FSSCC Cybersecurity Profile:

- Midsize Banks-

FSSCC

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.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.

Barth is a seasoned Information Technology and Cyber Security Professional. With over 35 years of experience he has seen the information technology industry evolve from the original IBM PC and has been involved with cyber security from the very first viruses and exploits to impact PC's and the Internet. With broad and deep expertise in the technology and cyber security fields, Barth has been in a variety of roles including technology consulting for a global firm, data and voice infrastructure architect, network operations, telecommunications, and cyber security operations. Barth has been with Fulton Financial Corporation since 2000 and is currently the Chief Information Security Officer, a role he has occupied since January of 2014.

Barth Bailey
SVP, Chief Information Security Officer
Fulton Financial Corp

Agenda

1.What is the FSSCC Cybersecurity Profile?

2.Use Case:

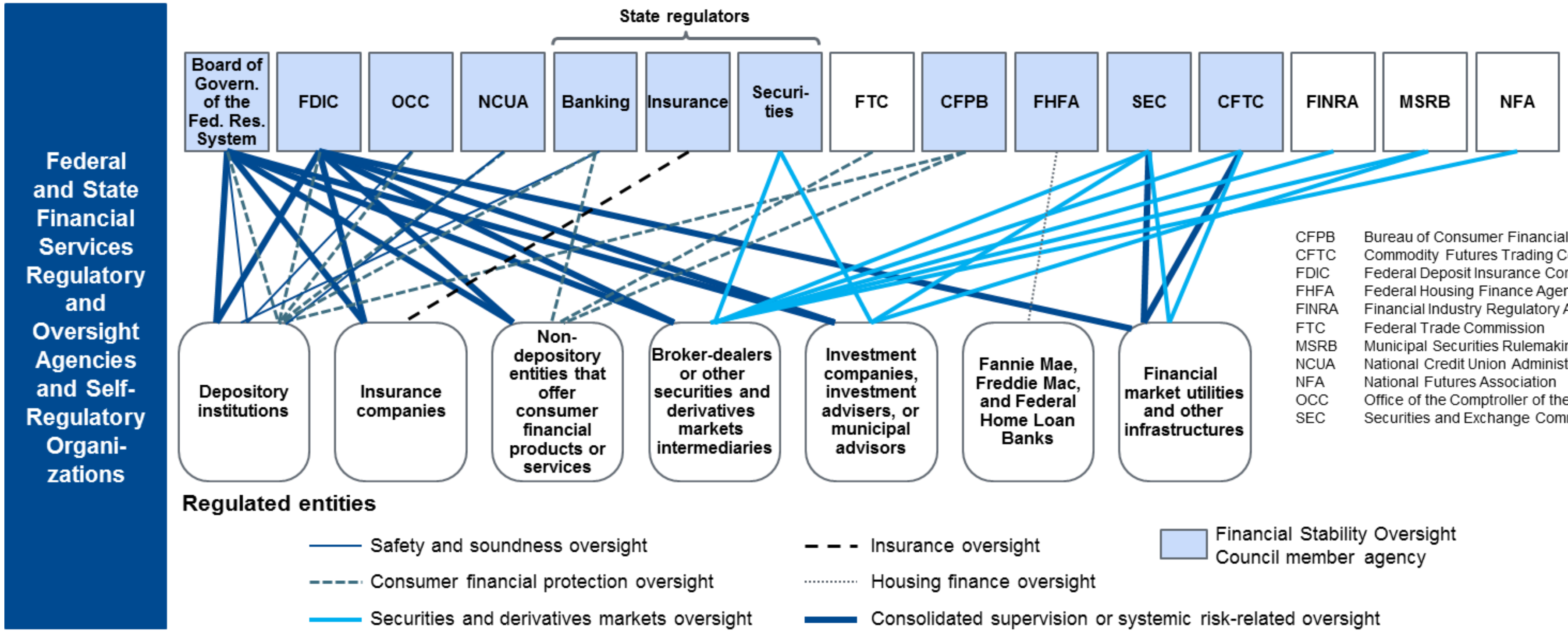
- Barth Bailey, CISO, Fulton Financial

3. Topics:

- Why did Fulton decide to use the Profile?
- What has been their implementation process and timeline?

- The Challenge -

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



Federal and State Financial Services Regulatory and Oversight Agencies and Self-Regulatory Organizations

State regulators

Board of Govern. of the Fed. Res. System | FDIC | OCC | NCUA | Banking | Insurance | Securities | FTC | CFPB | FHFA | SEC | CFTC | FINRA | MSRB | NFA

Regulated entities

Depository institutions | Insurance companies | Non-depository entities that offer consumer financial products or services | Broker-dealers or other securities and derivatives markets intermediaries | Investment companies, investment advisers, or municipal advisors | Fannie Mae, Freddie Mac, and Federal Home Loan Banks | Financial market utilities and other infrastructures

- Safety and soundness oversight
- Consumer financial protection oversight
- Securities and derivatives markets oversight
- Insurance oversight
- Housing finance oversight
- Consolidated supervision or systemic risk-related oversight
- ▭ Financial Stability Oversight Council member agency

