Today's State of Global Protection

Wealth[1]

2018 global economy estimated to be **$86 Trillion**

Internet Connected[2]

As of **June 2019**, there were **4,5B** people **connected** to the **Internet**
A **59%** penetration, based on a population of **7,7B**

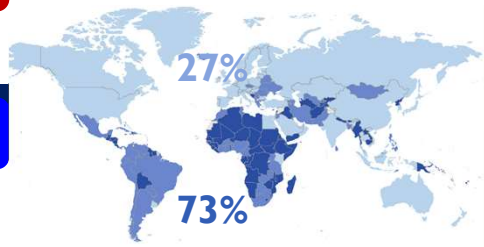
Not Sustainable

2019 Global Risks Report[3] According to the World Economic Forum

Identifies **Cyber** as the **4th** greatest risk facing the world

How well are we Protected? According to the **2018** ITU Global **Cybersecurity Index**[4]

27% or 1.2B people **think** they are protected
73% or **3.3B** people are under protected, with **45%** with little to no **protection**



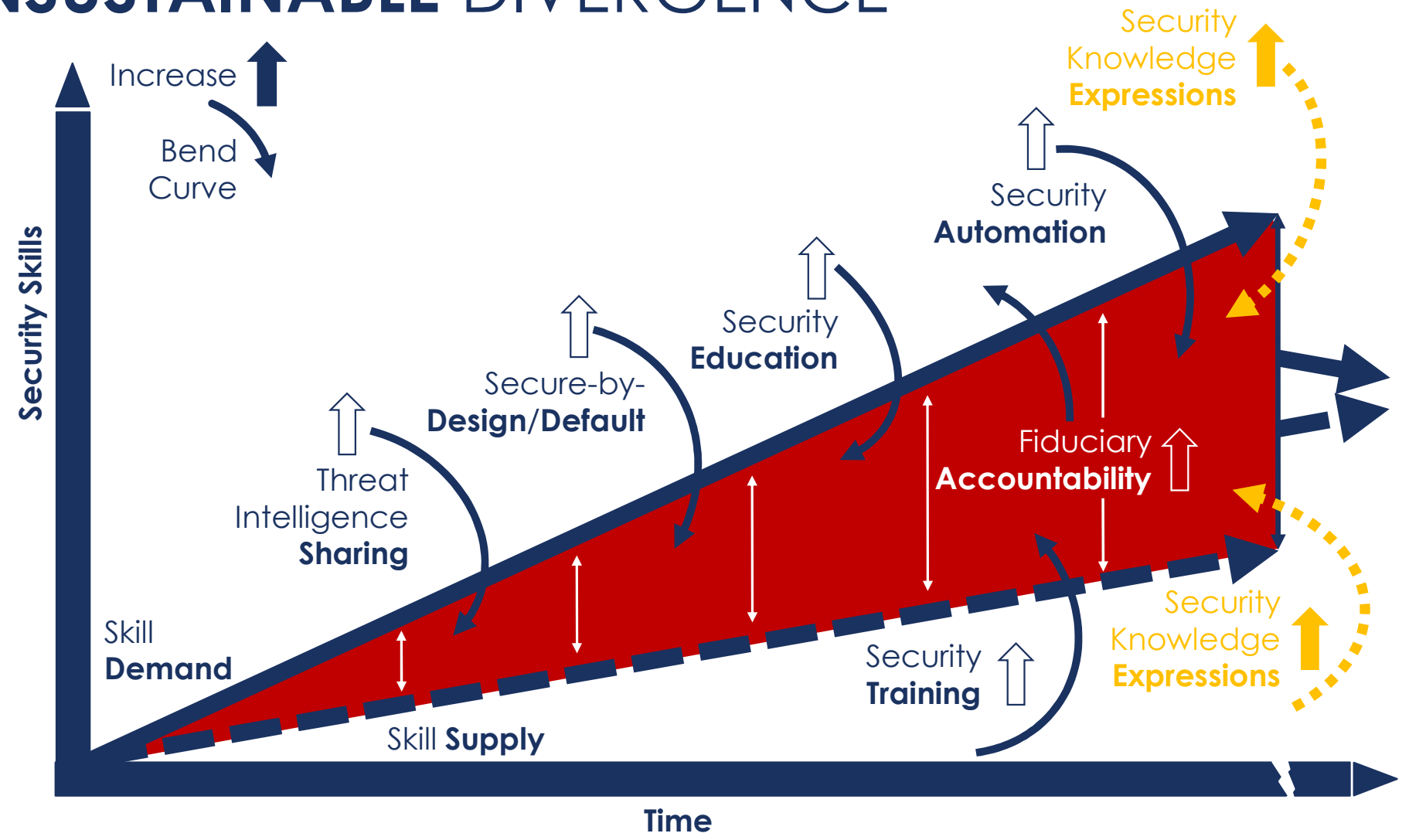
<< Protection >>

Security spending[5] estimated to be **$300B** by **2023**

27% or **1.2B** people who think they are protected will spend **~80%** of global **budget** estimated **$240B** 2023
Remaining **73%** or **3.3B** people that are under-protected will spend **~20%,** estimated **$60B** by 2023

