RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CXO-T10**

Frameworks, Mappings & Metrics Optimize Your Time As CISO Or Auditor

Freddy Dezeure

CEO
Freddy Dezeure BV
@FDezeure

Josh Magri

SVP, Counsel for Regulation & Developing Technology
Bank Policy Institute – BITS
@bankpolicy

Who Are We?

Freddy Dezeure

- Independent strategic advisor
- Advisor/Board Member in high-tech start-ups
- Community contributor
- Founder and Head of CERT-EU from 2011-2017

Josh Magri

- Senior Vice President, Bank Policy Institute-BITS Architect of the FSSCC Cybersecurity Profile
- Associate VP, Internet Security Alliance – Author of the NACD “Cyber Risk Oversight Handbook”
- Assistant District Attorney, Bronx County District Attorney’s Office

Agenda

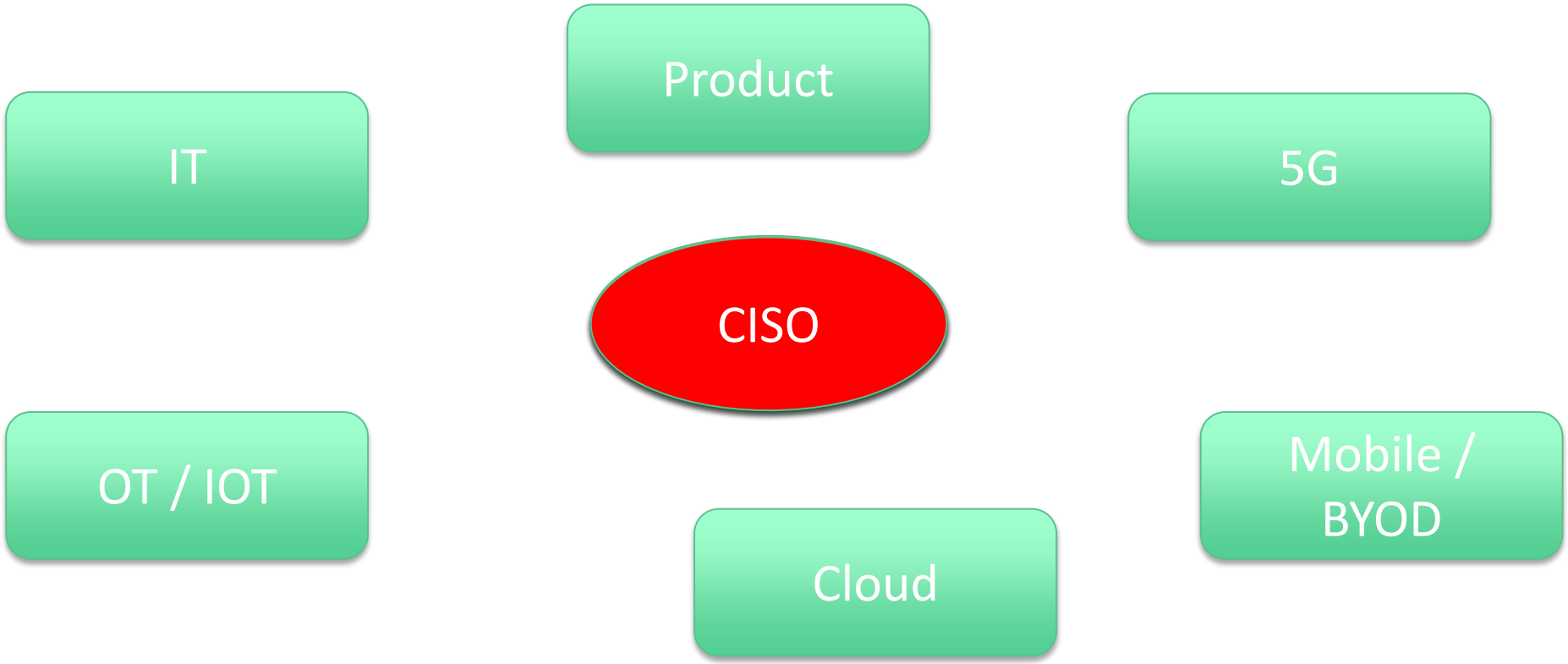
- Legal Context and Challenges
- A Solution : Mapping to a Common Framework
- Charting Progress : Metrics

RSAConference2020

Legal Context and Challenges

So Little Time Left To Do Our Work

The Infrastructure To Protect



Targeted Ransomware – "Big Game Hunting"

Asco closure after cyber-attack to last another week

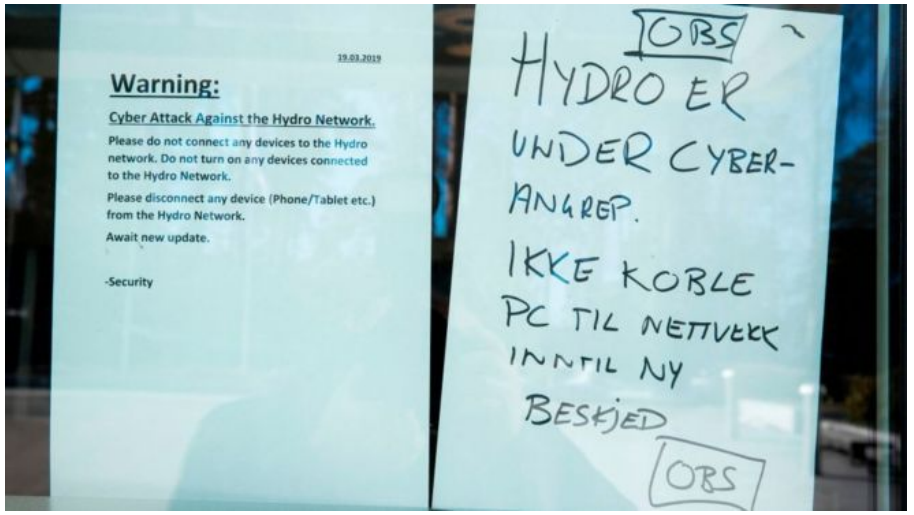
Saturday, 22 June 2019

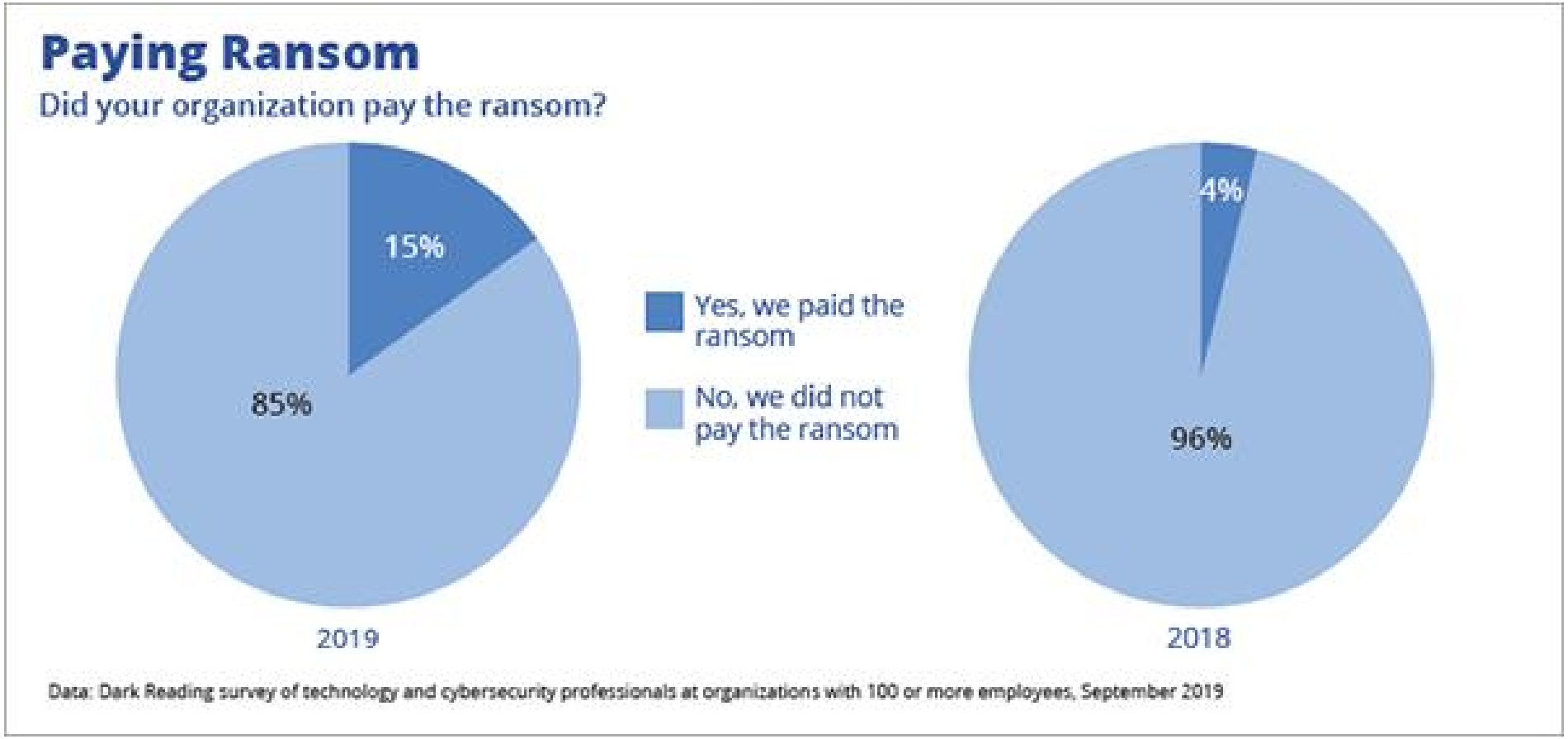
© Belga

Eurofins Scientific: Forensic services firm paid ransom after cyber-attack

By Danny Shaw
Home affairs correspondent

5 July 2019 Share




Paying Ransom
Did your organization pay the ransom?
15%
85%
2019
Yes, we paid the ransom
No, we did not pay the ransom
4%
96%
2018
Data: Dark Reading survey of technology and cybersecurity professionals at organizations with 100 or more employees, September 2019