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

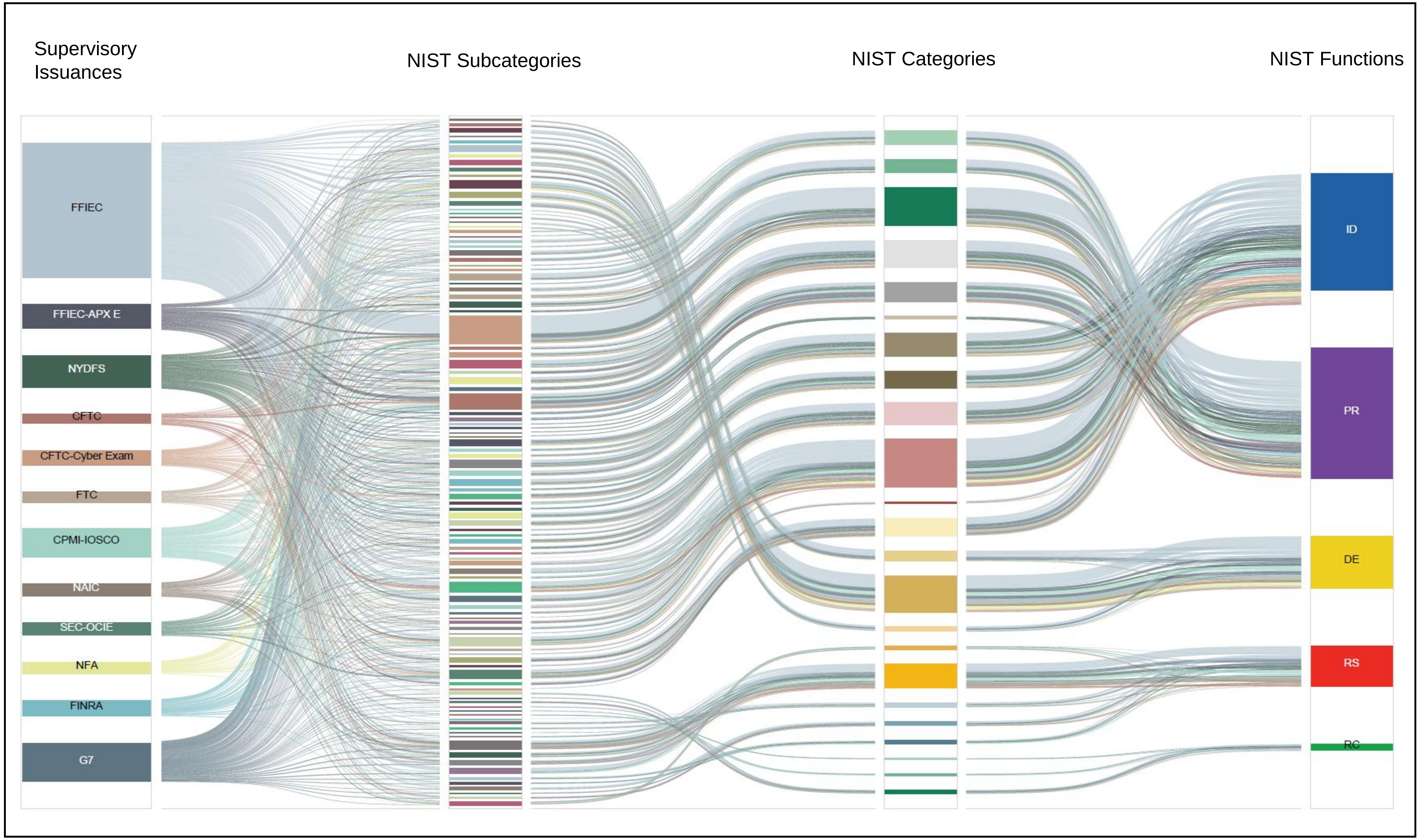
Source: GAO; GAO-16-175

Compliance Burden: Overlap and Redundancy

- 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



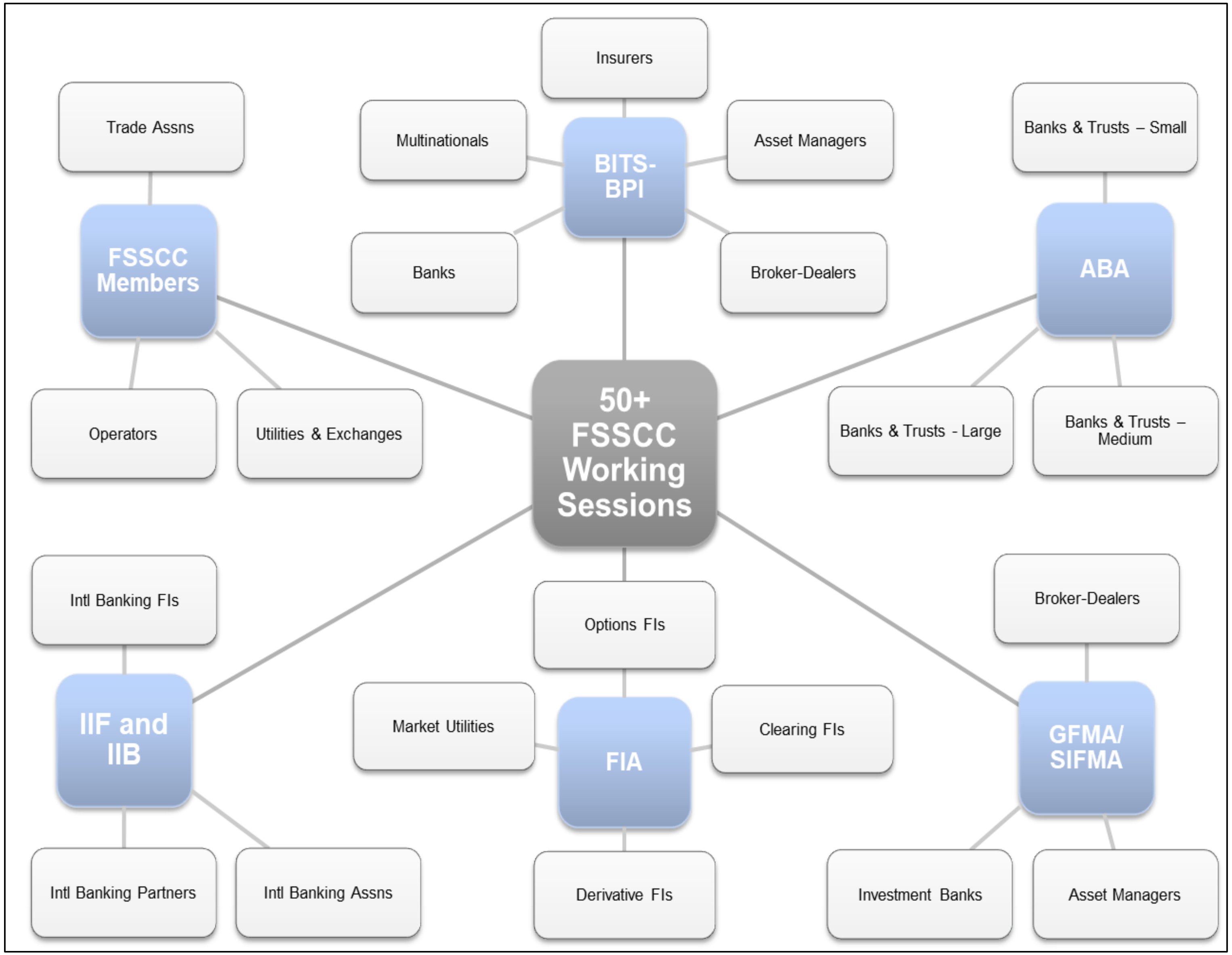
The Process, Development, and Participants

