FSSCC Cybersecurity Profile:
A NIST-based Cybersecurity Assessment Approach

- Community Banks -

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

Speakers Page: Introductions and Biographies

Denyette DePierro
Vice President & Senior Counsel
American Bankers Association

ddepierr@aba.com
202.663.5333

www.aba.com/cyberprofile

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.DR 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.

Joyce Flinn, VP Information Security & Disaster Recovery Officer, has 29 yrs of banking experience, having worked in Loan Operations, Finance, Risk Management, and IT. She was appointed Information Security Officer in 2001. Joyce also acted as the Privacy Officer and Security Officer at various times. She assumed the responsibilities of Disaster Recovery in 2017.

She currently chairs the company's Cybersecurity committee and implemented the Cybersecurity program, which included the NIST CSF and FFIEC CAT frameworks. Joyce participated in the validation and development of the FSSCC Cybersecurity Profile.

Joyce Flinn

Vice President
Information Security &
Disaster Recovery Officer
First United Bank & Trust

Agenda

1.What is the FSSCC Cybersecurity Profile?

2.Community Bank Use Case

- Joyce Flinn, First United Bank and Trust

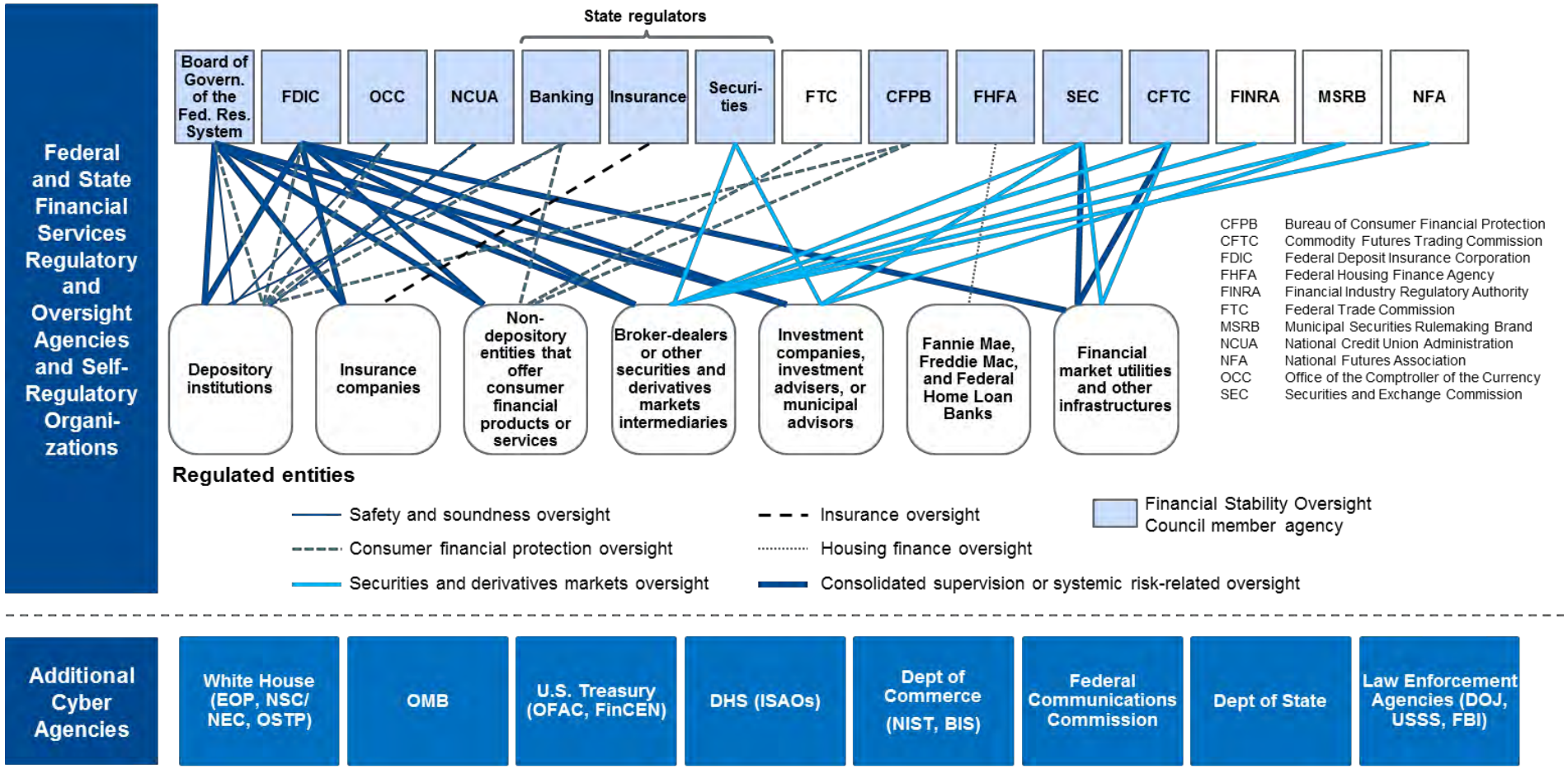
3. Topics:

- Why did First United Bank and Trust decide to use the Profile?
- What has been their implementation process and timeline?