Prevention, Detection, Response is not Enough

RESILIENCE

Frameworks


ISO
27001

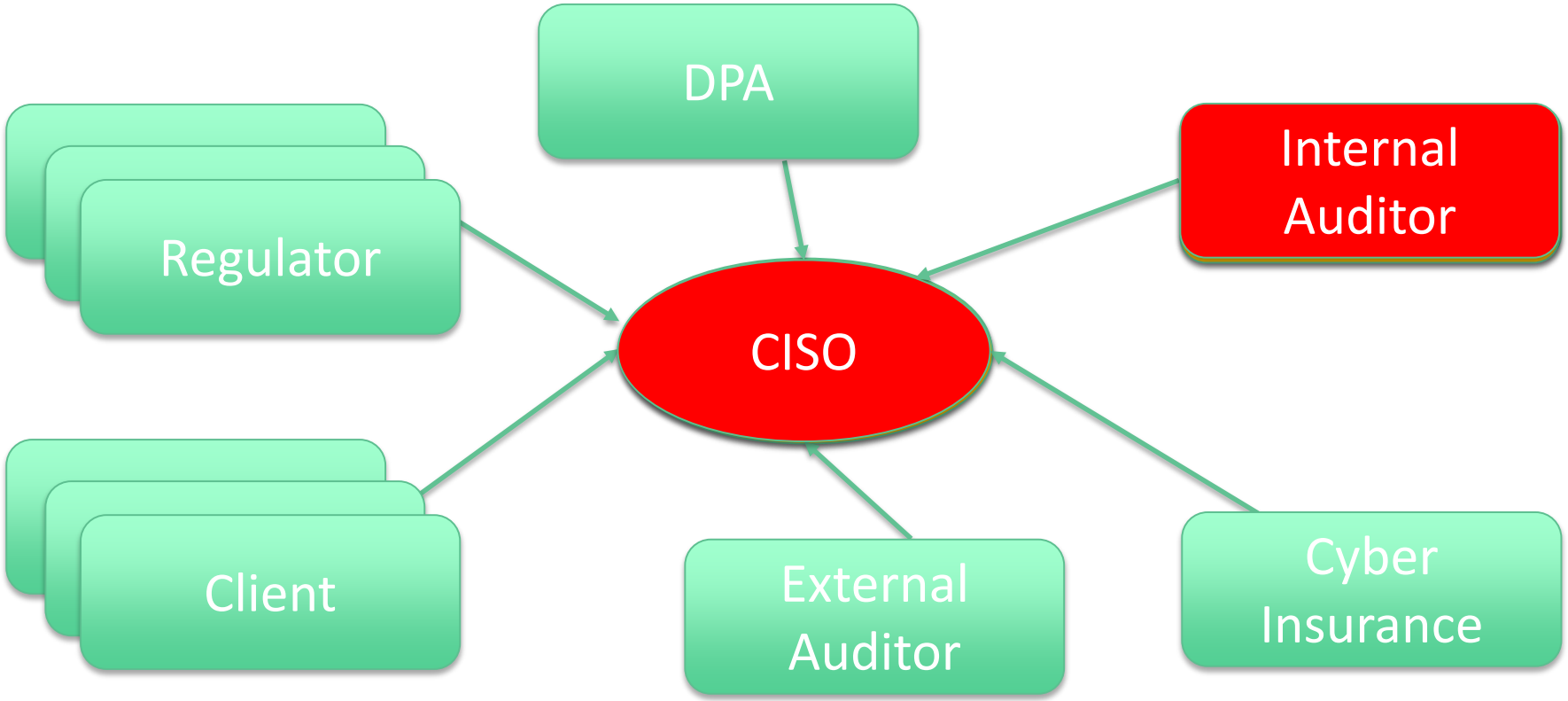

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1


CIS
Center for Internet Security®

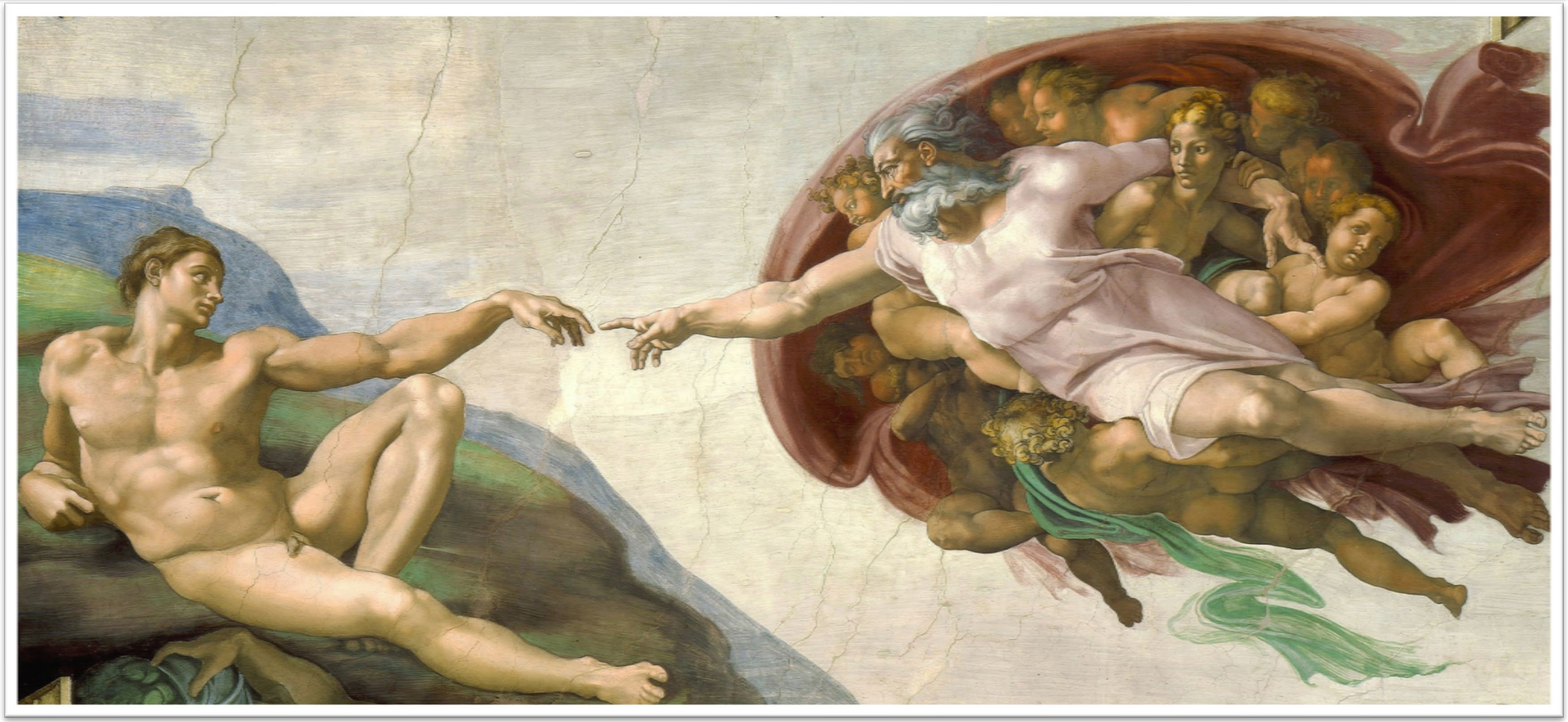

FFIEC


COBIT 5
AN ISACA® FRAMEWORK

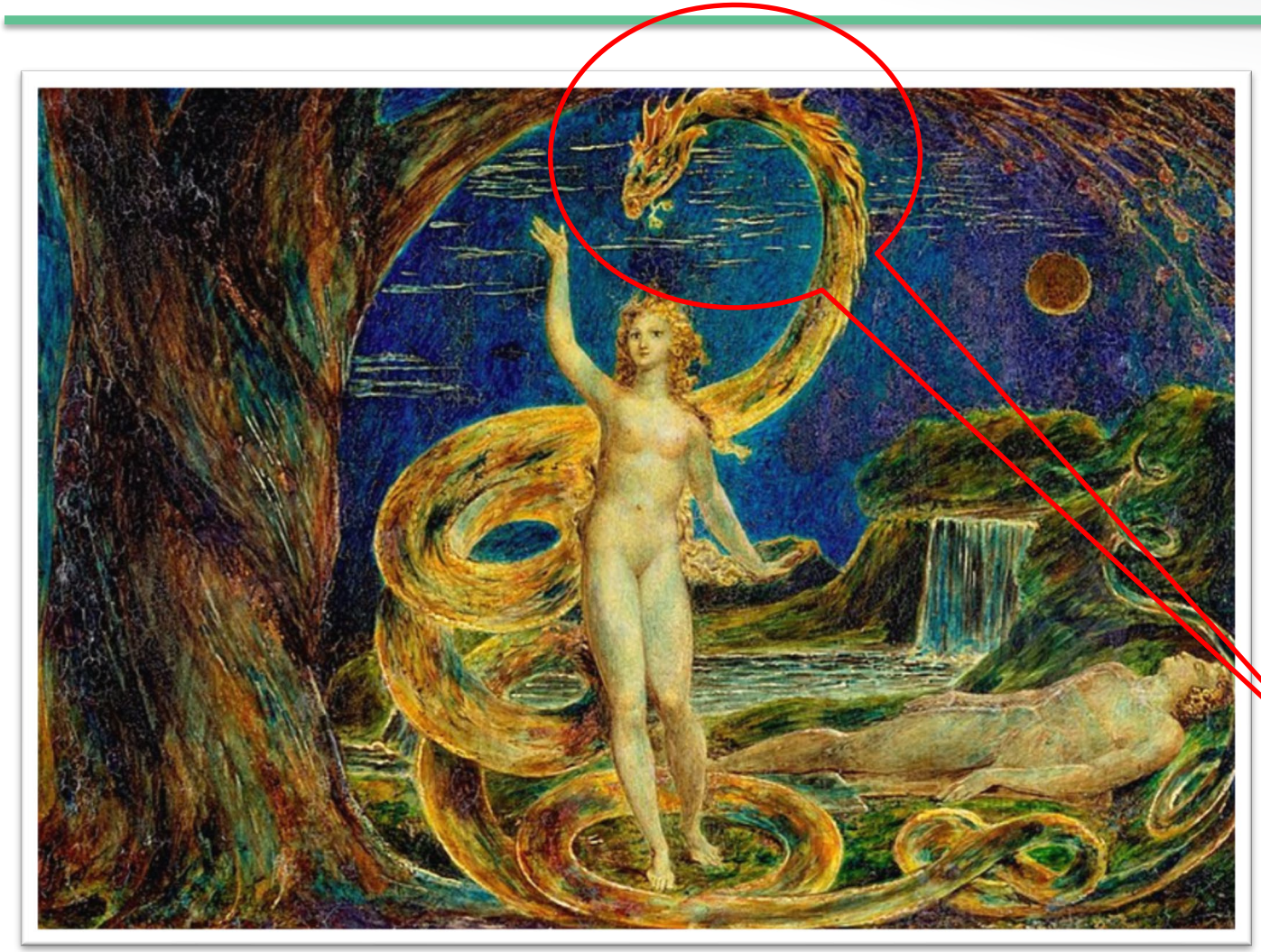
Compliance Demands



The Creation of Adam (Michelangelo)



Eve Tempted by the Serpent (William Blake)

