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

PLATINION
A COMPANY OF THE BOSTON CONSULTING GROUP

Financial Services Sector Specific Cybersecurity "Profile"

NIST Cybersecurity Workshop

May 17, 2017

Our Sector's Shared Goal

A Complex Regulatory and Cybersecurity Environment for Financial Services

Financial Services Sector Specific Cybersecurity "Profile"

The Way Forward: Collaboration and Next Steps

Our Sector's Shared Goal with the Financial Services Regulatory Community:

Advancing the safety, soundness, and resilience of the financial system by mitigating and protecting financial institutions and the financial sector from increasing cybersecurity risks.

Collective Action to Meet Our Shared Goal:

1) ***Established the Financial Services Information Sharing and Analysis Center (FS-ISAC)*** in 1999. Today, the FS-ISAC has ~7,000 members in 38 countries.

2) ***Fostered sector-wide cybersecurity collaboration through eight Joint Financial Associations Cybersecurity Summits***.

3) ***Created Sheltered Harbor*** to enhance resiliency and provide augmented protections for financial institutions' customer accounts and data.

4) ***Developed and convened 13 "Hamilton Series" cyber exercises*** in 2014-16 in collaboration with the various U.S. Government agencies.

5) ***Developed a DRAFT Financial Services Sector Specific Cybersecurity "Profile"*** in response to a complex regulatory and cybersecurity environment.

Our Sector's Shared Goal

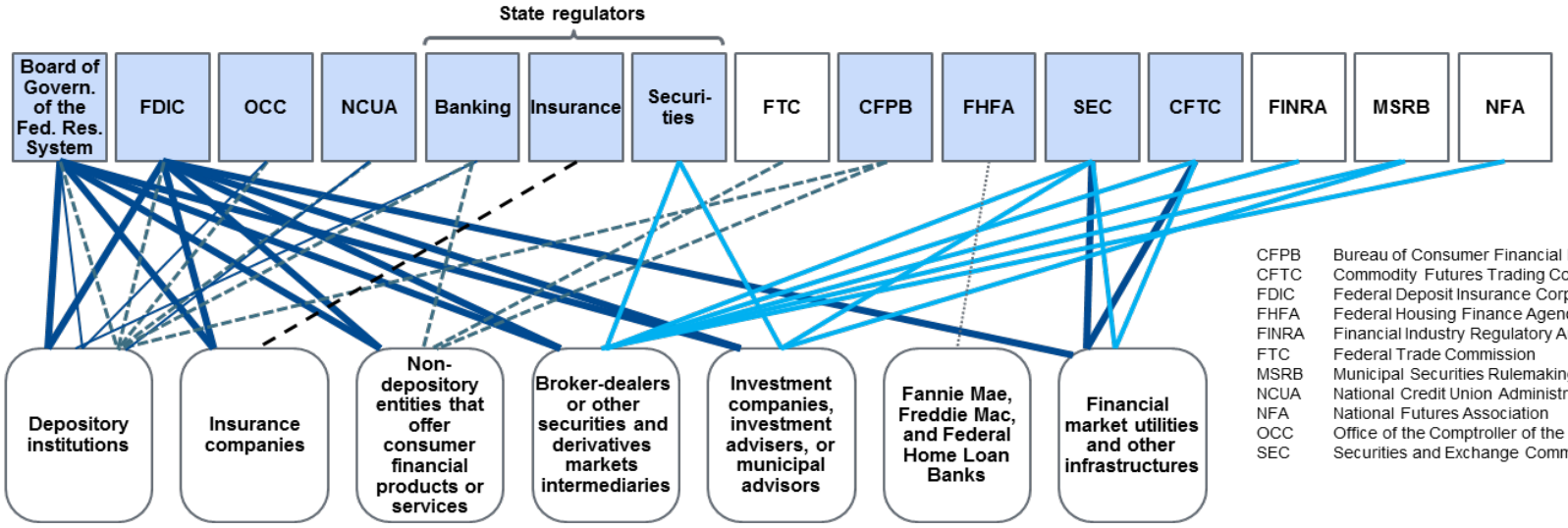
A Complex Regulatory and Cybersecurity Environment for Financial Services

Financial Services Sector Specific Cybersecurity "Profile"

The Way Forward: Collaboration and Next Steps

The U.S. Financial Services Regulatory Structure (2017)