1: https://howmuch.net/articles/the-world-economy-2018
2: June 2019 World Internet Usage & Population Statistics https://www.internetworldstats.com/stats.htm
3: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
4: Global Cybersecurity Index (GCI) 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
5: https://www.gminsights.com/pressrelease/cyber-security-market

UNSUSTAINABLE DIVERGENCE



SO MUCH SECURITY KNOWLEDGE CREATING **SO MUCH** COMPLEXITY ABOUT THE **SAME** TOPIC…

Regulations

Mandated Controls,
External Verification

Country specific, EU Directives

Standards

Recommended Controls,
Internal Validation

US NIST, ISO, ITU

Certifications

Mandated Controls,
External Accredited Verification

SIO Common Criteria,
US FedRamp

Associations

Recommended Controls,
Internal Validation

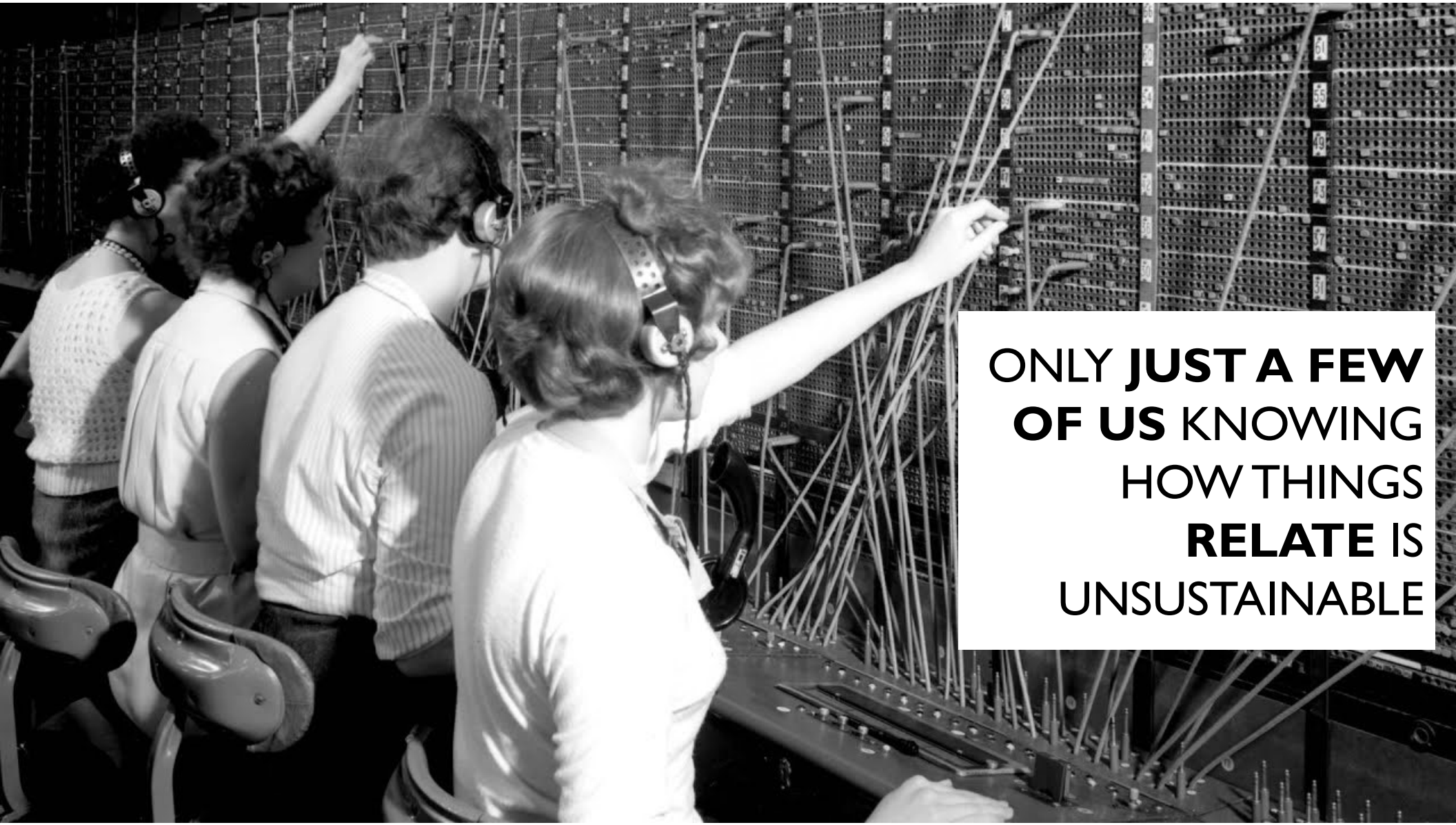
US Center Internet Security,
US HITRUST

Where does it all go?