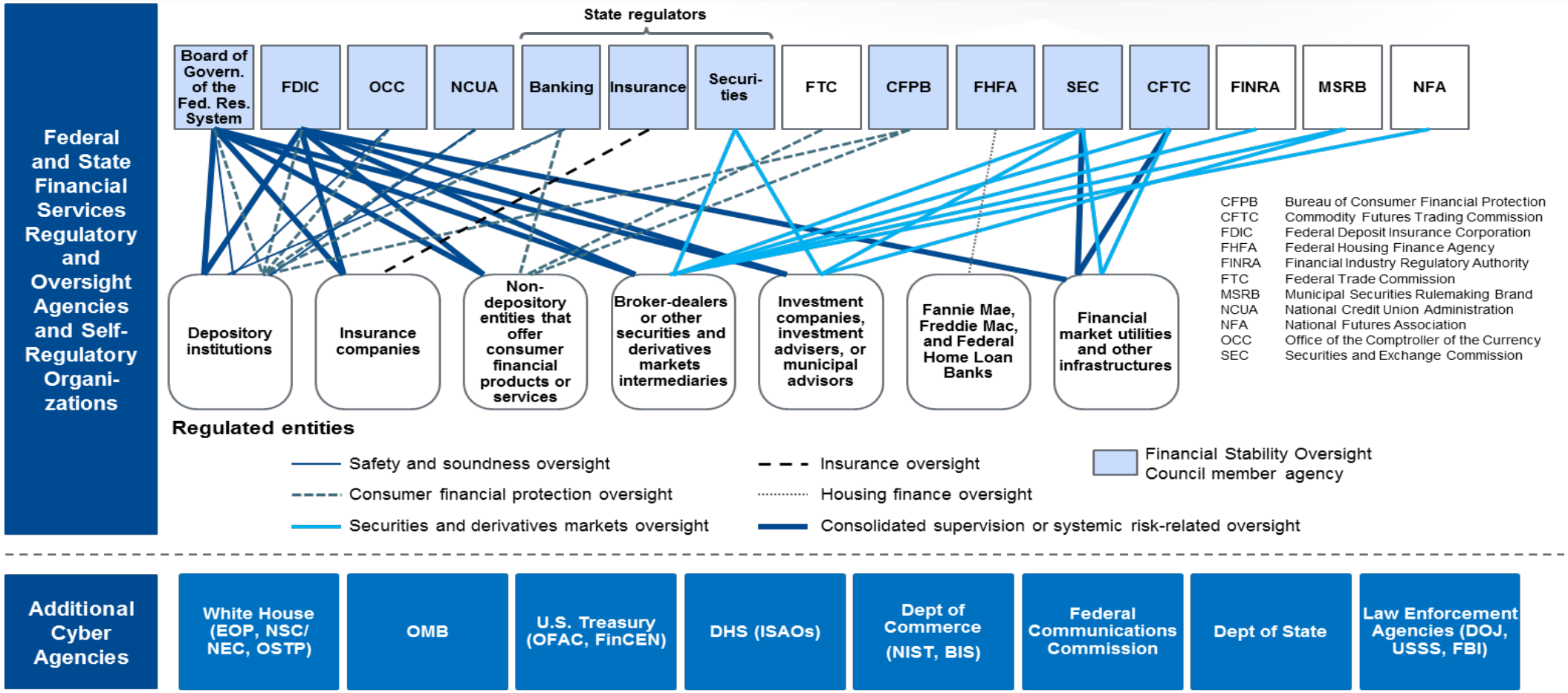


Genesis 3:1 -

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

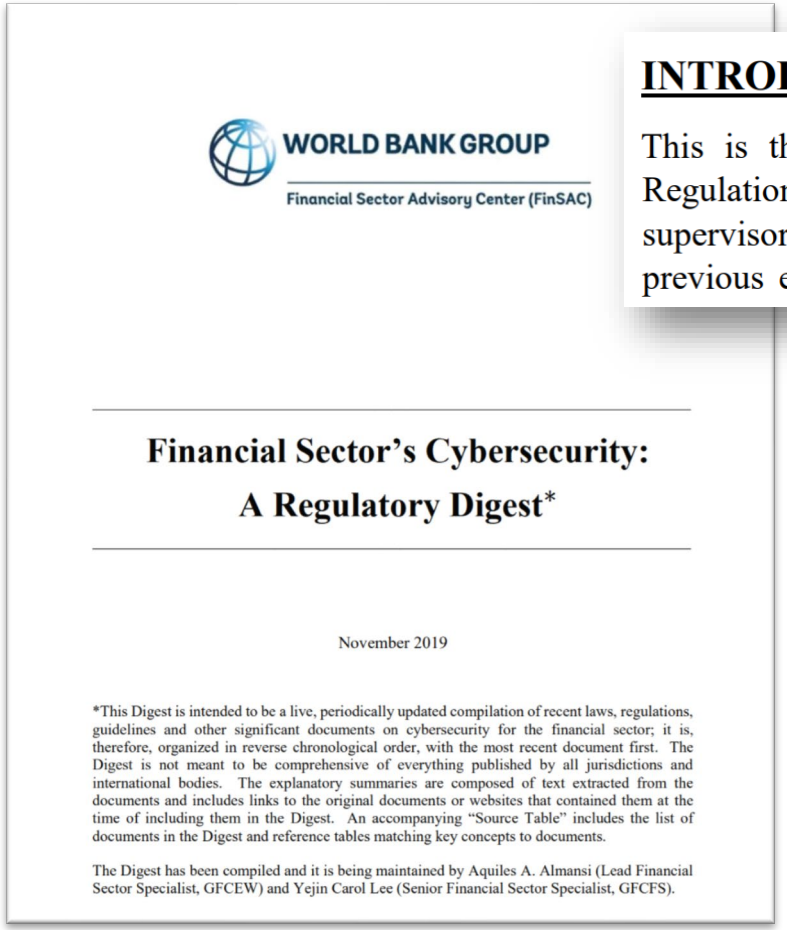
The first lawyer?

The U.S. Financial Services Regulatory Structure



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

That's Not All



WORLD BANK GROUP

Financial Sector Advisory Center (FinSAC)

Financial Sector's Cybersecurity:

A Regulatory Digest*

November 2019

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

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

INTRODUCTION

This is the fourth edition of the World Bank's FinSAC Digest of Cybersecurity Regulations in the Financial Sector. It adds 35 cybersecurity related regulatory or supervisory initiatives (in 44 documents) to the 157 (in 173 documents) included in the previous edition.

BANK OF ENGLAND

EUROPEAN CENTRAL BANK

EUROSYSTEM

MAS Monetary Authority of Singapore

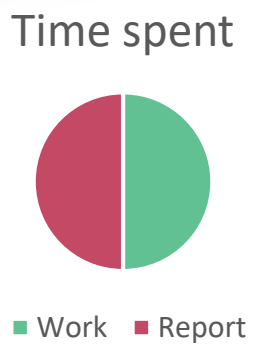
SWIFT

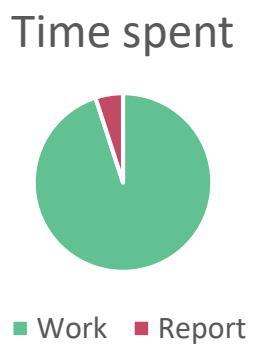
HONG KONG MONETARY AUTHORITY

香 港 金 融 管 理 局

bpi BANK POLICY INSTITUTE

*Tower of Babel (*Pieter Bruegel the Elder); And the 40%





Result From Cross-Sector Workshop 23 January 2020

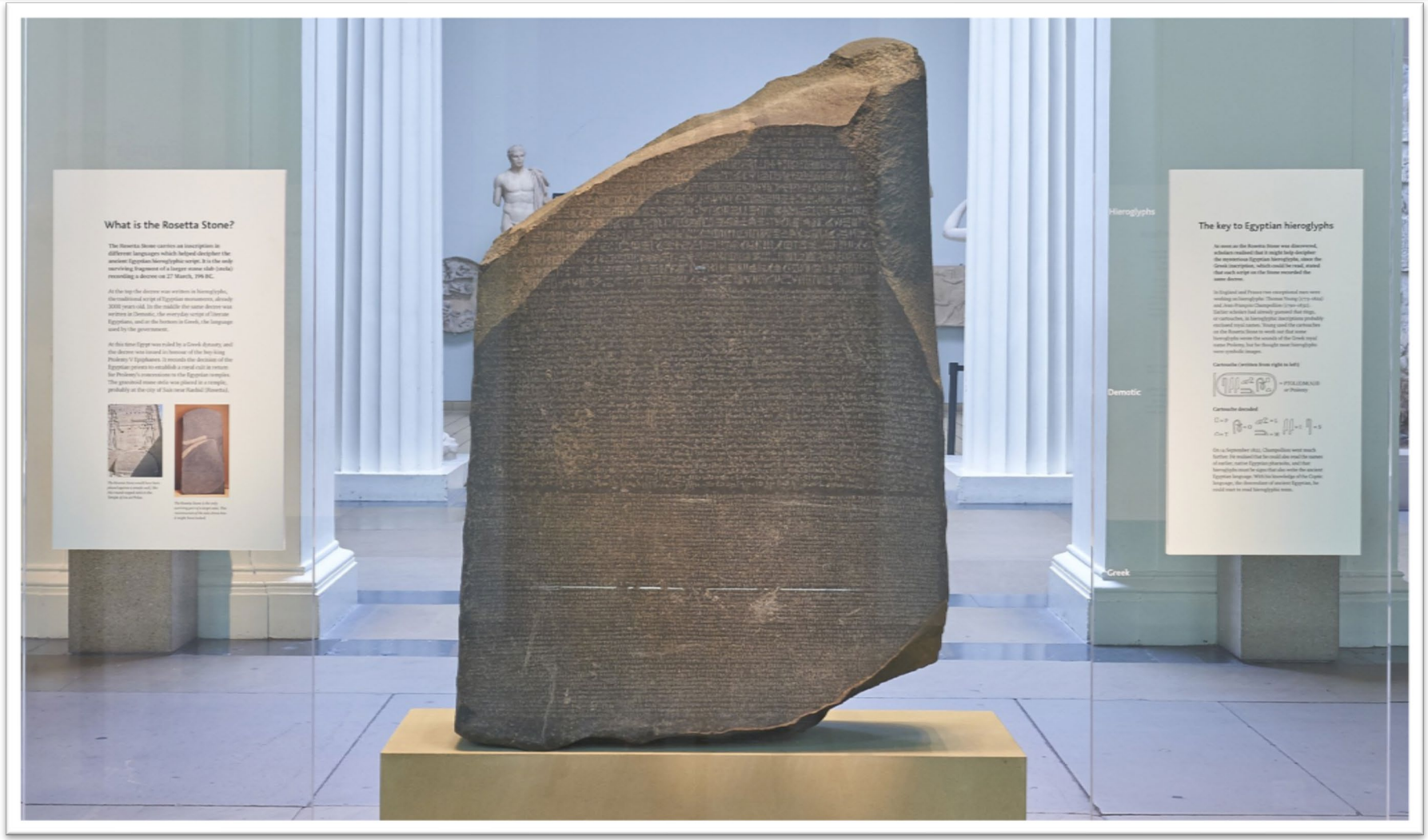
- This 40% burden is felt cross-sector and cross-region
- Large similarities in substance :
  - Threats
  - Vulnerabilities
  - Controls
  - Processes
  - Solutions
  - Oversight
- Gap in sharing of existing solutions