Over the past 2 years –

- Coalition under the FSSCC established;
- BITS and ABA co-lead;
- ***50+ working sessions;***
- ***300+ individual experts participated;***
- ***150+ financial institutions of all types provided 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.



Benefits and Efficiencies

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

- ***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). As compared to another widely-used assessment tool's 533 questions, this represents a ***73% reduction.***

- ***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) as compared to the other widely-used assessment's 533, ***a 49% reduction.***

…and the Agencies?

Documented 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.

FSSCC

FSSCC Cybersecurity Profile Component Parts

1) **Part I: Impact Risk Assessment**

2) **Part II: Supervisory Architecture**

Download the FREE FSSCC Cyber Profile:

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

PART I:
The Impact Assessment

Part 1: Impact Assessment's Risk Tiers

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 have over 5m customer accounts.
- Examples: Super-regional banks, significant portion of large insurance firms.

262 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

136 Diagnostics

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

Customer/3rd Party Impact Only – Tier 4

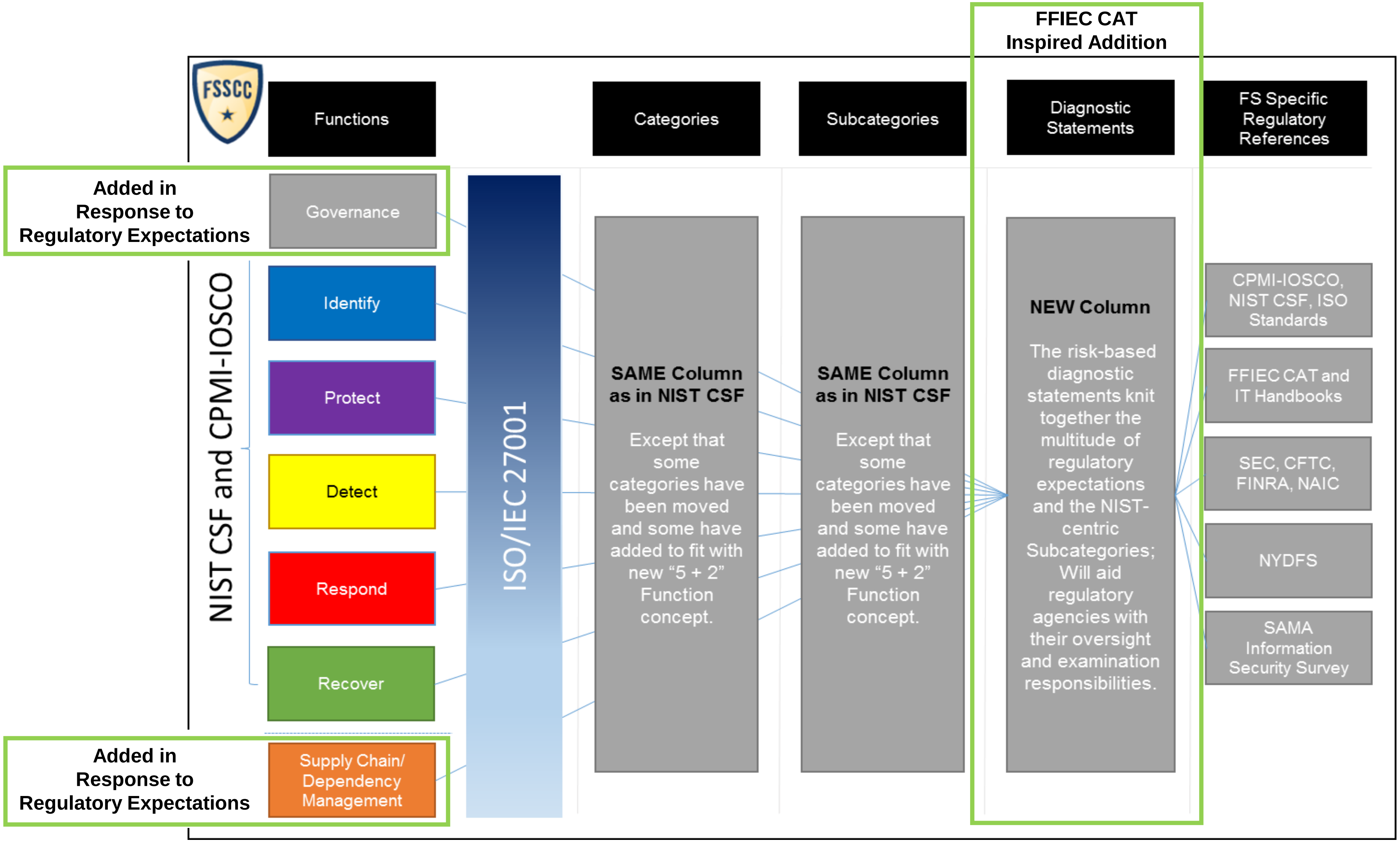
- Industry-wide scaling achieved through collaboration with NIST, Federal Reserve, OCC, FDIC, SEC, FINRA.

