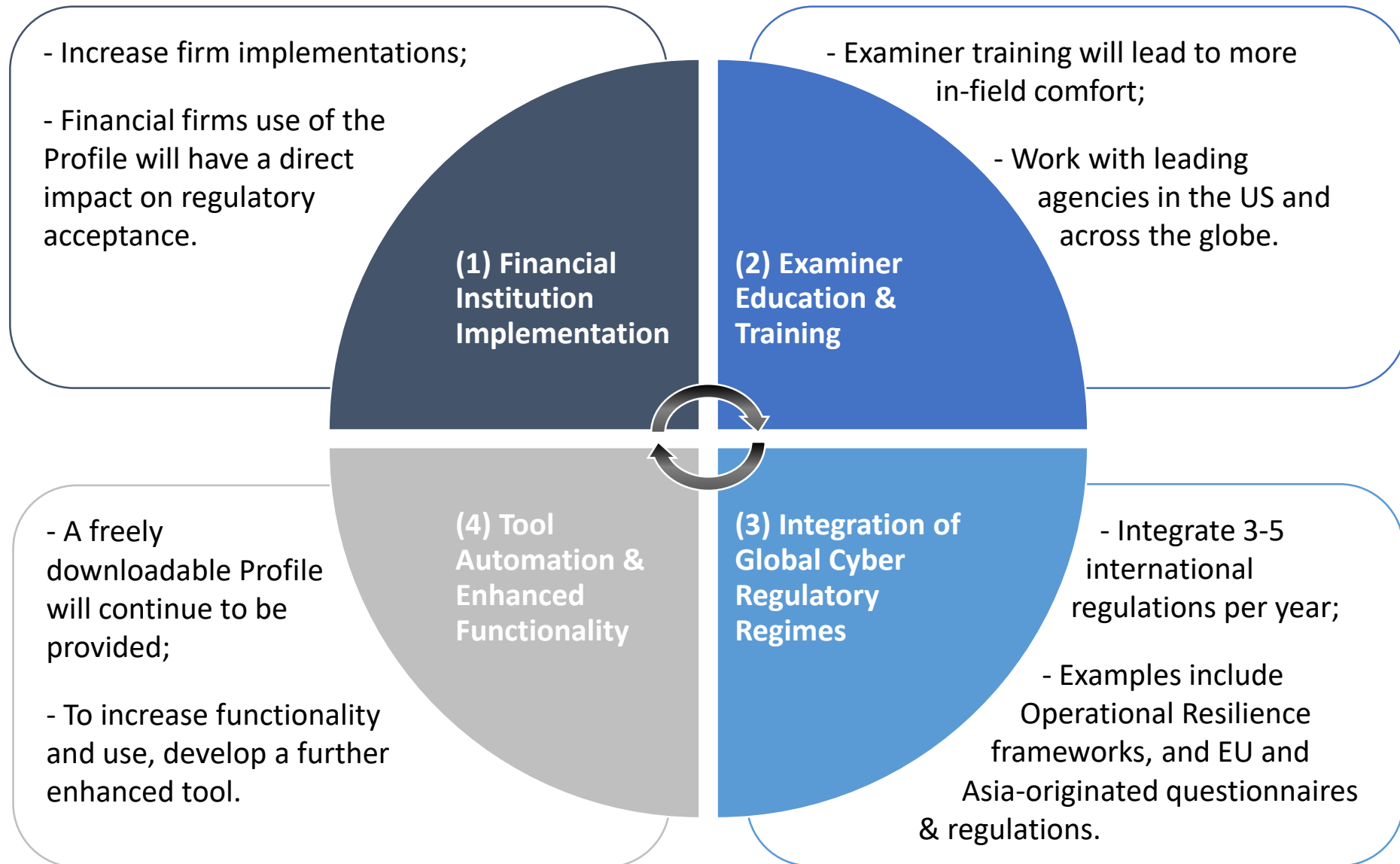
Profile Initiative

- ⑩ Produced a Version 1.0
- ⑩ Integrated 2300 cyber regulatory provisions and reduced them to 286 questions
- ⑩ Held numerous meetings with Regulators (including Principals) and a Cabinet level meeting to emphasize the benefits of the Profile and regulatory harmonization