- The Problem -

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

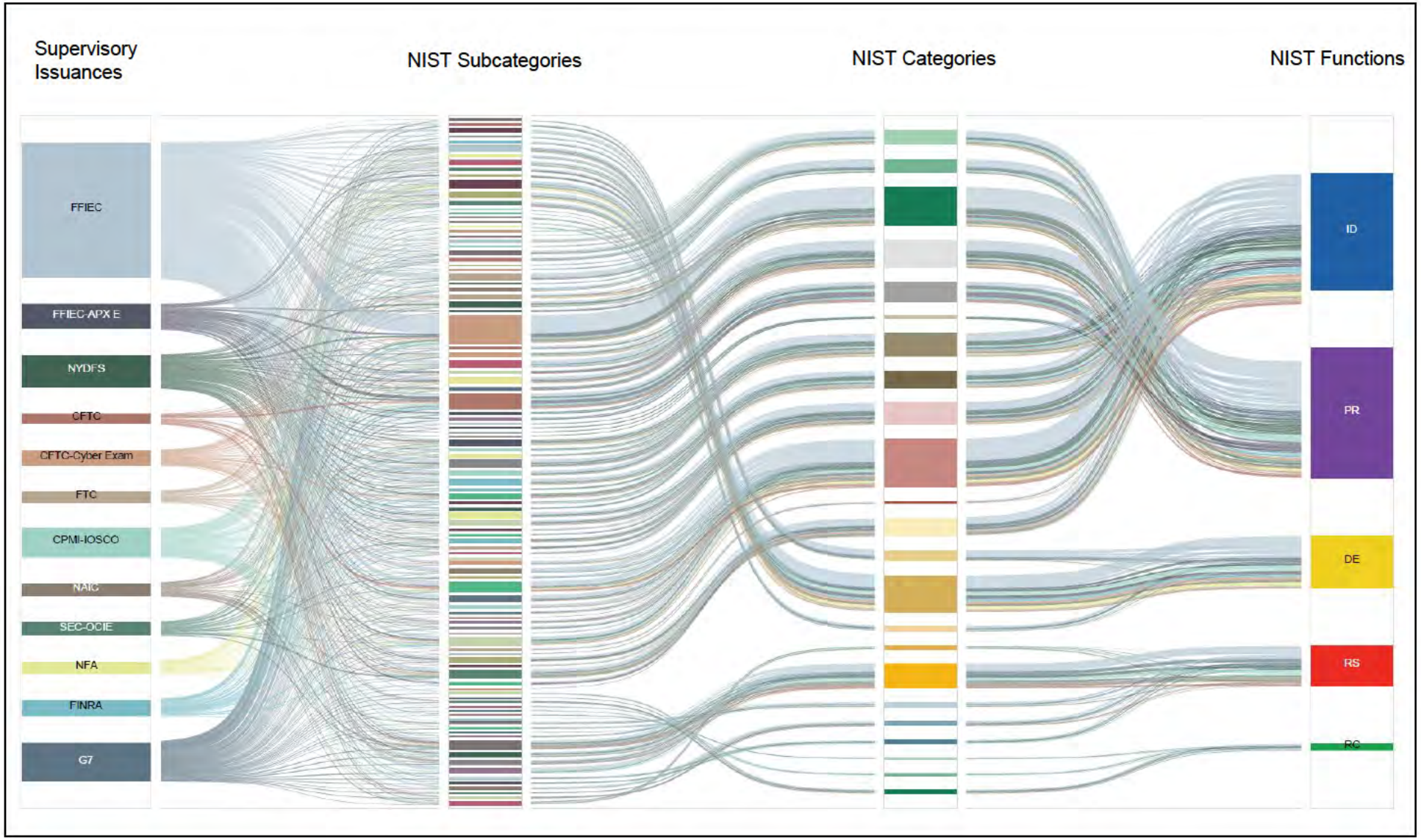
The U.S. Financial Services Regulatory Structure (2019)



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

Duplication, Compliance Burden, and Limited Cyber Resources

- 2016 Survey: **40%** of Information Security teams' time on avg spent on reconciliation of cyber expectations
- (ISC)2: Gap of cyber pros has been growing, with a **gap of 3 million projected for 2019**
- FSB (2018): **72% of jurisdictions** reported plans to issue new cyber requirements