- Over 40 firms implementing the Profile or actively exploring implementation for 2019/2020.

PART II:

The Architecture

The Profile's Architecture



FFIEC CAT Inspired Addition

Functions

Categories

Subcategories

Diagnostic Statements

FS Specific Regulatory References

Added in Response to Regulatory Expectations

Governance

NIST CSF and CPMI-IOSCO

Identify

Protect

Detect

Respond

Recover

Added in Response to Regulatory Expectations

Supply Chain/ Dependency Management

ISO/IEC 27001

SAME Column as in NIST CSF

Except that some categories have been moved and some have added to fit with new "5 + 2" Function concept.

SAME Column as in NIST CSF

Except that some categories have been moved and some have added to fit with new "5 + 2" Function concept.

NEW Column

The risk-based diagnostic statements knit together the multitude of regulatory expectations and the NIST-centric Subcategories; Will aid regulatory agencies with their oversight and examination responsibilities.

CPMI-IOSCO, NIST CSF, ISO Standards

FFIEC CAT and IT Handbooks

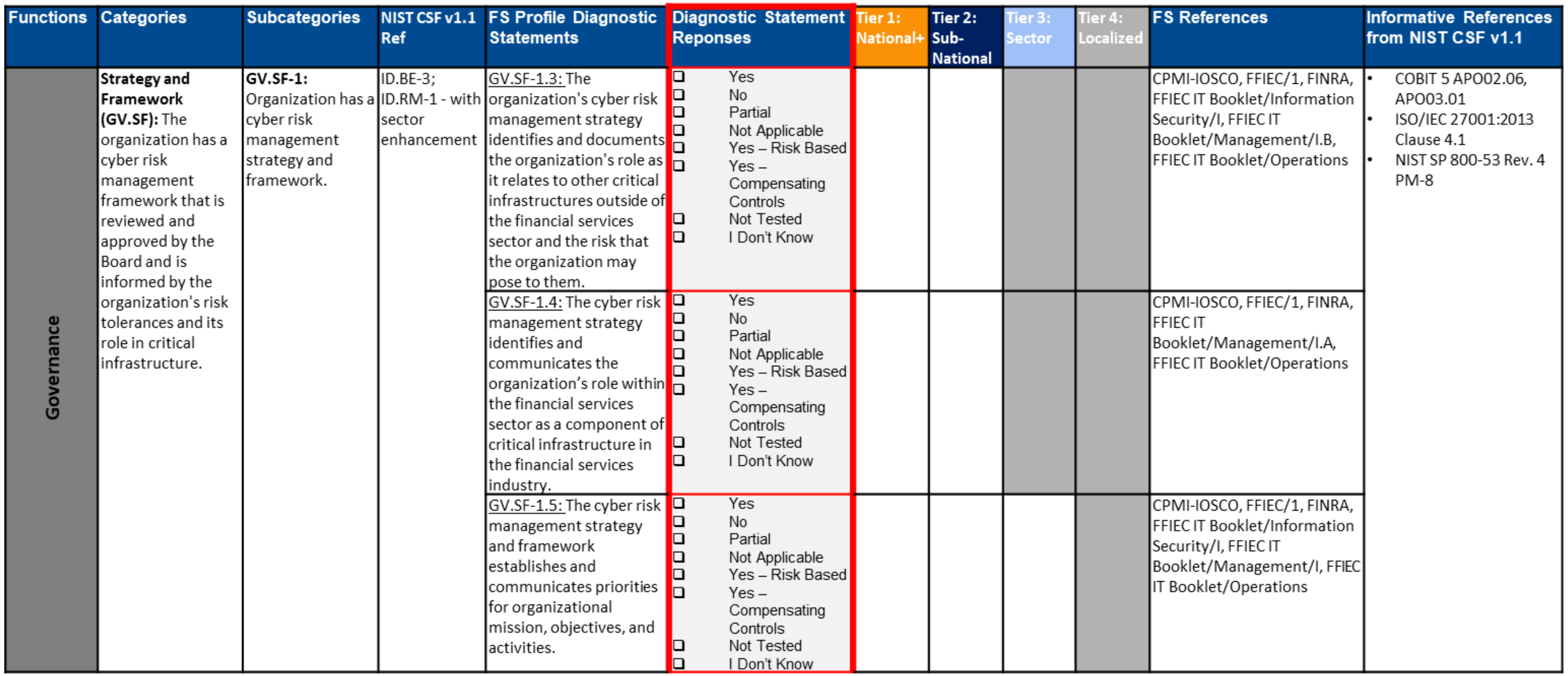
SEC, CFTC, FINRA, NAIC

NYDFS

SAMA Information Security Survey

The 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.