RSAConference2020

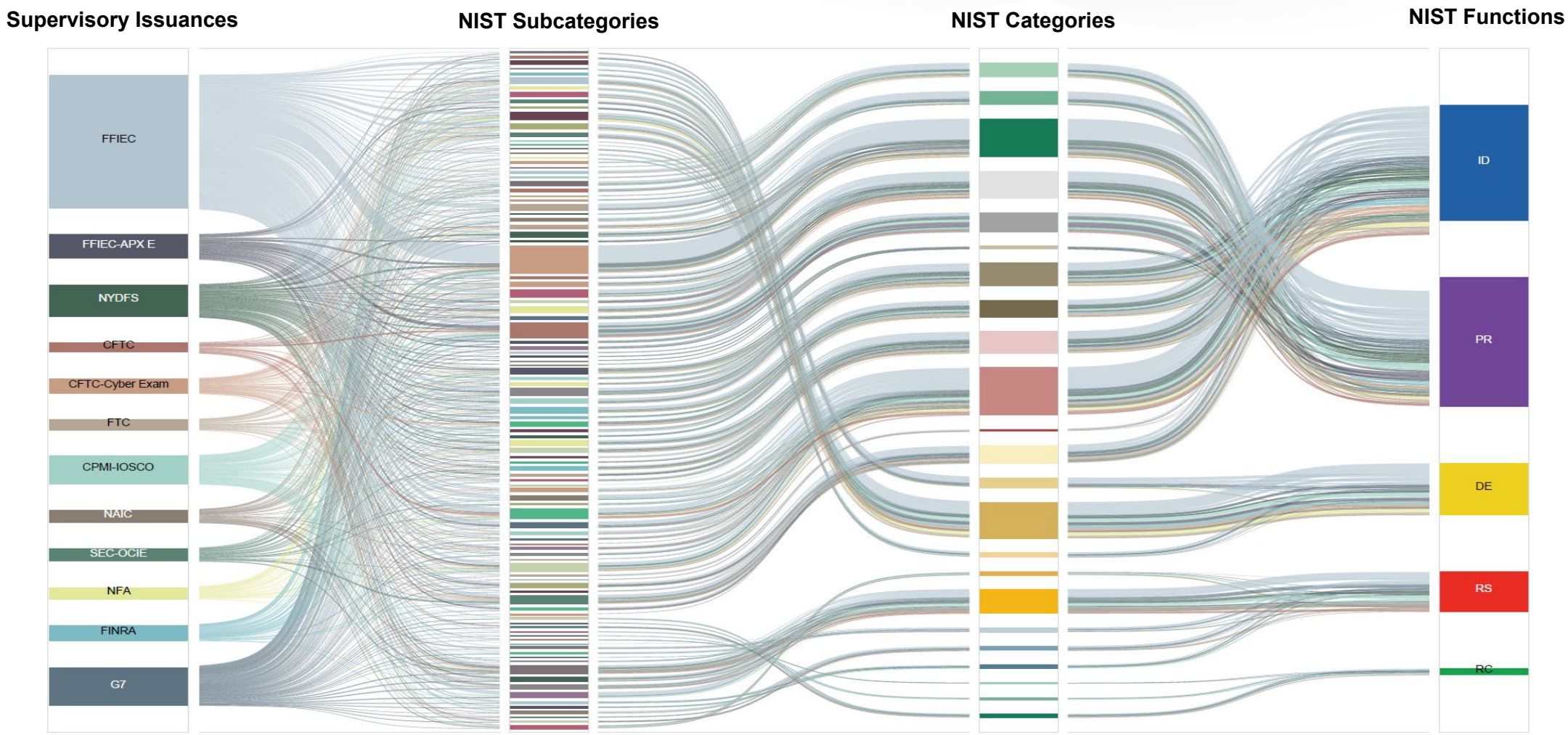
A Solution : Mapping to a Common Framework

Applicable for all sectors, developed in the financial services sector

The Rosetta Stone: The Inspiration for the FSSCC Profile



Graphical Depiction of the Reconciliation Process



The FSSCC Cybersecurity Profile

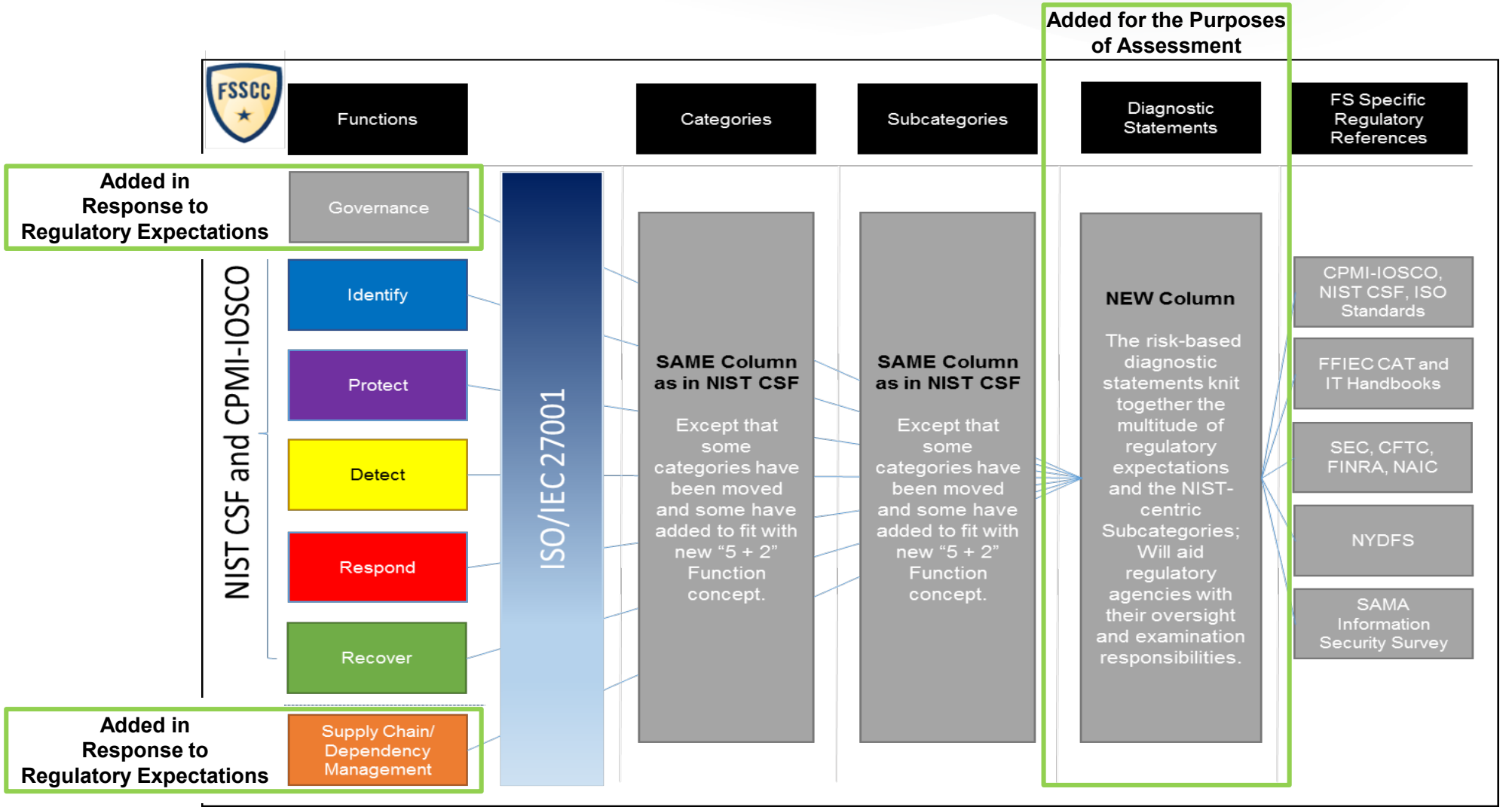
1) Part I: Impact Assessment (9 questions)

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

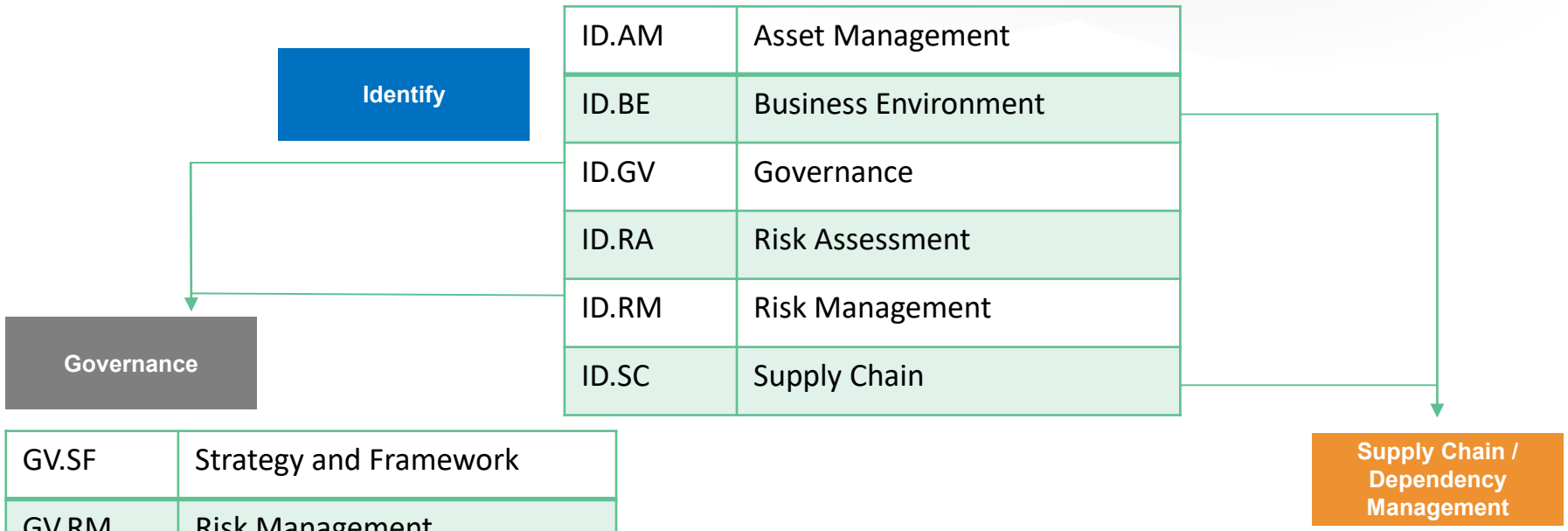
Profile and materials available at no cost:

- 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 Follows)



The Additions of Governance and Supply Chain/Dependency Management



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

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

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

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

Impact Questionnaire

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

National or Global Impact – Tier 1

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

277 Diagnostics

Subnational (Regional) Impact – Tier 2

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

262 Diagnostics

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

- ~ 100+ firms implementing the Profile or actively exploring implementation for 2020.