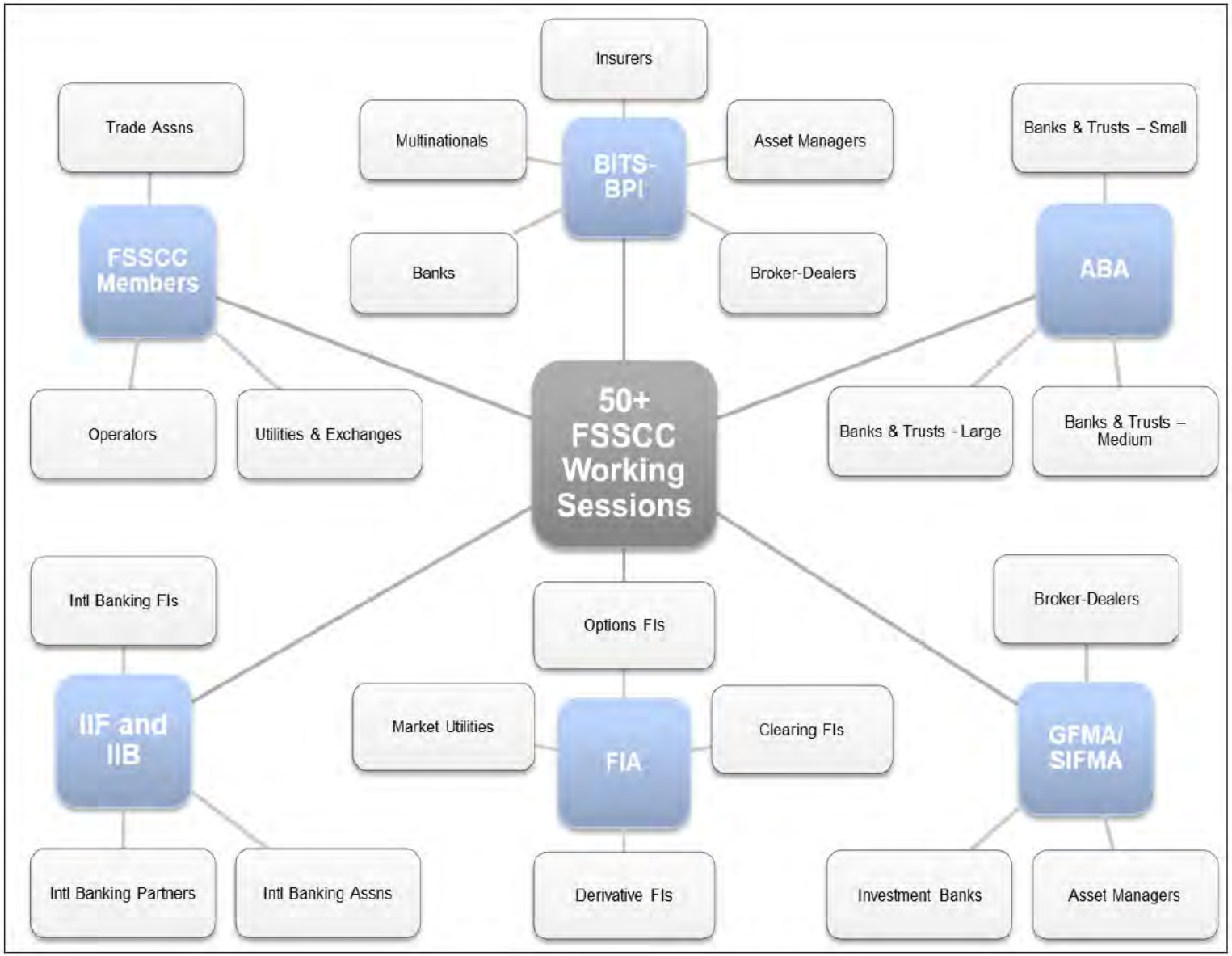
The Process for Development and Primary Participants

Over the past 2 years –

- Coalition under the FSSCC established;
- ABA and BPI/BITS co-lead;
- ***50+ working sessions;***
- ***300+ experts participating;***
- ***150+ financial institutions of all sizes and charter types providing input.***

Financial Services and Other Agencies –

- *Provided material for incorporation*, notably:
  - FRB;
  - OCC;
  - FDIC;
  - SEC;
  - CFTC;
  - FINRA;
- Facilitated a NIST workshop on risk/impact scaling (April 2018).



Immediate Benefits and Efficiencies

- ***More than 2300 regulatory provisions reduced to 9 tiering questions and 277 Diagnostic Statement questions, a reduction of approximately 88% overall.***

- ***73% Reduction for Community Institution Assessment Questions.*** For the least complex and interconnected institutions, it is expected that they would answer a total of 145 questions (9 tiering questions + 136 Diagnostic Statement questions).
- ***49% Reduction in Assessment Questions for the Largest Institutions.*** For the most complex and interconnected institutions, the reduction also is significant. With the Profile, it is expected that such institutions would answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions).

...and the Agencies?