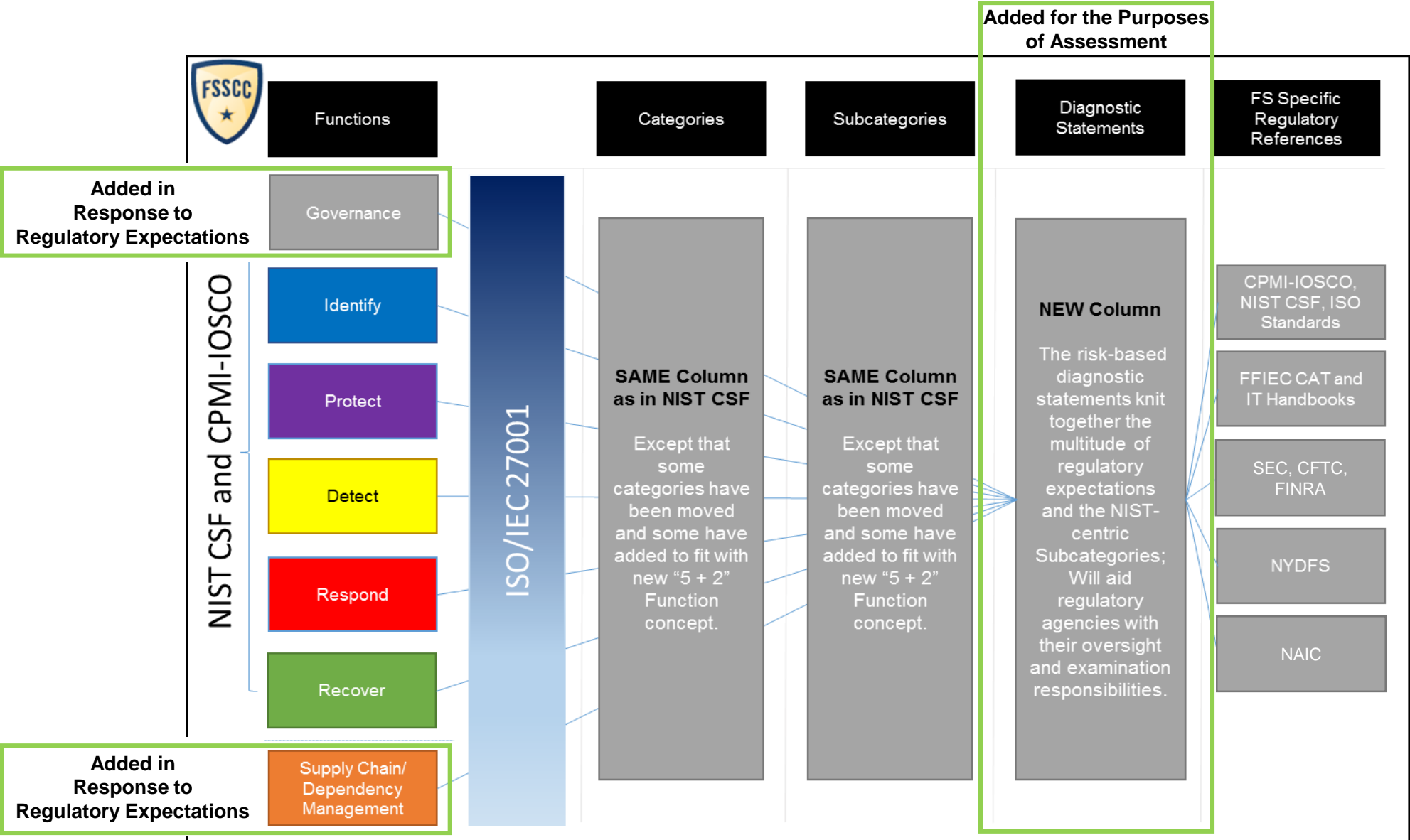
Dedicated Organization

- ⑩ Accelerate member firm implementation
- ⑩ Expand Regulatory Acceptance
 - ⑩ Within the US (federal and states)
 - ⑩ Globally (13 countries have interest)
 - ⑩ Create Examiner Education Materials
- ⑩ Reduce need for firms' own mappings: 10 priority mappings by 2022
- ⑩ Integrate Emerging Operational Resilience Requirements
- ⑩ Add Maturity Scoring Model
- ⑩ Automate Profile capabilities
- ⑩ Translate Profile into -
 - ⑩ Mandarin
 - ⑩ Japanese
 - ⑩ Spanish
 - ⑩ Portuguese
 - ⑩ French
 - ⑩ German