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

136 Diagnostics

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

Customer/3rd Party Impact Only – Tier 4

Benefits of the FSSCC 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

- ✓ *More time on defense*
- ✓ *Improved Boardroom and Executive engagement*

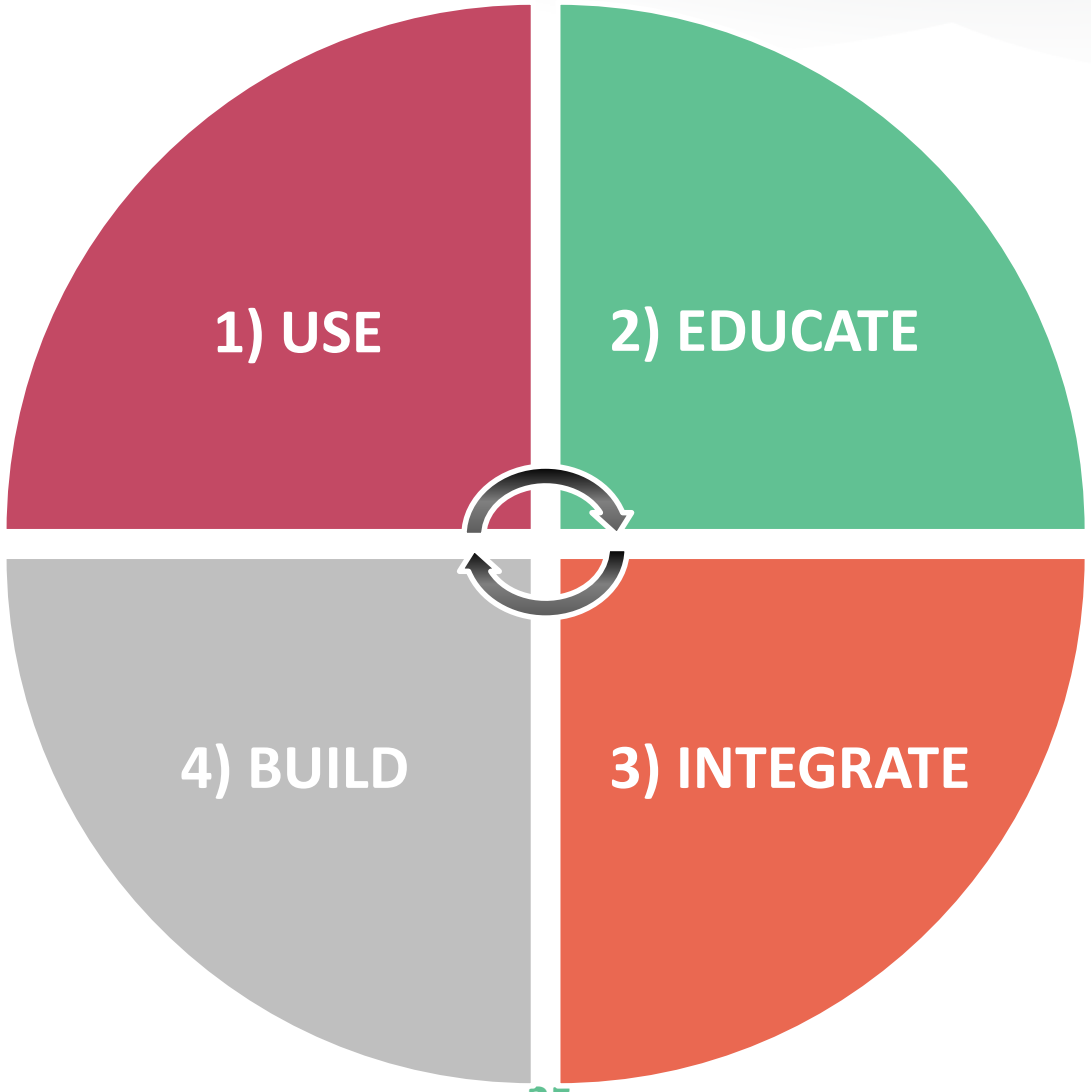
Supervisory Community

- ✓ *Enables systemic risk analysis*
- ✓ *Visibility of non-sector and third-party cyber risks.*

The Ecosystem

- ✓ *Standardized approach based on NIST and ISO for greater collaboration*
- ✓ *Enables evidence of compliance*

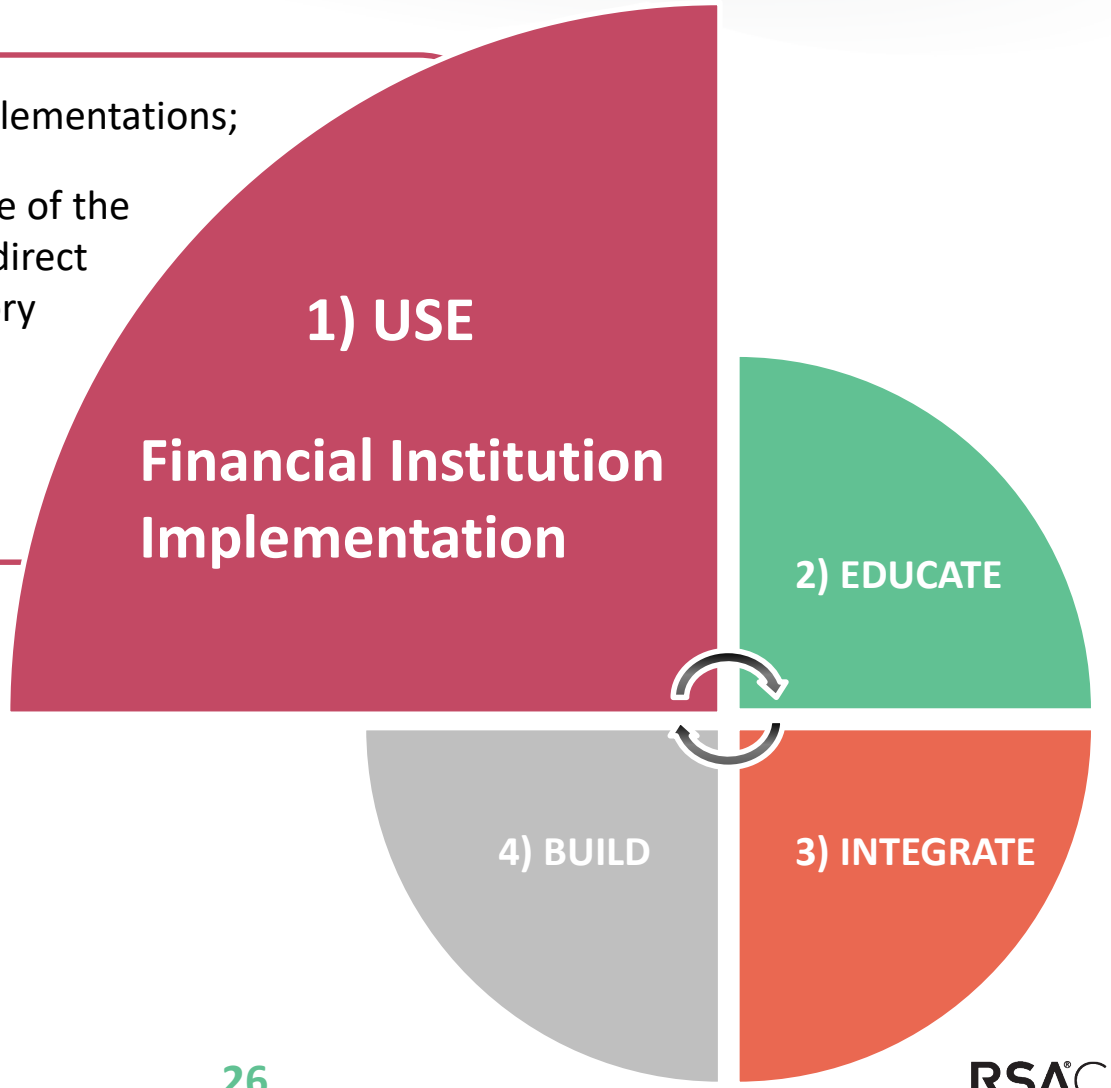
Four Areas of Focus



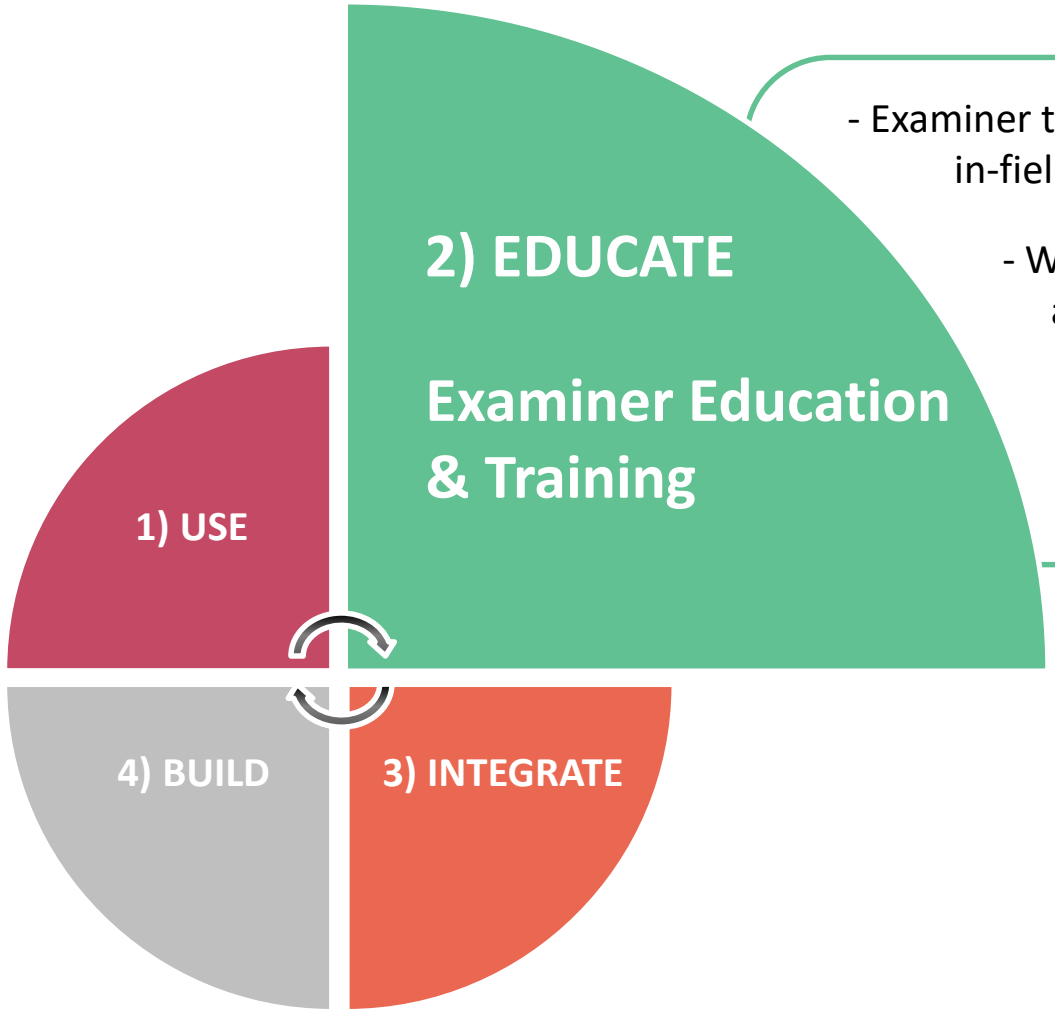
Four Areas of Focus: USE

- Increase firm implementations;

- Financial firms use of the Profile will have a direct impact on regulatory acceptance.



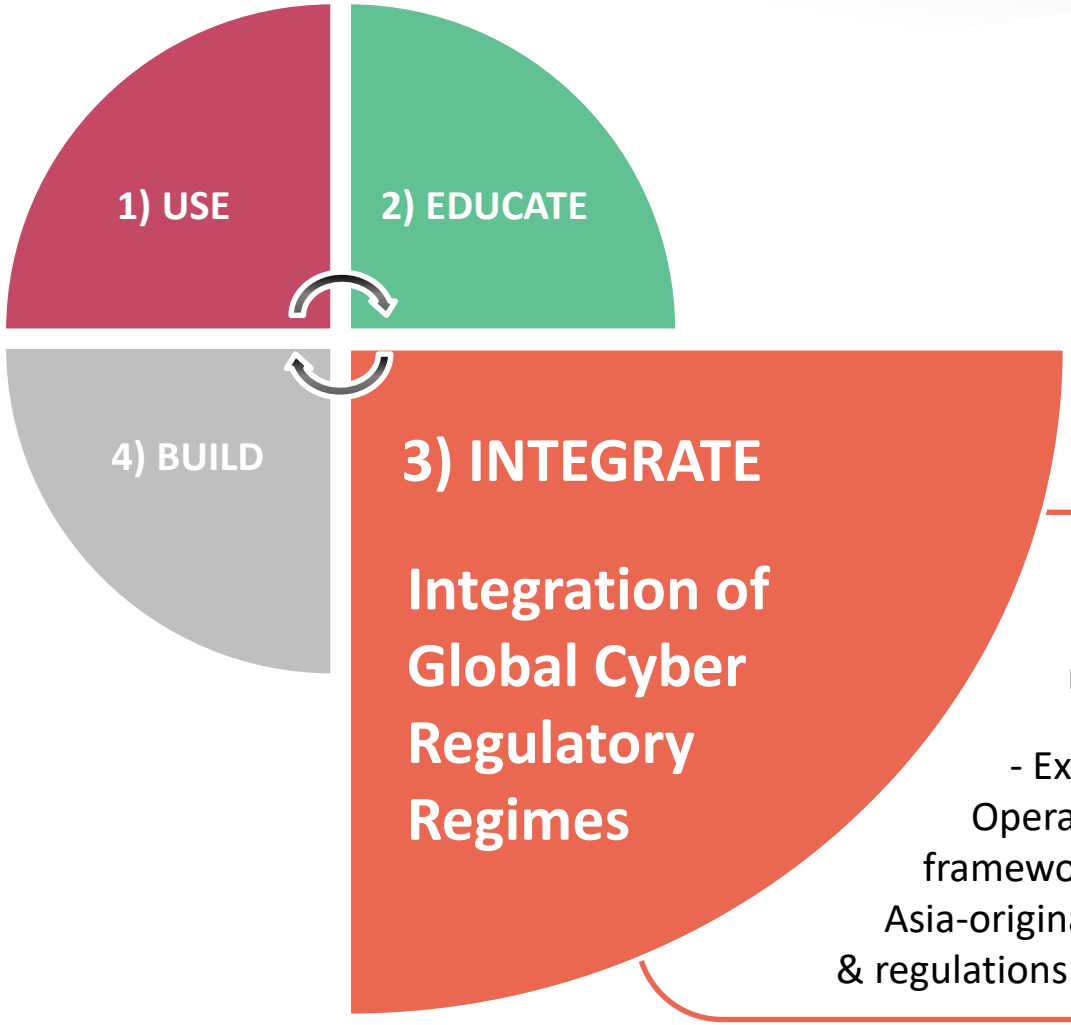
Four Areas of Focus: EDUCATE



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

- Work with leading agencies in the US and across the globe.