Agency Statements of Support

- **FFIEC:** "…These resources are actionable and help financial institutions manage cybersecurity risk regardless of whether they use the FFIEC Cybersecurity Assessment Tool, NIST Cybersecurity Framework, Financial Services Sector Specific Cybersecurity Profile, or any other methodology to assess their cybersecurity preparedness."

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

- **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."

The Profile as a Tool for Public/Private Collaboration

Globally

- ✓ **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.

The Structure:

1) An Impact Risk Assessment (Part I)

2) Cyber Framework + Supervisory Materials = Architecture (Part II)

Download Free Profile and Users Guide:

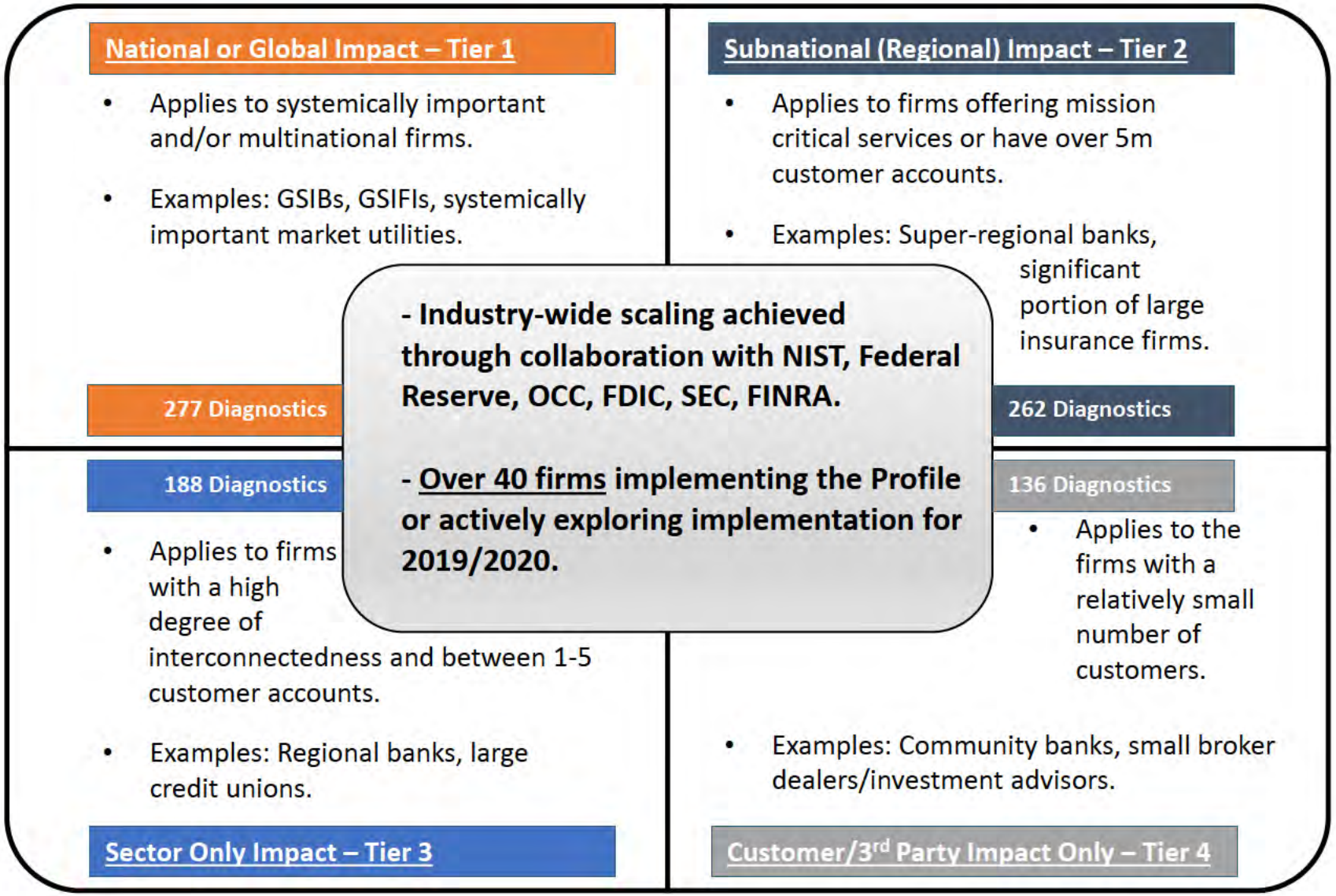
- https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
- https://www.fsscc.org/The-Profile-FAQs

PART I:

The Impact Assessment

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

Public/Private Collaboration to Achieve Sector-Wide Scaling by Impact

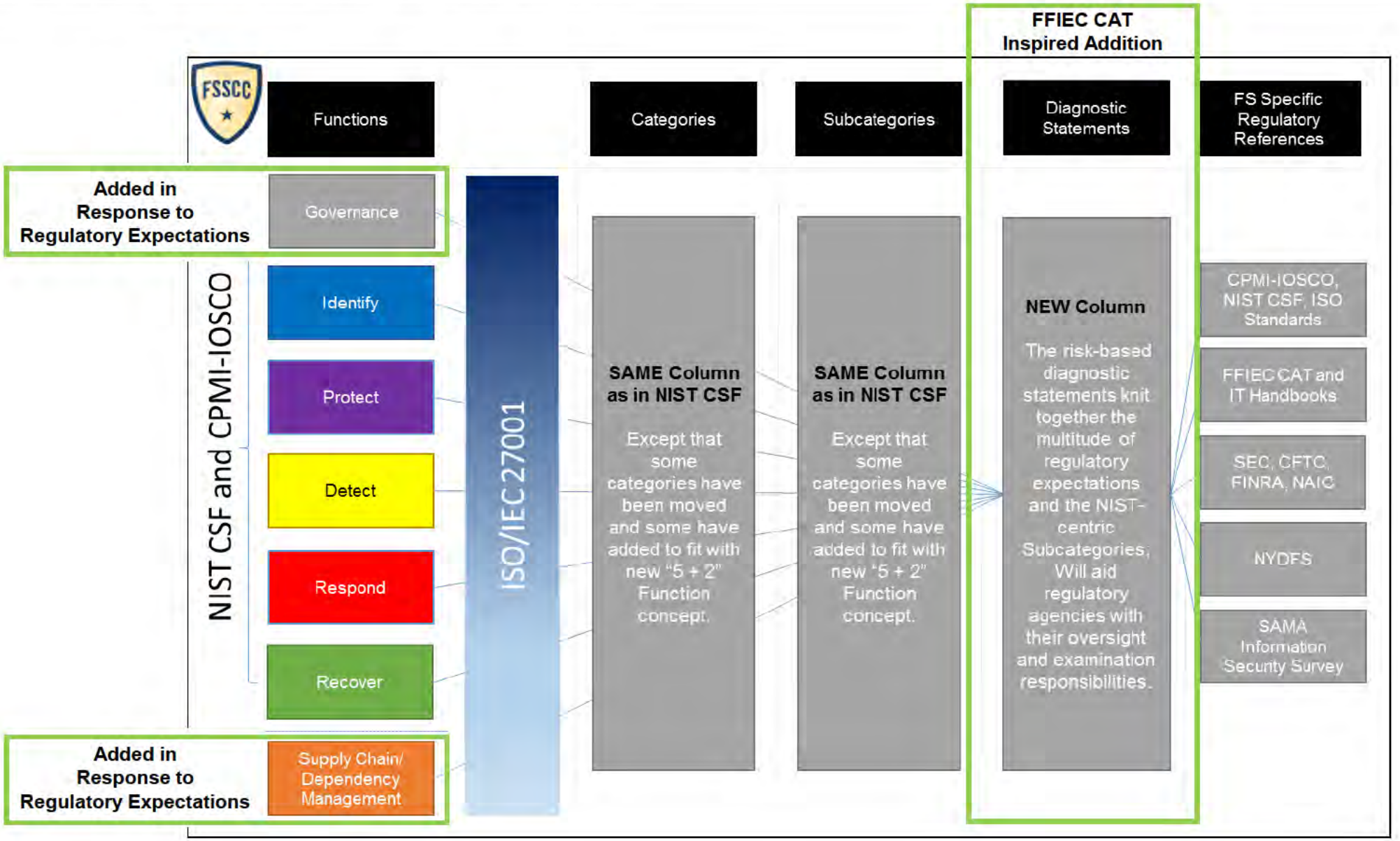


PART II:

The Architecture

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

The Profile's Underlying Architecture



Example: Tiering and Diagnostic Statements

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 international 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
Governance	**Strategy and Framework (GV.SF):** The organization has a cyber risk management framework that is reviewed and approved by the Board and is informed by the organization's risk tolerances and its role in critical infrastructure.	**GV.SF-1:** Organization has a cyber risk management strategy and framework.	ID.BE-3; ID.RM-1 - with sector enhancement	GV.SF-1.3: The organization's cyber risk management strategy identifies and documents the organization's role as it relates to other critical infrastructures outside of the financial services sector and the risk that the organization may pose to them.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Information Security/I, FFIEC IT Booklet/Management/I.B, FFIEC IT Booklet/Operations	• COBIT 5 APO02.06, APO03.01 • ISO/IEC 27001:2013 Clause 4.1 • NIST SP 800-53 Rev. 4 PM-8
				GV.SF-1.4: The cyber risk management strategy identifies and communicates the organization's role within the financial services sector as a component of critical infrastructure in the financial services industry.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Management/I.A, FFIEC IT Booklet/Operations	
				GV.SF-1.5: The cyber risk management strategy and framework establishes and communicates priorities for organizational mission, objectives, and activities.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Information Security/I, FFIEC IT Booklet/Management/I, FFIEC IT Booklet/Operations	