Federal and State Financial Services Regulatory and Oversight Agencies and Self-Regulatory Organi-zations



CFPB	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FINRA	Financial Industry Regulatory Authority
FTC	Federal Trade Commission
MSRB	Municipal Securities Rulemaking Brand
NCUA	National Credit Union Administration
NFA	National Futures Association
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission

Additional Cyber Agencies

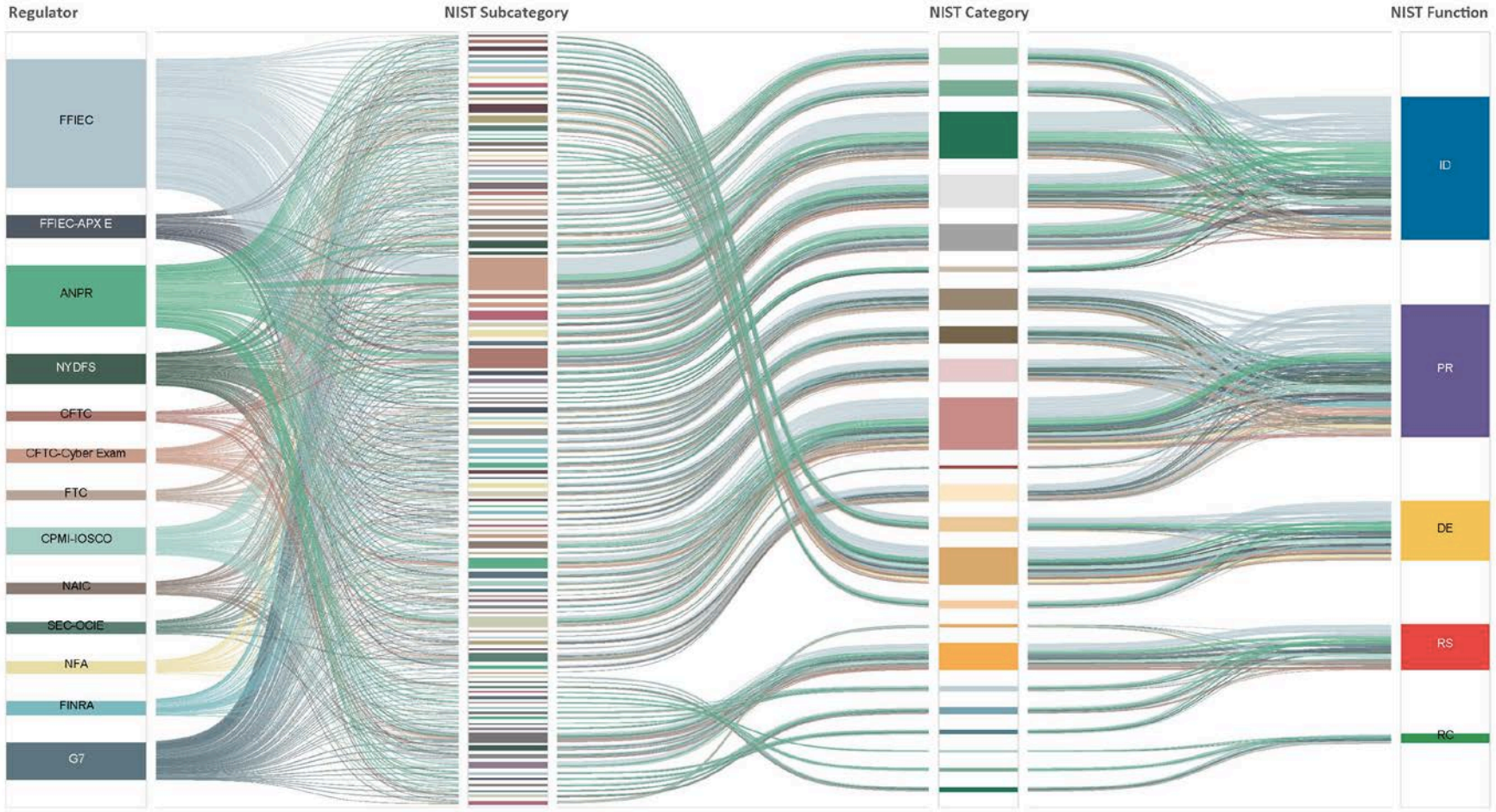
- White House (EOP, NSC/ NEC, OSTP)
- OMB
- U.S. Treasury (OFAC, FinCEN)
- DHS (ISAOs)
- Dept of Commerce (NIST, BIS)
- Federal Communications Commission
- Dept of State
- Law Enforcement Agencies (DOJ, USSS, FBI)