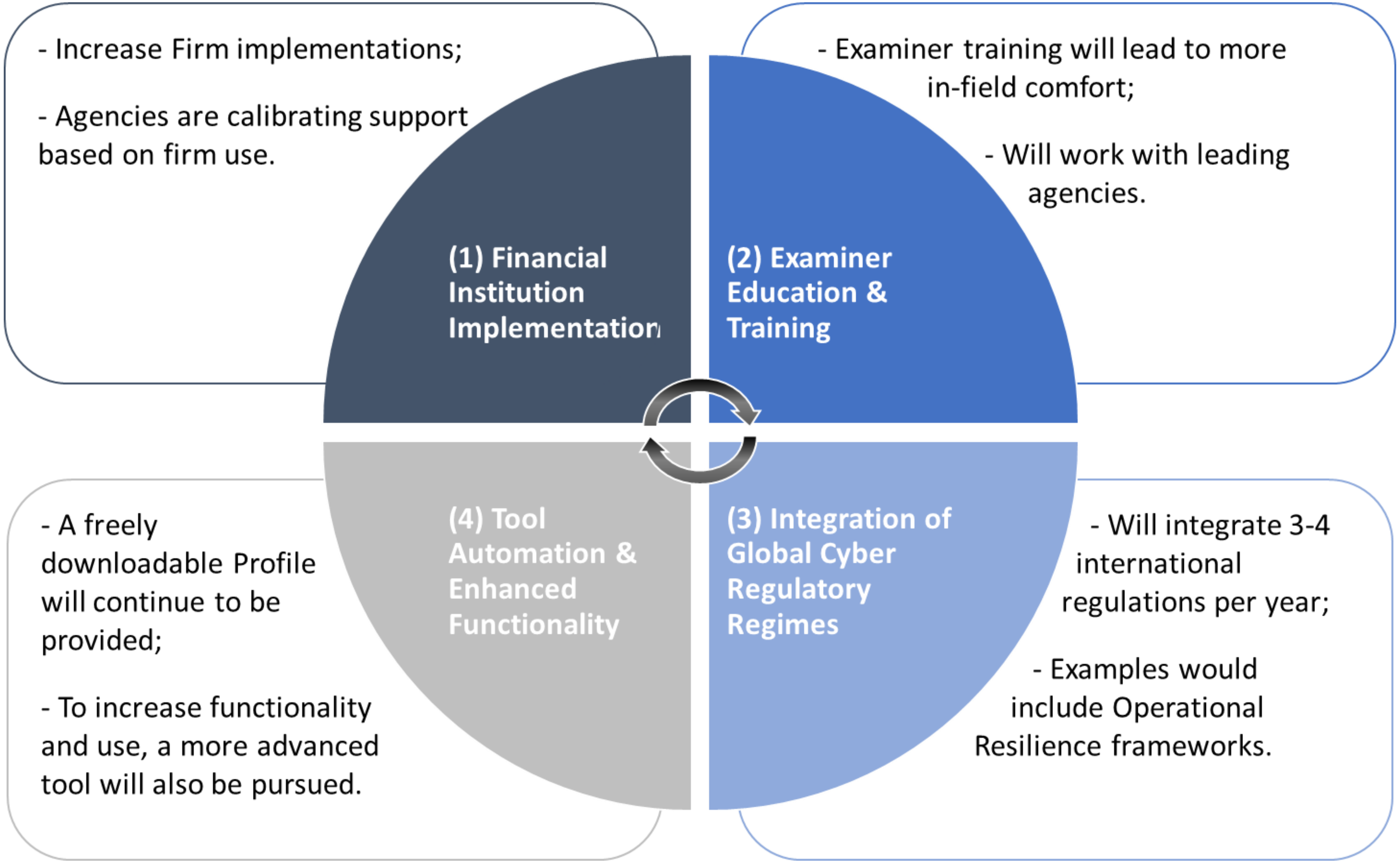
Functions	Categories	Subcategories	NIST CSF v1.1 Ref	FS Profile Diagnostic Statements	Diagnostic Statement Reponses	Tier 1: National+	Tier 2: Sub-National	Tier 3: Sector	Tier 4: Localized	FS References	Informative References from NIST CSF v1.1
Governance	**Strategy and Framework (GV.SF):** The organization 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

The Three Year Plan



(1) Financial Institution Implementation

- Increase Firm implementations;

- Agencies are calibrating support based on firm use.

(2) Examiner Education & Training

- Examiner training will lead to more in-field comfort;

- Will work with leading agencies.

(3) Integration of Global Cyber Regulatory Regimes

- Will integrate 3-4 international regulations per year;

- Examples would include Operational Resilience frameworks.

(4) Tool Automation & Enhanced Functionality

- A freely downloadable Profile will continue to be provided;

- To increase functionality and use, a more advanced tool will also be pursued.

Barth Bailey
SVP, Chief Information Security Officer
Fulton Financial

- Use Case -

Fulton Financial Corporation: About Us

- Regional Mid-Atlantic Bank Holding Company
- $19 billion in assets
- 255 offices in five states
- Headquartered in Lancaster, Pennsylvania
- Three affiliate banks
- Future consolidation into a single affiliate

We care about our relationships, we listen to what truly matters, and we deliver beyond what is expected to change lives for the better.

Fulton Financial: Cybersecurity Lines of Defense

First Line

- Information users (majority of employees)
- Information owners/ application owners
- Control owners
- Data custodians

Second Line

- Information security office
- Policies, procedures, governance, and administration
- Independent risk assessment, risk management of first line

Third Line

- Internal audit

Fulton Financial: Regulatory Oversight

U.S. Federal

- Federal Reserve (lead agency)
- OCC
- FDIC
- CFPB
- SEC

U.S. States

- Delaware
- Maryland
- New Jersey
- Pennsylvania
- Virginia

Fulton Financial: Top Reasons for Using the Cybersecurity Profile

1) ***Streamlines and reduces time spent on risk and compliance activities;***

2) ***Aligns with our strategic focus on 'simplification';***

3) Utilizes a single unified risk taxonomy and structure;

4) Integrates and aligns strongly with NIST CSF;

5) Replaces the FFIEC CAT;

6) Relies on direct mappings to demonstrate compliance with major financial sector regulatory requirements;

7) ***Provides meaningful and easy to understand board level reporting; and***

8) Integrates easily into our existing risk management framework.