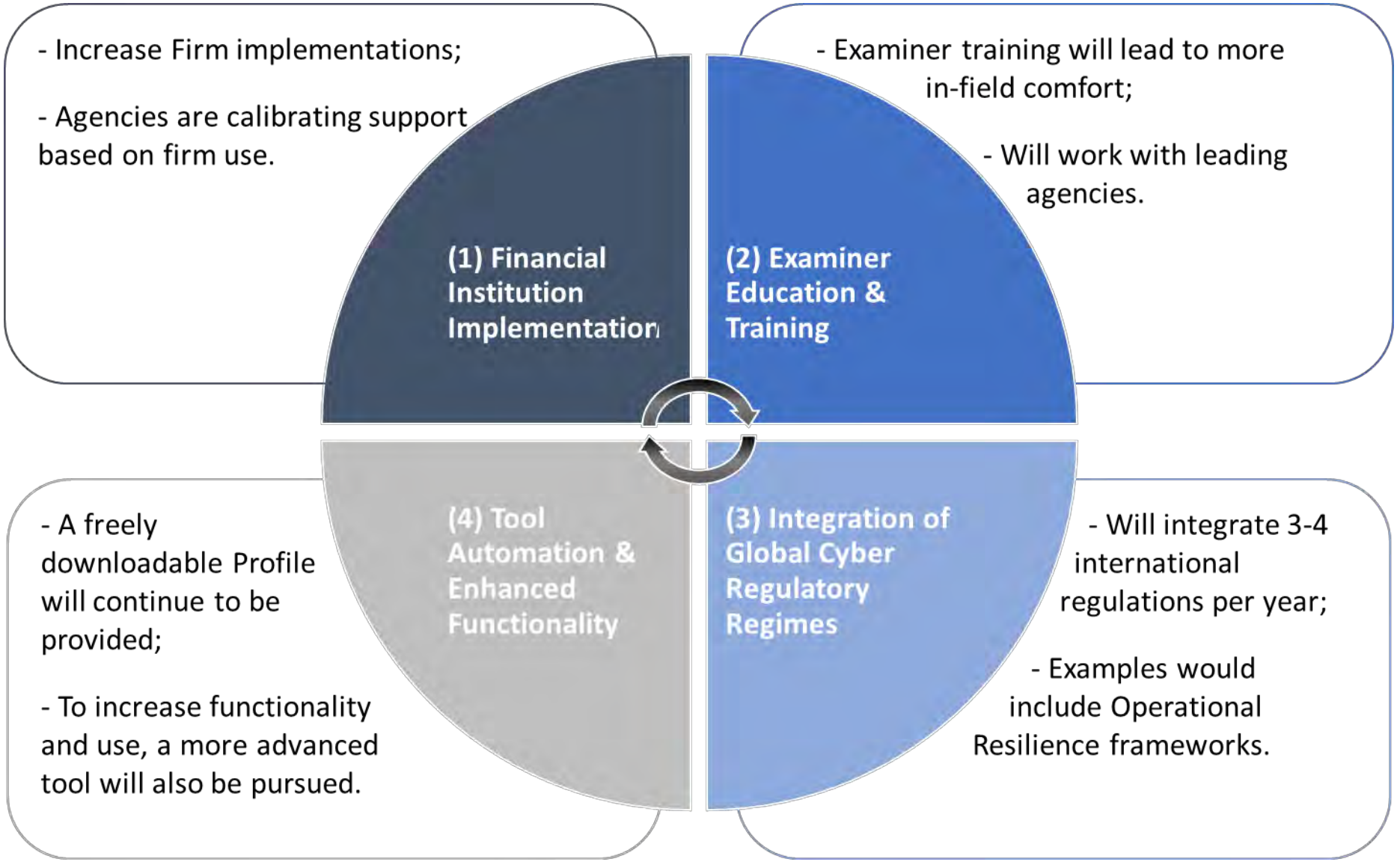
The '**Diagnostic Statements**' column defines authoritative, common language for multiple regulatory requirements, enabling Firms to comply with largely the same but distinct requirements from different supervisors

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

Looking Ahead

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

The Three Year Plan



Joyce Flinn
Vice President, Information Security & Disaster Recovery Officer
First United Bank & Trust

- Community Bank Use Case -

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

First United: About Us

- Community Bank Holding Company
- $1.4 billion in assets
- 25 offices in 2 states
- Headquartered in Garrett County, Maryland
- Retail bank offers full retail banking, full digital banking, including mobile, commercial and consumer products, and Trust/Investments division

To Enrich the Lives of Our Employees, Our Customers/Communities and Our Shareholders Through Uncommon Service and Effective Financial Solutions

First United: Regulatory Oversight

- Federal Deposit Insurance Corporation (FDIC)
- Federal Reserve
- Maryland State Agency

Normally, the FDIC completes the annual IT examinations, even if the State of Maryland is the lead agency for Safety and Soundness. This is the first year that Maryland is completing its own IT examination.