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

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

PLATINION
A COMPANY OF THE BOSTON CONSULTING GROUP

Many Financial Services Cyber-Related Proposals Describe Similar Concepts to the NIST Cybersecurity Framework (but with Different Terminology)



Why Language Matters

NIST's "Identify" function regarding "Risk Management Strategy" mapped to 9 different regulatory requirements.

NIST Functio	NIST Categor	NIST Subcategory
1 - IDENTIFY	Risk Management Strategy	Organizational risk tolerance is determined and clearly expressed

Regula	latory Engagemer	Domain	Requirement
G7	G7 Fundamental Elements Of Cybersecurity For	Element 1: Cybersecurity Strategy and	Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.
NYDFS	NYDFS Cybersecurity Requirements for	Section 500.09 Risk Assessment	(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of
FRB, OCC, FDIC	ANPR on Enhanced Cyber Risk Management	Category 1: Cyber Risk Governance	"The strategy would articulate how the entity intends to address its inherent cyber risk (that is, its cyber risk before mitigating controls or other factors are taken into consideration)";
FRB, OCC, FDIC	ANPR on Enhanced Cyber Risk Management Standards	Standards for Sector-Critical Systems of Covered Entities	"Board-supervised covered entities, at the holding company level, [must] measure (quantitatively) their ability to reduce the aggregate residual cyber risk of their sector-critical systems and their ability to reduce such risk to a minimal level Such measurement would take into account the risks associated with internal dependencies, external dependencies, and trusted connections with access to sector-critical systems"
FINRA	FINRA 2016 Regulatory and Examination Priorities	Cybersecurity Governance and Risk Management	(a) defining a governance framework to support decision making based on risk appetite;
CPMI-IOSCO	CPMI-IOSCO release guidance on cyber resilience	Governance	Board and senior management responsibilities. An FMI's board is ultimately responsible for setting the cyber resilience framework and ensuring that cyber risk is effectively managed. The Board should endorse the FMI's cyber resilience framework, and set the FMI's tolerance for cyber risk. The board should be regularly apprised of the FMI's cyber risk profile to ensure that it remains consistent with the FMI's risk tolerance as well as the FMI's overall business objectives. As part of this responsibility, the board should consider how material changes to the FMI's products, services, policies or practices, and the threat landscape affect its cyber risk profile. Senior management should closely oversee the FMI's implementation of its cyber resilience framework, and the
FFIEC	FFIEC Cybersecurity Assessment Tool	1: Cyber Risk Management &	The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.

The "Requirement" column, shows how each proposal modifies language and definitions, requiring firms to comply with largely the same but distinct requirements.

Meanwhile, with respect to the NIST Cybersecurity Framework …

✓ NIST Cybersecurity Framework (CSF) is -

- De facto standard for firms seeking guidance to counter cyber threats.[1]
- Meets the requirements to be flexible, repeatable, performance-based, and cost-effective.
- Adaptable to organization's maturity through implementation Tiers.

✓ According to an industry survey 91% of companies surveyed either use NIST CSF or ISO/IEC 27001/27002.[2]

✓ Federal entities and Sector-specific agencies (SSA) have promoted and supported the adoption of the NIST CSF in the critical infrastructure sectors.

- Department of Homeland Security (DHS) Critical Infrastructure Cyber Community (C3) Program
- SSAs for 5 sectors - Communications, Energy, Healthcare and Public Health, Transportation Systems, and Water and Wastewater Systems, developed NIST CSF implementation guidance.

✓ 7 other sectors (Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, Information Technology, and Nuclear Reactors, Materials, and Waste) have begun drafting implementation guidance in partnership with their SSAs.