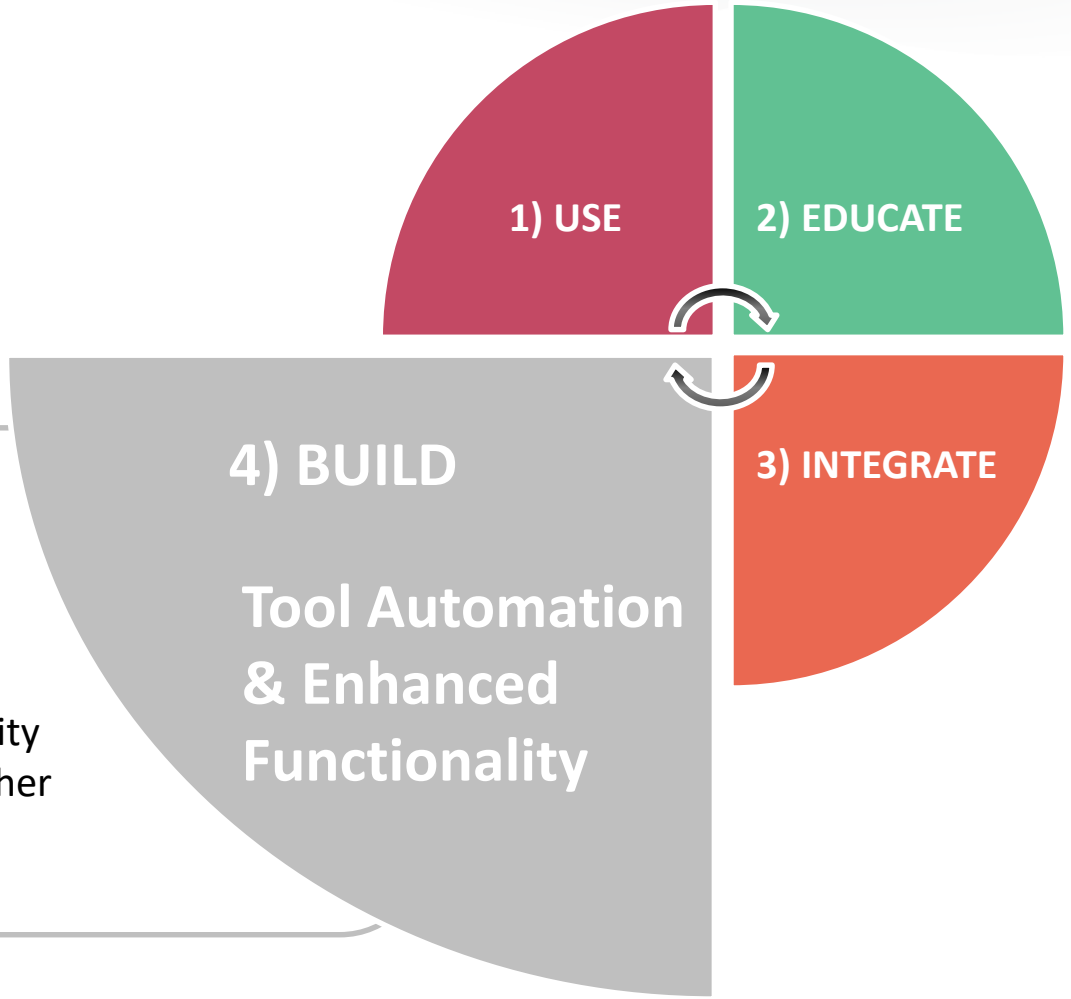
Four Areas of Focus: INTEGRATE



- Integrate 3-5 international regulations per year;

- Examples include Operational Resilience frameworks, and EU and Asia-originated questionnaires & regulations.

Four Areas of Focus: BUILD



- A freely downloadable Profile will continue to be provided;

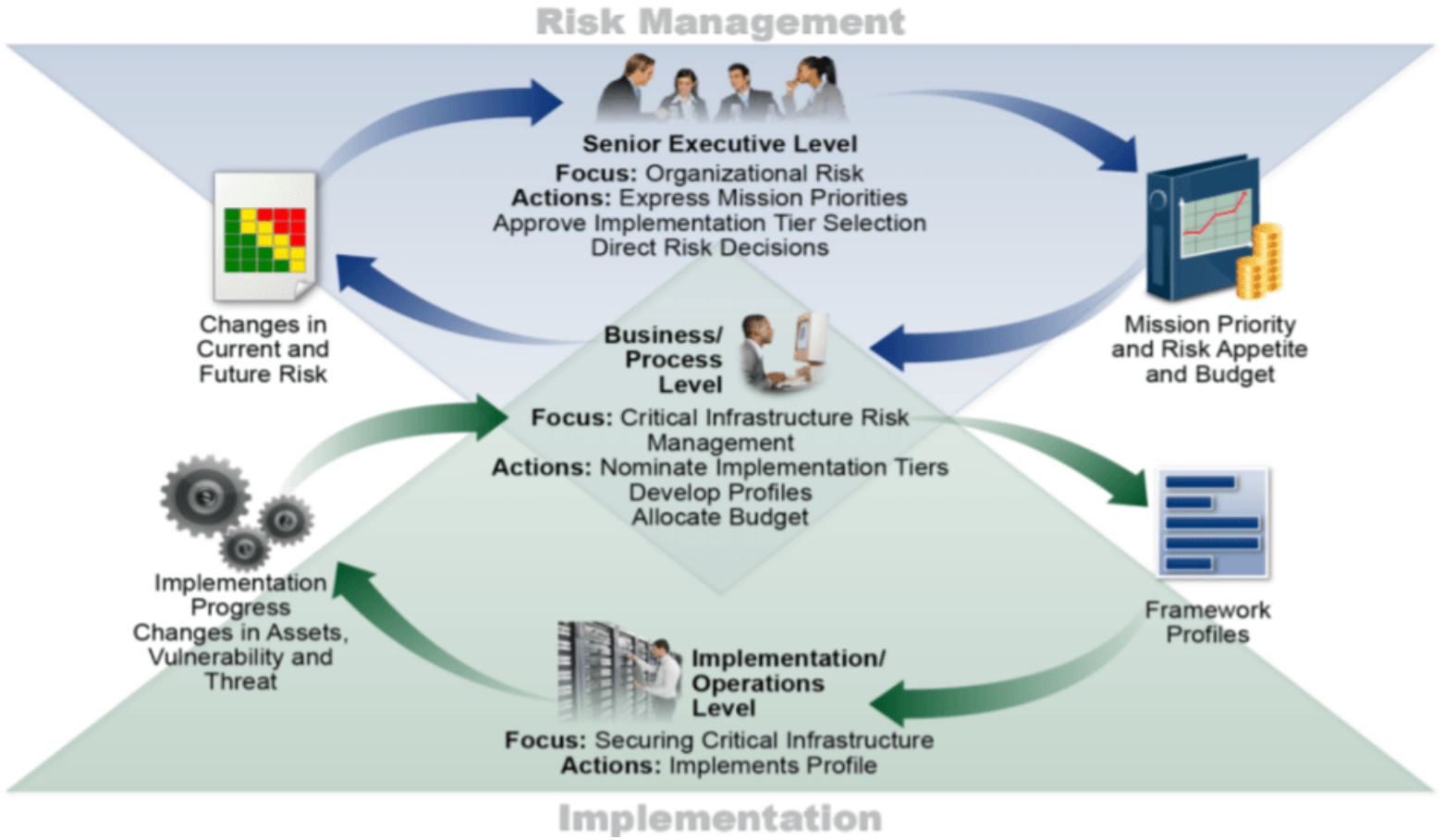
- To increase functionality and use, develop a further enhanced tool.

RSAConference2020

Charting Progress : Metrics

Objectivize Your Dashboard

What Matters Most?



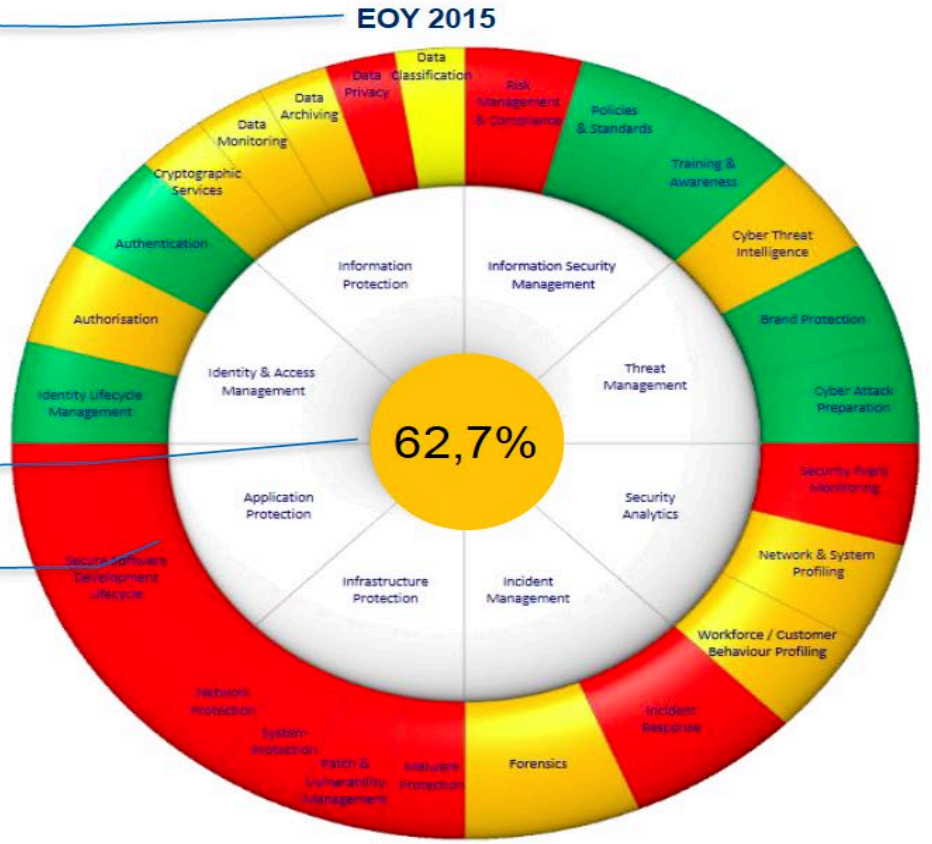
Make Metrics Talk

This shows the moment in time for the presented values
… assuming technology doesn't change
… assuming the threat landscape doesn't shift
… assuming all planned projects can/will be implemented