First United: Timeline of Events

2014

- Implement NIST Cybersecurity Framework
- Bank establishes Cybersecurity Committee: CSI-MyBank ----

CSI-MyBank Mission: Safeguard critical data through comprehensive identification, analysis, communication, and mitigation of risk by striving for information security excellence and business-focused outcomes.

The pillars of success are to:

- Protect what matters most;
- Change behavior; and
- ...ilities

Members of the Committee include:

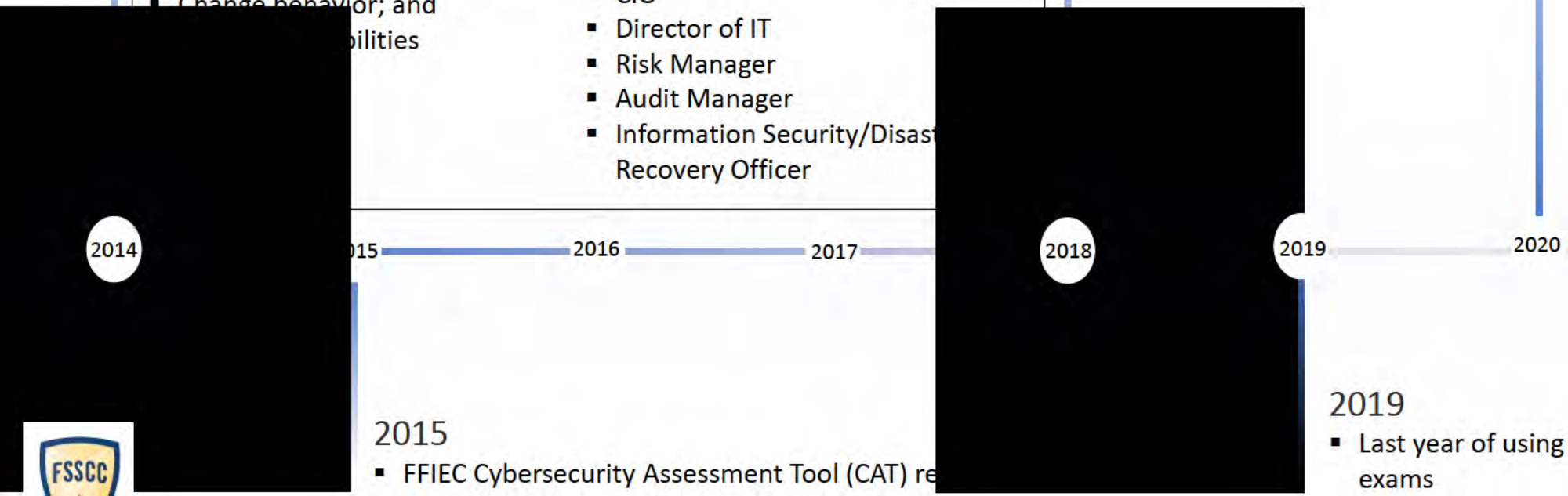
- COO
- CIO
- Director of IT
- Risk Manager
- Audit Manager
- Information Security/Disast... Recovery Officer

2018

- First United joins FSSCC cybersecurity working group
- Volunteers as community bank beta tester of FSSCC Cybersecurity Profile
- Runs NIST CSF, CAT, and DRAFT/Beta Profile concurrently

2020

- Full transition to the Profile



2015

- FFIEC Cybersecurity Assessment Tool (CAT) re...
- Committee decides to complete CAT and maintain NIST CSF

2019

- Last year of using CAT and Profile together for exams
- Bank Board will only be briefed using the Profile

First United: NIST CSF and FFIEC CAT Use and Framework Challenges

NIST Cybersecurity Framework (2014 Release)

Process

- Committee reviewed all items in framework.
  Extensive time commitment
- Identified controls to meet framework requirements.
- Identified gaps.
- Prioritized and began implementing controls.
- Implemented the NIST CSF in our ERM solution.

Challenges

- Doesn't address **Governance or Supply Chain** to the level we would like.
- No method to determine **'maturity' and levels of compliance**.
- Not geared to financial institutions, **supervisory expectations, or regulations**.

FFIEC Cybersecurity Assessment Tool (2015 Publication)

FFIEC
The FFIEC Cybersecurity Assessment Tool

Process

- Highly recommended by agencies.
- Decided to complete CAT and maintain NIST CSF.
- Completed CAT review in 2015, identified gaps.
- Identified controls in ERM to address control requirements.

Challenges

- **Delivery Channels = Highest CAT risk.**
  Most financial institutions with any online presence would identify this as a Significant risk.
- **Region/State presence considered.**
  Geography does not indicate higher risk, rather depends on concentration within market area.
- **Scrutiny of Cloud providers.**
  Most vendors are moving to cloud solutions.
- **Intermediate Level compliance out of reach** for many community banks.