1. U.S. Department of the Treasury, Office of Financial Research. "Financial Stability Report." 15 December 2015. https://financialresearch.gov/financial-stability-reports/files/OFR 2015-Financial-Stability-Report 12-15-2015.pdf
2. PwC. "Global State of Information Security Survey 2016." 9 October 2015: http://www.pwc.com/ gx/en/issues/cyber-security /information-security-survey.html
Source: US GAO, Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework (December 2015): http://www.gao.gov/products/GAO-16-152

Our Sector's Shared Goal

A Complex Regulatory and Cybersecurity Environment for Financial Services

Financial Services Sector Specific Cybersecurity "Profile"

The Way Forward: Collaboration and Next Steps

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

PLATINION
A COMPANY OF THE BOSTON CONSULTING GROUP

Sector is Working on a Detailed Profile Intended as Discussion Starting Point

Why the Profile

- Since NIST CSF release, the FS sector has had to respond to a multitude agency-issued cyber-related
- NIST CSF and ISO/IEC 27001 have emerged as de facto standards

Our Process

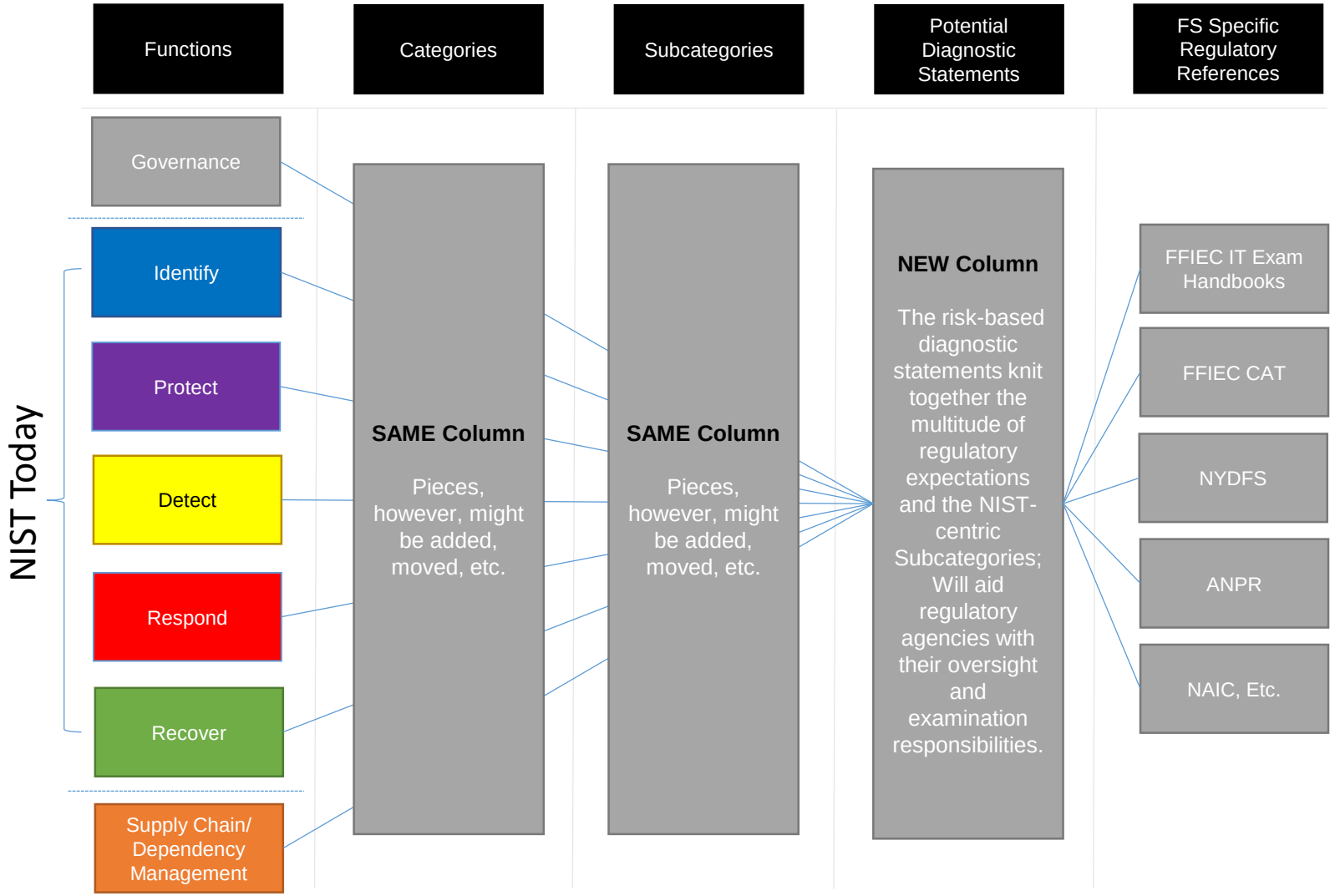
- Mapped most significant FS regulations to NIST CSF and ISO/IE 27001
- Validated mapping with FS industry stakeholder group
- Achieved consensus on the Profile structure
- Developed profile by summarizing regulatory statements
  - Common themes
  - Applicable to industry
  - Flexible to accommodate different size and type entities
- Solicited and received comments
- Adjudicated comments in a group setting with the members achieving consensus in the meeting (a la standards)
- Currently revising to address comments