Fulton Financial: The Profile Pilot

Third Party Risk Management

2019 pilot as assessment tool for critical Technology Service Providers (TSPs)

Utilized the 4-step process for assessment to the right

1) Information Gathering

- Business unit risk profiles
- Interviews with 1st line risk and control owners
- Credible challenge and validation

2) Control Maturity and Gap Assessment

- Cybersecurity Profile Assessment Primary 2019 Tool
- FFIEC CAT Assessment: Update based on the Cybersecurity Profile
- Gather and organize supporting documentation

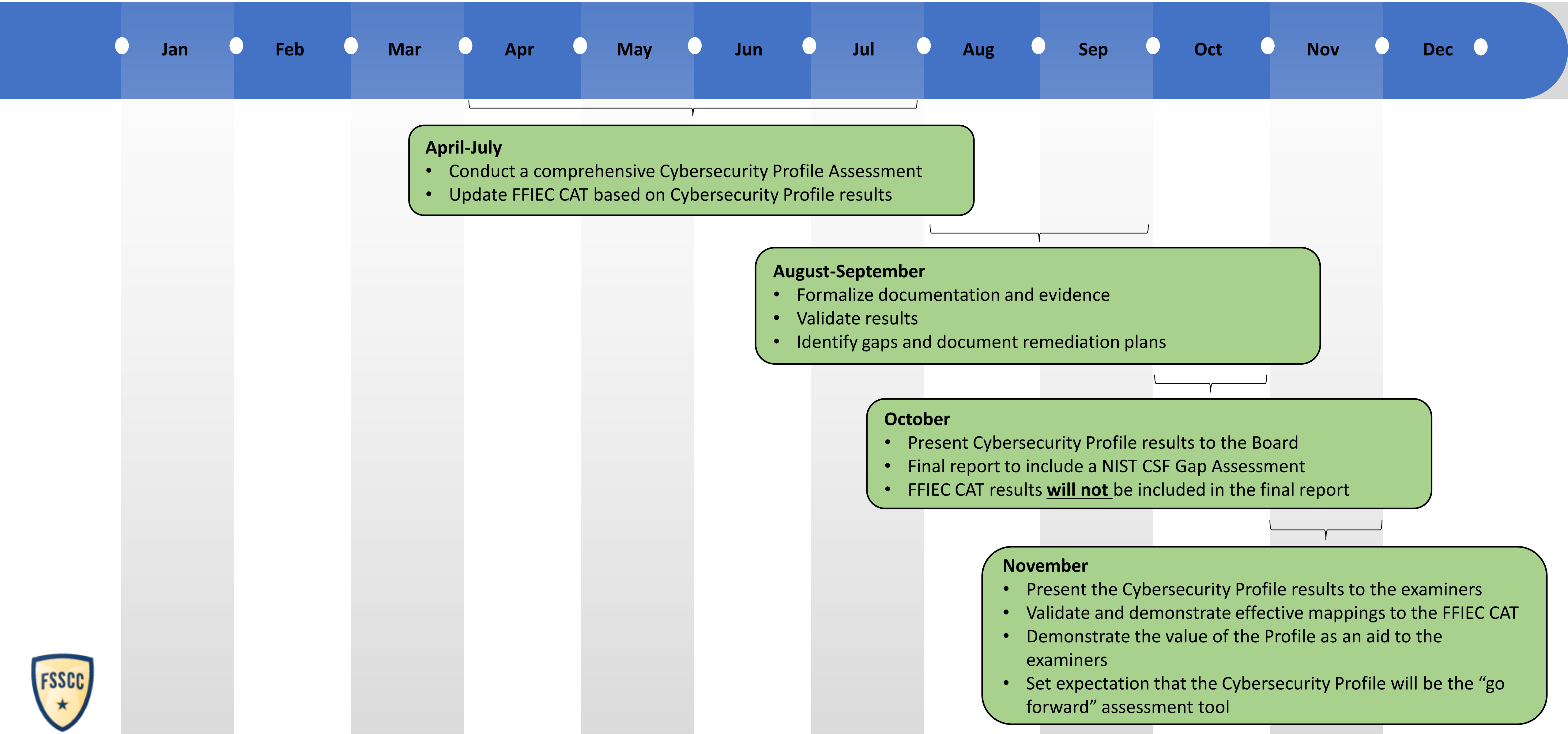
3) Identify and Assess Risk

- Cybersecurity Profile assessment
- Threat and vulnerability analysis
- Business unit risk profiles and interviews
- Risk assessment based on qualitative criteria and quantitative scoring elements

4) Manage Risk

- Aligned with Corporate Risk Appetite
- Develop risk treatment plans: ***Accept. Mitigate. Transfer. Avoid.***
- Track and document progress
- Updated Cybersecurity Profile Assessment annually or when material “Trigger Event” occurs

Fulton Financial: 2019 Implementation Timeline and Milestones



Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

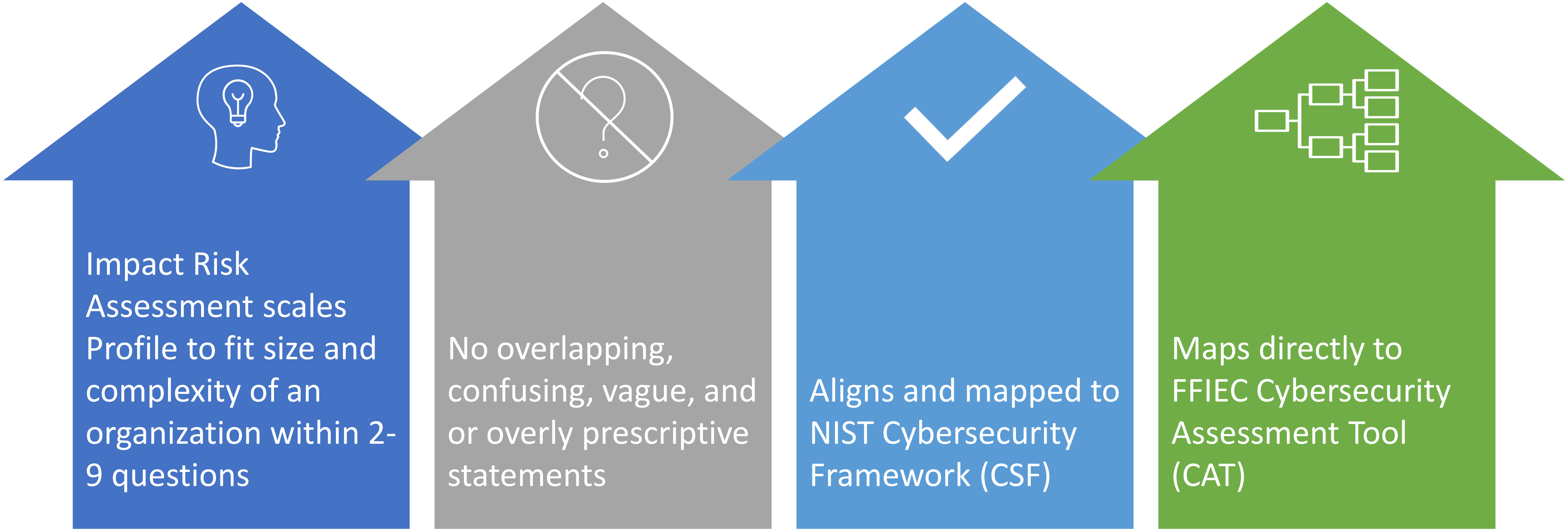
April-July
- Conduct a comprehensive Cybersecurity Profile Assessment
- Update FFIEC CAT based on Cybersecurity Profile results