FSSCC

First United: Transition to the FSSCC Cybersecurity Profile

Prior Process Frustrations → **Profile Implementation Initiated** → **Setting the Stage for Transition**

General Frustrations Using the NIST CSF and FFIEC CAT

- Maintaining two different profiles/assessments.
- **Gaps in risk profile not addressed.**
- Presenting two differing methods of assessment to the Board of Directors.
- **Lack of consistency across third parties and for third party review.**

2018 Profile Implementation Exploration

- Relied on Cybersecurity Committee.
- Completed tiering and first run through Level 4 items in 2 hours.
- Identified items that are partially completed, and one "I don't know."

Thoughts Upon Initial Completion

- Really liked the selection options
- Surprised to find items not addressed in CAT Evolving

2019 Profile Implementation Evolution

- Using FFIEC CAT and FSSCC Cybersecurity Profile in parallel for 2019 Examination cycle.
  - IT Exam completed by State this year.
  - *Engage FDIC Examiners in conversations concerning implementation.*
  - Determine use of Profile going forward.
- Develop Profile in ERM system to link audit workpapers and findings.
- **Board presentation in 2019 will only include the Profile and CAT.**
  - Demonstrate differences between assessments.
  - Attain approval to maintain one assessment going forward.

First United: Implementation Guide and Session Takeaways

Implementation Guide

1) Communicate

- Identify internal and external stakeholders
- Provide information on the Profile (*e.g., Benefits, Mappings, etc.*)
- Build expectations and momentum

2) Plan

- Identify or create group to implement
- Include Subject Matter Experts
- Involve Risk and Audit staff
- Establish time frames

3) Implement

- Complete Impact Assessment/Tiering
- Complete FSSCC Profile
- Establish action plans with due dates to remediate gaps

4) Maintain

- Assure gaps are addressed
- Reporting to Board, and Executive Management
- Establish Audit requirements
- Review at least annually

Session Takeaways

1) **Define the use case, current frustrations, and benefits for your organization.**

2) **Socialize and Communicate**.
   Internal and external stakeholders

3) **Stay focused on the positive**.
   Goals. Objectives. Benefits.

4) **Develop the implementation plan and timeline.**

5) **Execute and Maintain.**

An Executive Summary: Issue, Solution, Benefits, and Support

The Issue: Domestic and international regulatory agencies asking the same question in many different ways, stretching already scarce cybersecurity talent.

The Profile as a Solution: The Profile, which is a common, standardized approach that can act as a baseline for examination and future cyber regulation - **fill out once per exam cycle, report out many.**

Voluntary with Many Benefits, Including:

- Provides more consistent and efficient processing of examination material by both firms and regulators.
- Allows Regulators and Firms to focus on systemic risk and risk residual to firms.
- Establishes an Industry best practice beyond regulatory use.

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

Supporting Associations:

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

Benefits of the Profile Approach

Financial Institutions

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

Supervisory Community

- ✓ ***Examinations more tailored to institutional complexity, enabling "deeper dives"*** in those areas of greater interest to that particular agency.
- ✓ ***Enables supervisory agencies to better discern the sector's systemic risk***, with more agency time for specialization, 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 evidence security*** against the standardized set of compliance requirements.

The Profile: A NIST Cybersecurity Framework Extension to Align Financial Services Requirements and Supervisory Expectations

NIST Cybersecurity Framework provides a globally accepted organizational structure and taxonomy for cybersecurity and cyber risk management

The following countries are either exploring its use or promoting it through translation –

- Bermuda
- Brazil
- Canada
- Israel
- Italy
- Japan
- Malaysia
- Mexico
- Philippines
- Saudi Arabia
- Switzerland
- United Kingdom
- Uruguay

The Profile extends the NIST Cybersecurity Framework to be more inclusive of financial services requirements and supervisory expectations

Extended NIST to highlight 2 special categories of particular (& appropriate) regulatory focus:

Governance

Supply Chain/ Dependency Management

The following international governments and organizations have expressed positive interest in the Profile –

- Argentina
- Brazil
- China (Mainland and Hong Kong)
- Chile
- European Union
- International Standards Organisation
- Japan
- Singapore
- United Kingdom

A Customization for Financial Services: Focus on Governance and 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

Governance - Mapping Leads to New Categories

The Governance Function provides greater level of detail and granularity, as is found in financial services regulatory guidance

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

- Establishing appropriate cybersecurity governance in an FS organization, including for new technology design and usage
- 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 role and responsibilities of an independent risk management function

Supply Chain/Dependency Management: Mapping Reveals Maturity of FS Regulatory Focus

The Supply Chain/Dependency Management Function was developed because of the financial services regulatory community's greater focus on firm and sector dependencies

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