The Profile provides us numerous benefits

Benefits of Profile Adoption

- Better capabilities in protecting our financial and economic platforms
- Enhanced collective understanding of the state of cybersecurity for regulators and industry
- Greater intra-sector, cross-sector and international cybersecurity collaboration and understanding
- Enhanced internal and external oversight and due diligence and Third Party Vendor management programs
- Improved Boardroom engagement
- Reduced cybersecurity administrative burdens and regulatory compliance complexity
- More efficient and effective resource allocation to address risks
- Greater innovation as technology companies, including FS startups

We are proposing to add two Functions of priority to the FS Sector



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.AU	Assurance and Audit

Supply Chain / Dependency Management

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

The Governance Function provides greater level of detail and granularity

Governance

GV.SF	Strategy and Framework
GV.RM	Risk Management
GV.PL	Policy
GV.RR	Roles and Responsibilities
GV.SP	Security Program
GV.AU	Assurance and Audit

- Establishing appropriate cybersecurity governance in an FS organization
- Implementing robust risk management practices
- Maintaining a comprehensive cybersecurity policy
- Designating appropriate senior individuals and giving them the resources and access they need
- Putting together and running a comprehensive cybersecurity program
- Giving appropriate attention to segregation of duties between security implementation, oversight, and audit

The Supply Chain/Dependency Management Function helps manage many dependencies in the FS Sector

Supply Chain / Dependency Management

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

- Managing risks from internal dependencies
- Managing risks from external dependencies – business partners, suppliers, contractors, consultants, customers, etc…..
- Assuring resilience of the enterprise, financial services sector, and entire critical infrastructure
- Establishing and maintaining robust business environment

Our Sector's Shared Goal

A Complex Regulatory and Cybersecurity Environment for Financial Services

Financial Services Sector Specific Cybersecurity "Profile"

The Way Forward: Collaboration and Next Steps

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

PLATINION
A COMPANY OF THE BOSTON CONSULTING GROUP

Making this all work

Collaboration is Essential

- To achieve success, we have to collaborate with the regulators
- The Profile is a starting point for discussions with the regulators and self-regulatory bodies
- This will set the stage for international collaboration

Profile Development Next Steps

- Complete initial drafting process for the Profile
- Collaborate with the regulators on Draft Profile to meet expectations & needs
- Together, develop a risk-tiering and maturity model that could
  - Work seamlessly with the Profile
  - Fulfill expectations for institutions of all sizes & complexity

- ***If you are a representative of a financial institution and want to participate, please contact Josh Magri, VP and Counsel, Financial Services Roundtable/BITS at Josh.Magri@FSRoundtable.org***