The Cyber Resilience shows how close this organization is compared to the maturity that is required for its specific threat landscape

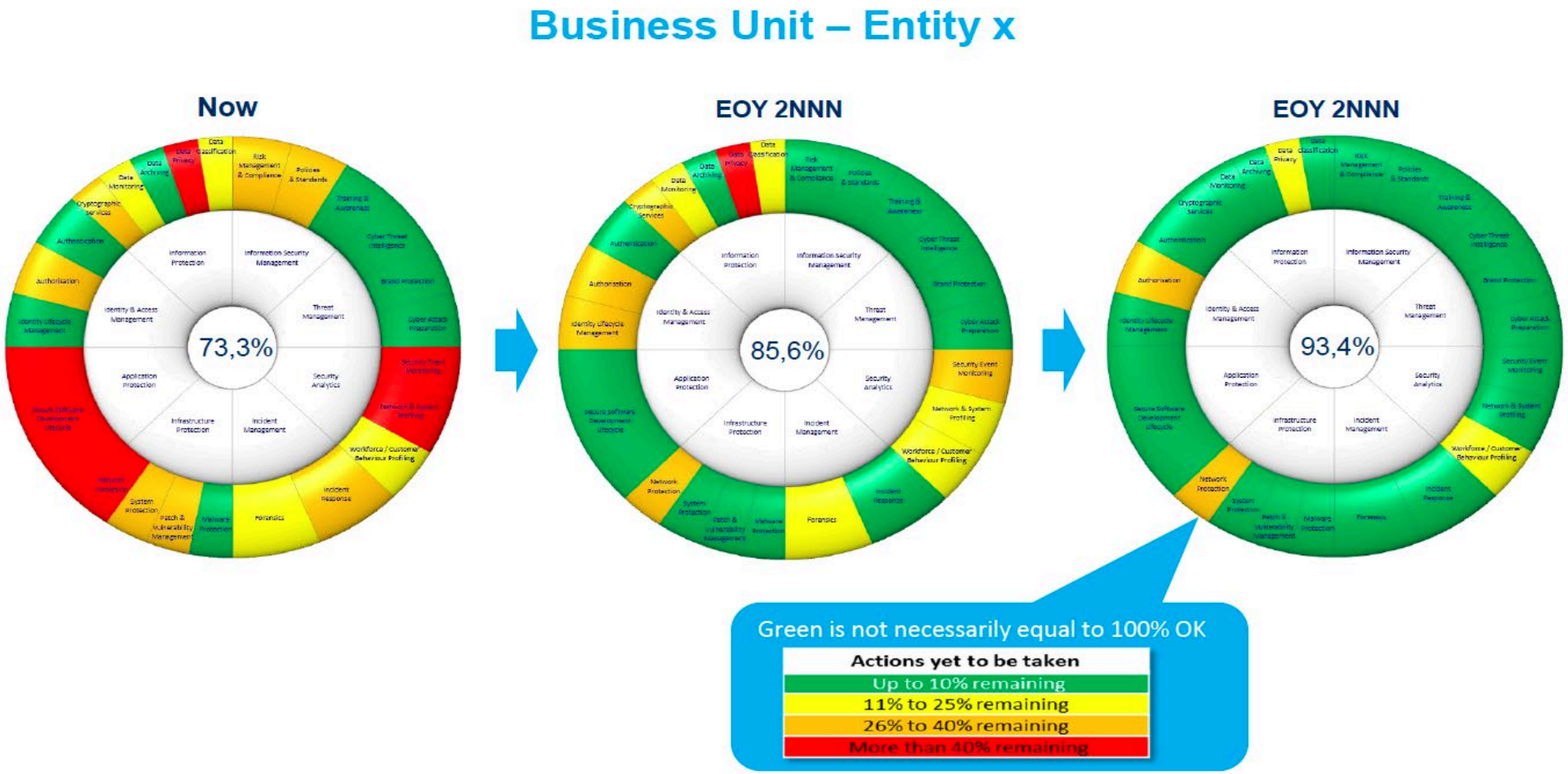
Color coding

Actions yet to be taken
Up to 10% remaining
11% to 25% remaining
26% to 40% remaining
More than 40% remaining



Jan Nys, KBC, presentation at RSA 2016

Charting Progress Over Time



Metrics: Principles To Follow

- Linked to your applied Framework
- Continuously drawing from your data
- Continuously improved
- Integrated in your business risk process

Metrics: Principles To Follow (2)

- Choose them carefully
  - Input indicators: implement a system/process
  - Output indicators: statistical results
  - Impact indicators: measurable outcome in terms of risk mitigation

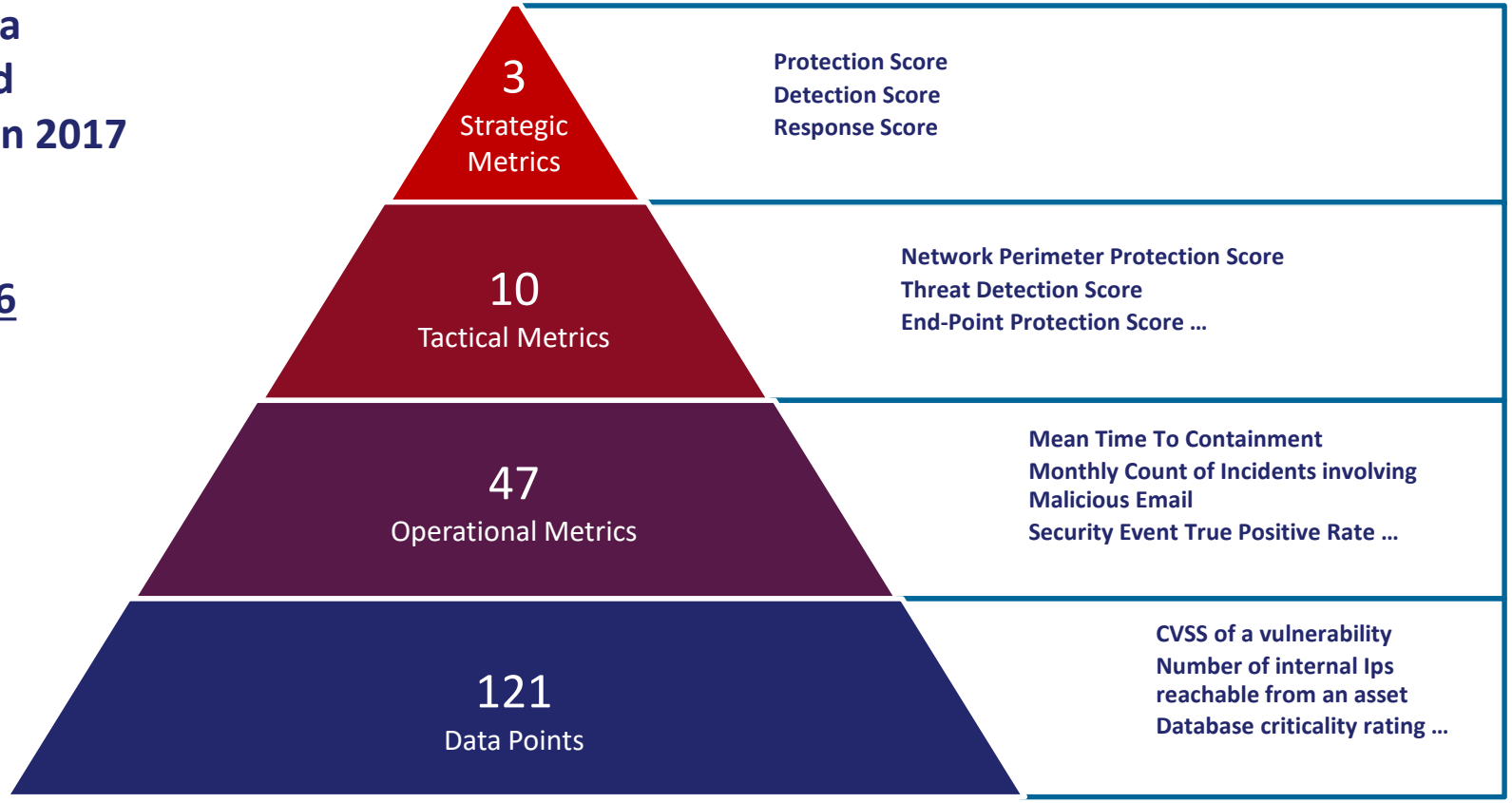
- Differentiate between your audiences: which ones do you report and to whom?
  - Consider the strategic, operational, risk and control level needs as a CISO
  - Ones that evidence impact on the strategic and business enablement needs of your C-Suite and Board
  - Your regulator / auditor
  - Other key external stakeholders (clients, insurance…)

Cyber Security Metrics for the Electric Sector

Full lists of metrics, data points, descriptions and formulae are included in 2017 Technical Update:

Product ID: 3002010426 (www.epri.com)

EE-ISAC



bpi BANK POLICY INSTITUTE

Metrics Linked To Your Framework (1)

Function	Category	Subcategory
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1: Physical devices and systems within the organization are inventoried**
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

How to Measure?

CMDB <-> what can be seen on the network.

Input Metric

Design and implement a system to generate the inventory of assets in an automated manner and identify anomalies

Output Metric

Critical assets

Green: 100%, Amber: 80%, Red: <80%

Non-critical assets

Green: 90%, Amber: 50%, Red: <50%

Impact Metric

Number of identified rogue devices.

Metrics Linked To Your Framework (2)

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
	DE.DP-2: Detection activities comply with all applicable requirements
	DE.DP-3: Detection processes are tested
	DE.DP-4: Event detection information is communicated
	DE.DP-5: Detection processes are continuously improved

How to Measure?

Results of Red Team exercises.

Input Metric

Design and implement a process to test the effectiveness of prevention and detection by carrying out Red Team exercises.

Output Metric

Number of issues found

% of success in capturing the DA creds

Impact Metric

Value of the damage avoided

Metrics Linked To Your Framework (3)

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
	DE.DP-2: Detection activities comply with all applicable requirements
	DE.DP-3: Detection processes are tested
	DE.DP-4: Event detection information is communicated
	DE.DP-5: Detection processes are continuously improved

How to Measure?

Identify the effectiveness of detective measures.

Input Metric

Design and implement detection measures based on identified risks/threats.
% of coverage of identified MITRE techniques.