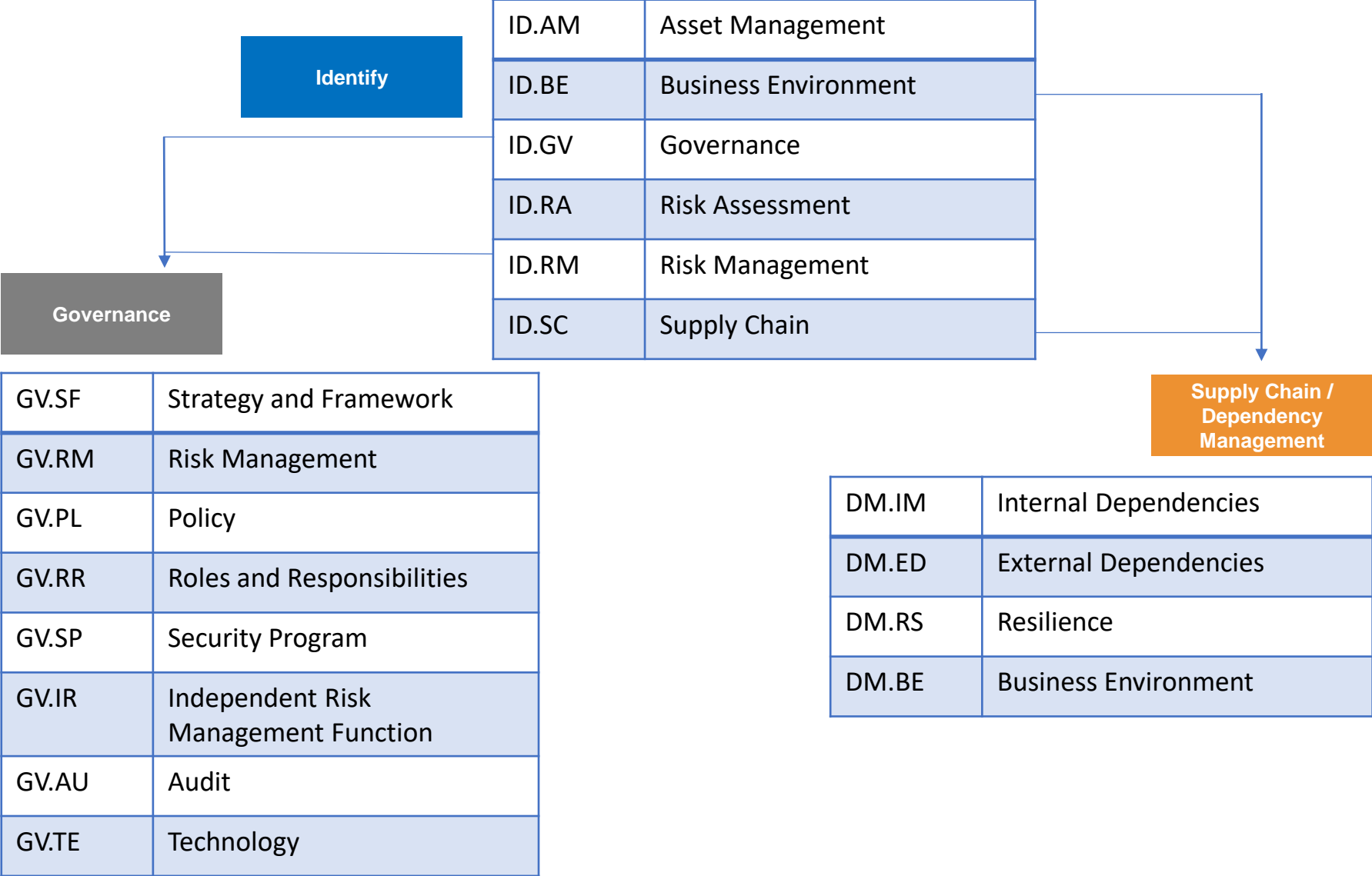
The Organization's Four Areas of Focus: The Three Year Plan



Appendix: Architecture, Diagnostic Statements, and Example Regulations



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



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. | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> Not Applicable <input type="checkbox"/> Yes – Risk Based <input type="checkbox"/> Yes – Compensating Controls <input type="checkbox"/> Not Tested <input type="checkbox"/> 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 | <ul style="list-style-type: none"> 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. | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> Not Applicable <input type="checkbox"/> Yes – Risk Based <input type="checkbox"/> Yes – Compensating Controls <input type="checkbox"/> Not Tested <input type="checkbox"/> 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. | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> Not Applicable <input type="checkbox"/> Yes – Risk Based <input type="checkbox"/> Yes – Compensating Controls <input type="checkbox"/> Not Tested <input type="checkbox"/> 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.

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.

277 Diagnostics

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

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

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

262 Diagnostics

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 all: Proceed to **Criticality Level 2: Subnational Impact** and its questions.

If Yes to any: 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) OR 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

| | <i>To assess compliance with a requirement defined in multiple sources...</i> | <i>...each regulator asks for information in a different way...</i> | <i>...to which a financial institution provides a different response.</i> |
|---|---|---|---|
| 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 |
| 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 |
| 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 International 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 | <p>Functions:</p> <ol style="list-style-type: none"> 1. Identify, 2. Protect, 3. Detect, 4. Respond, 5. Recover | <p>Risk Management Categories:</p> <ol style="list-style-type: none"> 1. Governance, 2. Identification, 3. Protection, 4. Detection, 5. Response and Recovery <p>Overarching Components:</p> <ol style="list-style-type: none"> 1. Testing, 2. Situational Awareness, 3. Learning and Evolving | <p>27001: Defines a suite (menu) of activities for managing information risks</p> <p>27002: Code of good practices recommended to meet security control objectives</p> | <p>27 Articles:</p> <p>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</p> | <p>The elements include:</p> <ol style="list-style-type: none"> 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 | <p>Defines generic processes for the management of IT, with each process defined together with –</p> <ul style="list-style-type: none"> • 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”

Cybersecurity Profile 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.



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



Cybersecurity Profile 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.