August-September
- Formalize documentation and evidence
- Validate results
- Identify gaps and document remediation plans

October
- Present Cybersecurity Profile results to the Board
- Final report to include a NIST CSF Gap Assessment
- FFIEC CAT results **will not** be included in the final report

November
- Present the Cybersecurity Profile results to the examiners
- Validate and demonstrate effective mappings to the FFIEC CAT
- Demonstrate the value of the Profile as an aid to the examiners
- Set expectation that the Cybersecurity Profile will be the “go forward” assessment tool

Fulton Financial: Ease of Use is a Key Benefit



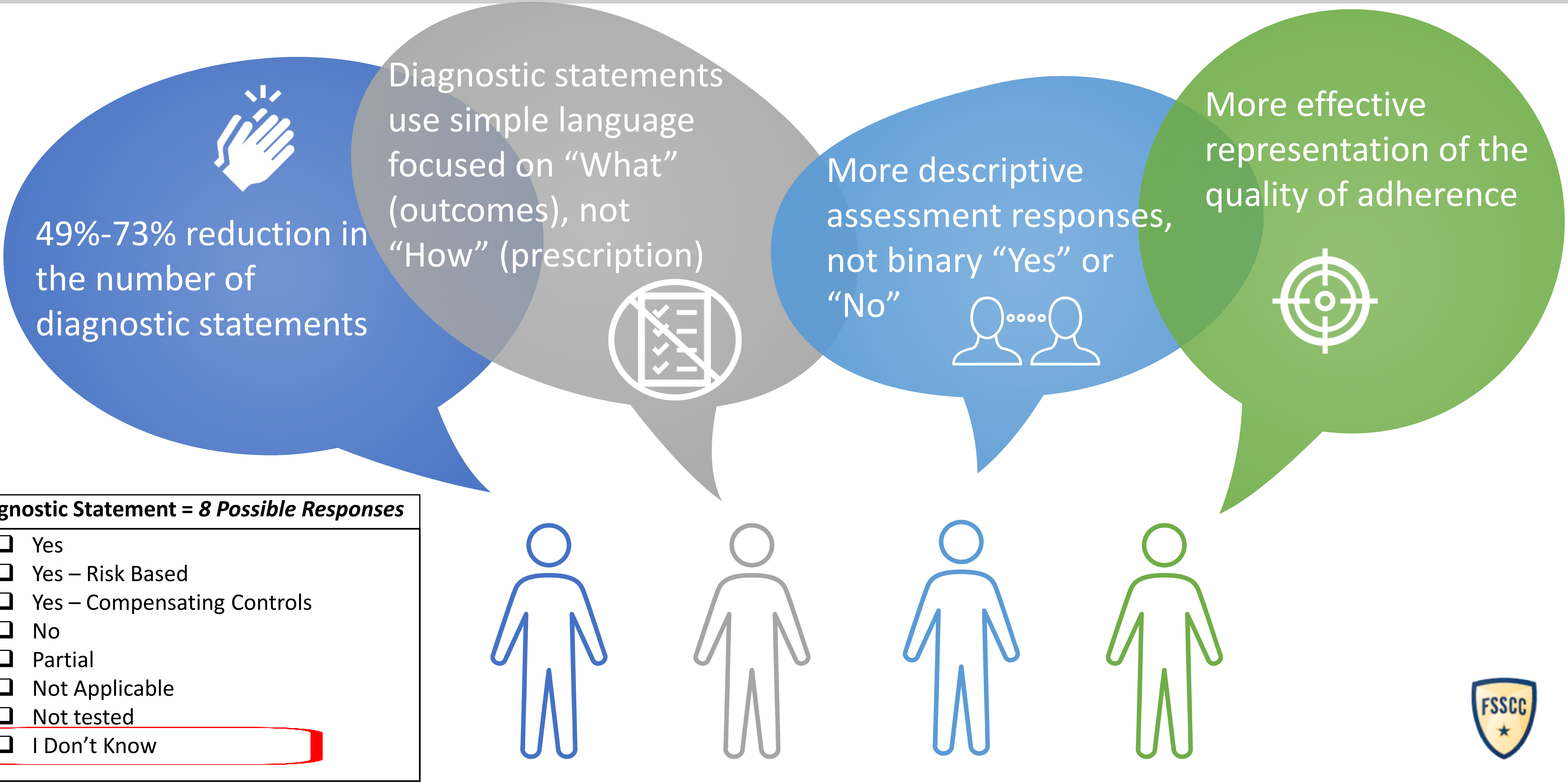
Impact Risk Assessment scales Profile to fit size and complexity of an organization within 2-9 questions