Appendix – Detailed Profile Examples

Functions	Categories	Subcategories	NIST CSF v1.1 Ref	Potential Diagnostic Statements / FS Profile	Potential Diagnostic Statement Reponses	FS References	(NIST) Informative References
Governance (Partial)	**Policy (GV.PL):** The organization established cybersecurity policy in support of its cyber risk management framework. Technology	**GV.PL-1:** Organizational cybersecurity policy is established and has been approved by appropriate governance bodies.	ID.GV-1	GV.PL-1.1: The organization maintains a documented cybersecurity policy or policies approved by appropriate Senior Officer or an appropriate governing authority.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No	ANPR/1/Considerations, NYDFS/500.03, NFA, SAMA, FRBNY/I/ II/ III, FFIEC/1	• COBIT 5 APO01.03, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6 • ISO/IEC 27001:2013 A.5.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all families
				GV.PL-1.2: The organization's cybersecurity policy integrates with appropriate employee accountability policy to ensure that all personnel are held accountable for complying with cybersecurity policies and procedures.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
		GV.PL-2: Organizational cybersecurity policy addresses appropriate controls, identified through risk assessment.	None	GV.PL-2.1: The cybersecurity policy is based on the organization's risk management program, legal and regulatory requirements, and other applicable factors.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No	FFIEC/1, FFIEC-APX E, NYDFS/500.08 /500.09, NFA	TBD
				GV.PL-2.2: Cybersecurity processes and procedures are established based on the cybersecurity policy.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
				GV.PL-2.3: Cybersecurity policy is reviewed and revised by a responsible cybersecurity manager (e.g., CISO) and organization to address changes in the inherent risk profile, based on a periodic risk assessment, as well as to address other changes, e.g., new technologies, products, services, interdependencies, and evolving threat environment.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		

Functions	Categories	Subcategories	NIST CSF v1.1 Ref	Potential Diagnostic Statements / FS Profile	Potential Diagnostic Statement Reponses	FS References	(NIST) Informative References
Detect (Partial)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events.	DE.CM-2	DE.CM-2.1: The organization's controls include monitoring and detection of anomalous activities and potential cybersecurity events across organization's physical environment and infrastructure, including unauthorized physical access to high-risk or confidential systems.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No	CPMI-IOSCO/Protection, CPMI-IOSCO/Detection, FFIEC/3, FINRA/Technical Controls, ANPR/2, ANPR/5, FTC/5, G7/ 4, NAIC/4, NFA	• ISA 62443-2-1:2009 4.3.3.3.8 • NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3 through DE.CM-7 not included for presentation purposes					
		DE.CM-8: Vulnerability scans are performed.	DE.CM-8	DE.CM-8.1: The organization conducts periodic vulnerability scanning, including automated scanning across all environments to: (1) identify potential system vulnerabilities, including publicly known vulnerabilities, upgrade opportunities and new defense layers; (2) identify vulnerabilities before deployment/redeployment of new/existing devices.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No	CFTC/E, CFTC-Cyber Exam/E, CPMI-IOSCO/Detection, CPMI-IOSCO/Testing, FFIEC/3, FFIEC-APX E/Risk Mitigation, FINRA/Technical Controls, ANPR/2, FTC/7, G7/ 4, NYDFS/500.05, SEC-OCIE/1	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5
				DE.CM-8.2: The organization conducts, either by itself or by independent third-party, periodic penetration testing and red team testing on organization's network, internet-facing applications or systems, critical applications, to identify gaps in cybersecurity defenses.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
				DE.CM-8.3: The organization establishes a process to prioritize and remedy issues identified through vulnerability scanning.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		

Functions	Categories	Subcategories	NIST CSF v1.1 Ref	Potential Diagnostic Statements / FS Profile	Potential Diagnostic Statement Reponses	FS References	(NIST) Informative References
Supply Chain/Dependency Management (Partial)	**Resilience (DM.RS):** The organization is resilient and able to operate while experiencing a cyber under attack.	**DM.RS-3:** Organizational incident response, business continuity, and disaster recovery plans and exercises incorporate its external dependencies and critical business partners.	Similar to ID.SC-5	DM.RS-3.1: The organization has incorporated its external dependencies and critical business partners into its cyber resilience (e.g. incident response, business continuity, and disaster recovery) strategy, plans, and exercises.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No	ANPR/4, ANPR/5, NAIC-5, FFIEC/1	• CIS CSC: 19.7, 20.3 • COBIT 5: DSS04.04 • ISA 62443-2-1:2009: 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013: SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
				DM.RS-3.2: The organization's cyber resilience strategy addresses the organization's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
				DM.RS-3.3: The organization designs and tests its cyber resilience plans, and exercises to support financial sector's sector-wide resilience and address external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
				DM.RS-3.4: The organization periodically identifies and tests alternative solutions in case an external partner fails to perform as expected.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		
				DM.RS-3.5: The organization prioritizes incident response of systems critical to the enterprise and to the financial services sector.	❑ Not Applicable ❑ Yes ❑ Yes – Risk Based Approach ❑ Yes – Compensating ❑ Partial – Ongoing Project ❑ Not Tested ❑ No		