Output Metric

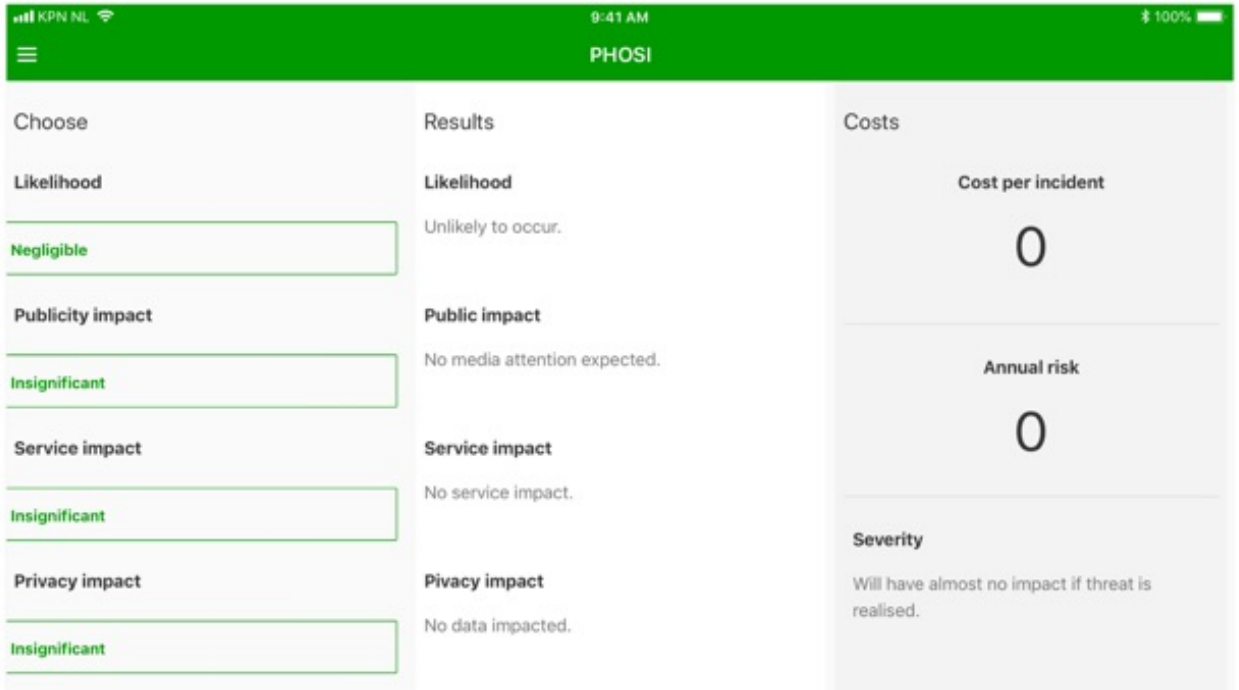
Number of real positives found

Impact Metric

% of incidents with real impact
Total value of the incidents with impact

KPN PHOSI (Potential Harm Of a Security Incident)

Calculate the potential cost of a security incident.



Library of Cyber Resilience Metrics

Dutch Payments Association (2017)

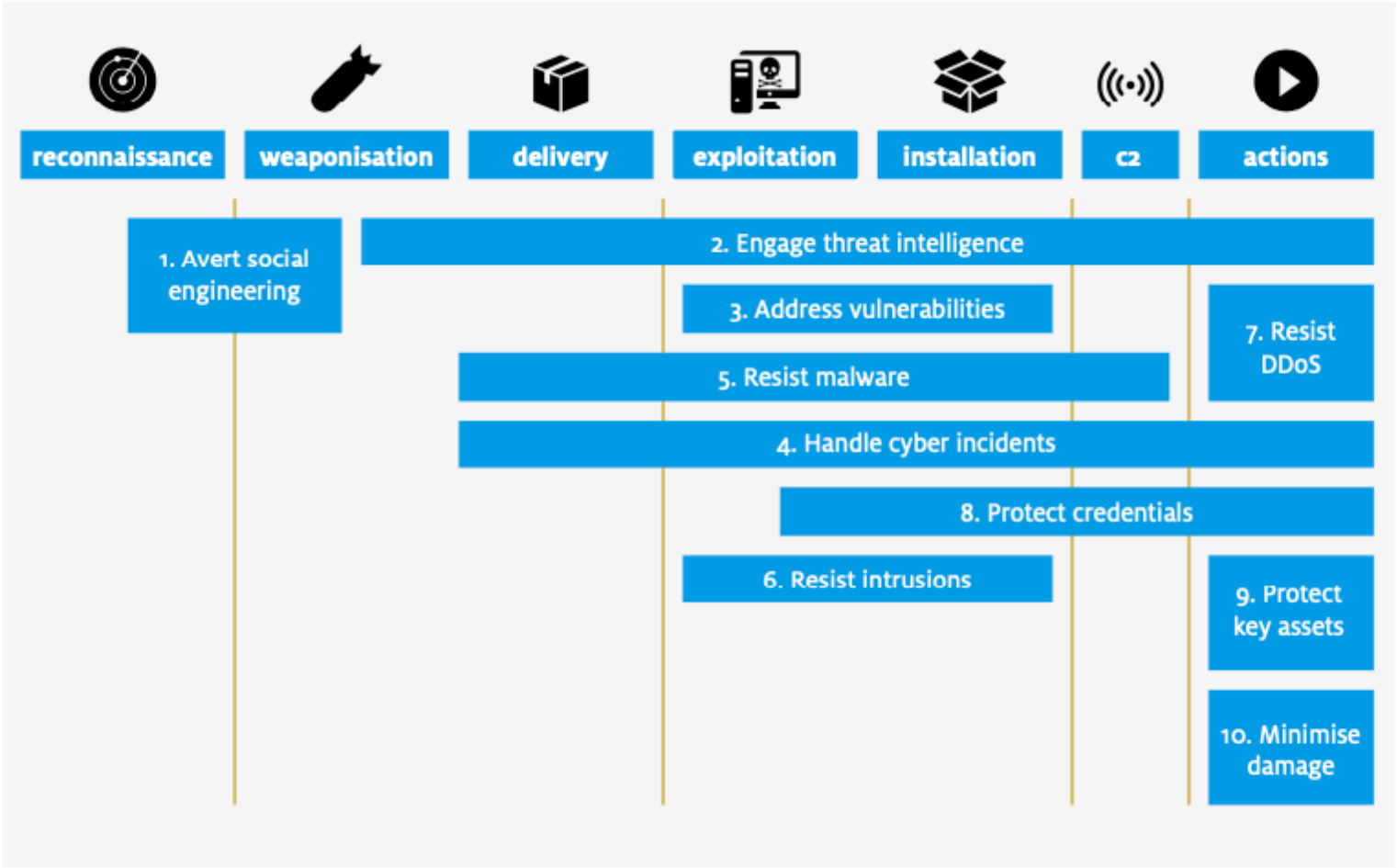


Figure 1: Core categories of cyber resilience metrics

Take Aways

- Increasing compliance obligations
- We spend more time than reasonable on reporting
- Cross-sector and cross-region very similar
- FSSCC framework aims to restore the balance
- It maps to other Frameworks and and to Regulations
- It is thorough and comprehensive
- Metrics can convert controls into a meaningful dashboard
- Integrate them into your business processes

"Apply" Slide

- Next week you should:
  - Have a look at the FSSCC Framework for inspiration
- In the first three months following this presentation you should:
  - Choose a Framework and map it to your stakeholders' references
  - Agree on relevant Metrics
- Within six months you should:
  - Gain and maintain C-Suite support
  - Gain and maintain support from your auditor/regulator

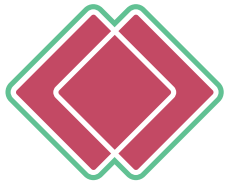
References

- FSSCC Financial Sector Cybersecurity Profile
- How To Steer Cybersecurity With Only One KPI (Jan Nys, KBC)
- Cyber security metrics for the electric sector (EPRI)
- Library of Cyber Resilience Metrics (Dutch Payments Association)
- KPN CISO App

RSAConference2020

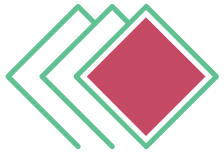
Appendices

Appendix: Rigor of FSSCC Cybersecurity Profile development approach



Syntactic mapping

Analyzes the *linguistic* meaning of the reference document element and framework element to develop the conceptual comparison set.



Semantic mapping

Analyzes the *contextual* meaning of the reference document element and framework element to develop the conceptual comparison set.

Functional mapping

Analyzes the *functions* of the reference document element and framework element to develop the conceptual comparison sets.

- Source: Cybersecurity Framework Online Informative References (OLIR): Specification for Completing the OLIR Template (NISTIR 8204)

Appendix: Syntactic mapping - uses literal analysis or translates the two elements

Financial Service Profile: GV.AU-2.1

A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.

FFIEC CAT: Domain 1, Audit

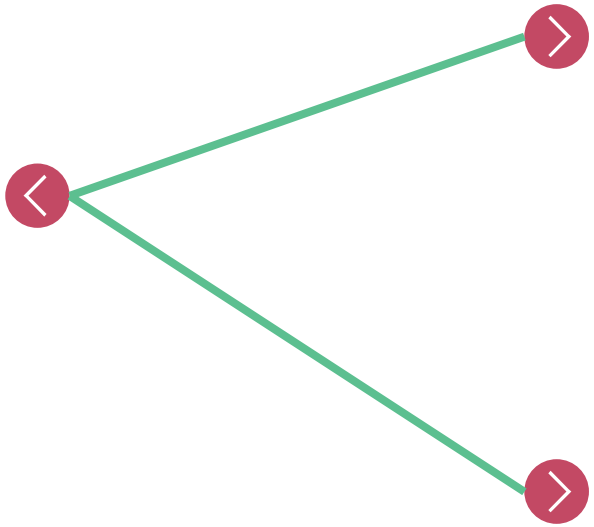
A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.

Source: Cybersecurity Framework Online Informative References (OLIR): Specification for Completing the OLIR Template (NISTIR 8204), FSP 1.0

Appendix: Semantic mapping - interprets or transliterates the language within the two elements

Financial Service Profile: PR.AT-1.1

All personnel (full-time or part-time; permanent, temporary or contract) receive periodic cybersecurity awareness training, as permitted by law.



ISO/IEC 27001:2013: A.7.2.2

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

ISO/IEC 27001:2013: A12.2.1

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

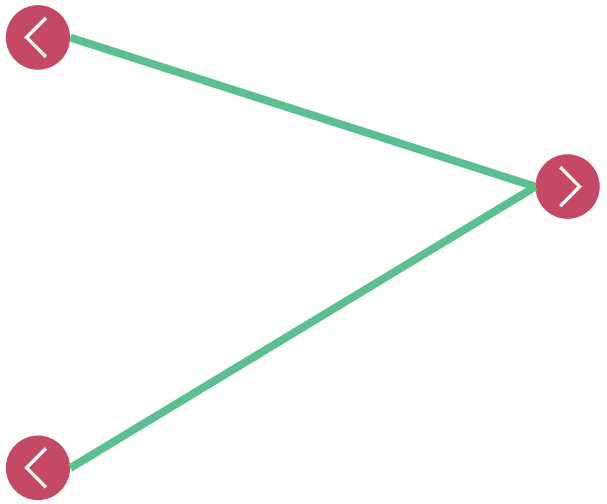
Appendix: Functional mapping - transposes the functional meaning of the two elements

Financial Service Profile: PR.AC-7.2

Based on the risk level of a given transaction, the organization has defined and implemented authentication requirements, such as including implementing multi-factor, out-of-band authentication for high risk transactions.

Financial Service Profile: DE.CM-4.1

The organization implements and manages appropriate tools to detect and block malware from infecting networks and systems.



HKMA-CRAF: 3.2.4 Customer Access Mgmt

Controls are in place to prevent malware and man-in-the-middle attacks for customer authentication in high-risk transactions.

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

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

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

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

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

Appendix: Impact Tiering Questionnaire – An Example

Example Off-Ramp for Impact Tier 1

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

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

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

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

Legend

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

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

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

Appendix: Regulatory Complexity Example with Respect to Third Party Oversight

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

bpi BANK POLICY INSTITUTE