No overlapping, confusing, vague, and or overly prescriptive statements

Aligns and mapped to NIST Cybersecurity Framework (CSF)

Maps directly to FFIEC Cybersecurity Assessment Tool (CAT)

Fulton Financial: Use of Diagnostic Responses



49%-73% reduction in the number of diagnostic statements

Diagnostic statements use simple language focused on “What” (outcomes), not “How” (prescription)

More descriptive assessment responses, not binary “Yes” or “No”

More effective representation of the quality of adherence

Diagnostic Statement = *8 Possible Responses*

- ❑ Yes
- ❑ Yes – Risk Based
- ❑ Yes – Compensating Controls
- ❑ No
- ❑ Partial
- ❑ Not Applicable
- ❑ Not tested
- ❑ I Don’t Know

Fulton Financial: Socialization for Supervisors

Share your vision.

Focus on your strategic goal of transitioning to the FSSCC Cybersecurity Profile and its associated benefits

Keep it practical.

Explain the tangible benefits of the Profile to the organization, sector, and the examination process

WASH. RINSE. REPEAT.

Be prepared to re-socialize multiple times

Focus on the positive benefits.

Press though initial apprehension with facts

Fulton Financial: Internal Socialization

Board of Directors

- Provide a high-level overview of the strategic benefits of the Profile
- Focus on potential benefits around reporting, trending, and benchmarking

Enterprise Risk Management and Internal Audit

- Easy to understand, logically organized, risk and control language and taxonomy
- Aligns with NIST CSF
- Integrates reporting within the ERM organization risk taxonomy

Lessons Learned 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.**

FSSCC

Executive Summary:

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.

Supporting Associations:

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

American Bankers Association

bpi BITS Business Innovation Technology Security

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’s 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.

Global Interest in NIST and FSSCC Cyber Profile

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:

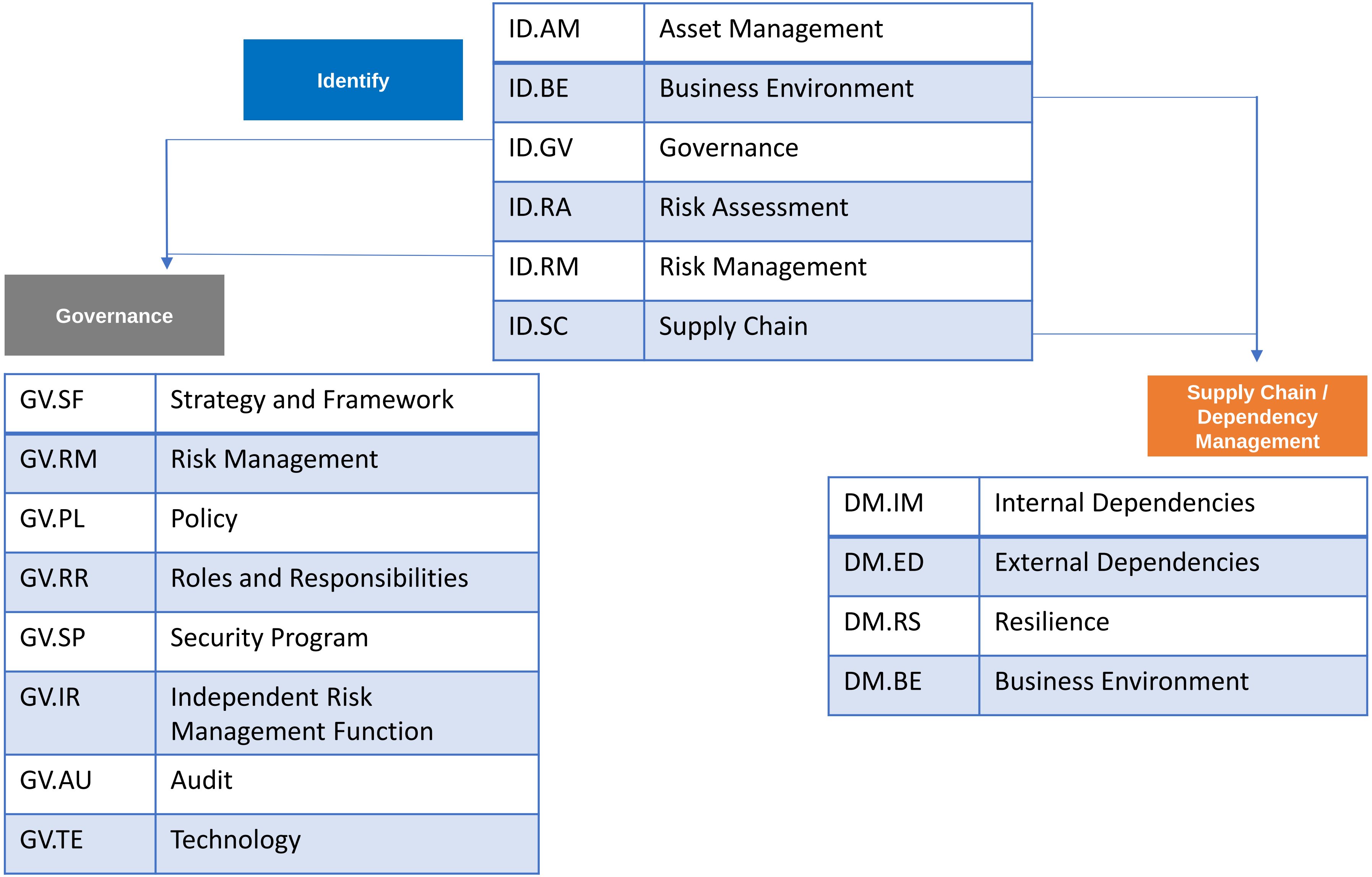
Governance

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

Customized for Financial Services: Governance, Third Parties



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/Third Party Due Diligence

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