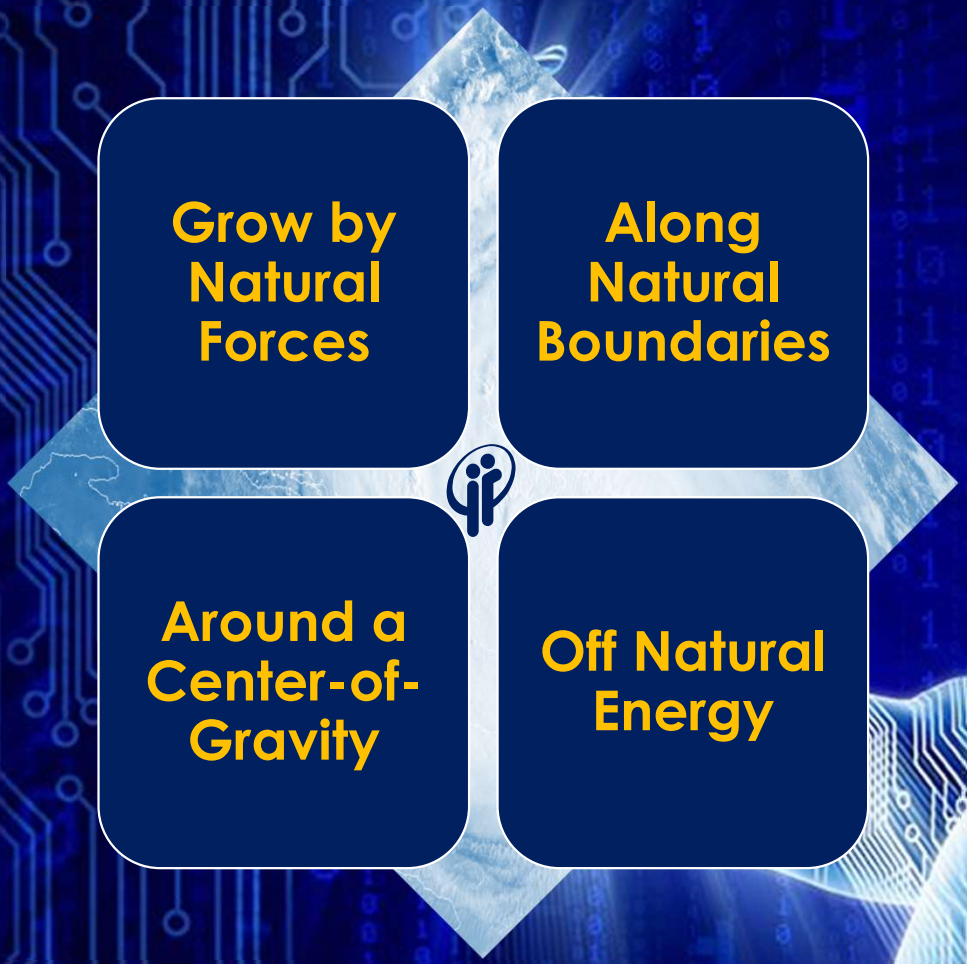
How does it all relate?

What does it all mean?

How do I … ?


ONLY **JUST A FEW OF US** KNOWING HOW THINGS **RELATE** IS UNSUSTAINABLE

Vision



For a capability to be sustainable, a seeding must **grow by natural forces**, crystalize **along natural boundaries**, develop momentum around a **center-of-gravity**, and feed off **natural energy**

Vision

The Genesis Program delivers new "all matters" security model & training Platform to Centers-of-Brainpower to Create & Exchange Security Value around the world


The **Digital** Protection **Divide** …
Those **who are** Protected & Those Who **are Now**

Internet-of-**Value** **Ecosystem**

Value **Creation**
*Anywhere - **from** the Edges*

Value **Consumption**
to the Edges

Digital Currency

Value Exchange **Friction** & **Loss**?

The **Struggle** to Protect

Internet-of -**Value**

Value **Creation** *Anywhere*

Value **Consumption** Somewhere Else

Value **Creation** Force

Value **Risk** Force

Value Creation "**is Threatened by**" Value Risk

Value Creation "**is Protected by**" Value Preservation

Value **Assurance** Force

Value Preservation "**is Validated by**" Value Assurance

Value **Preservation** Force

A **Need** for a **Rethink**?

Digital Currency: Standards, Laws, Regulations

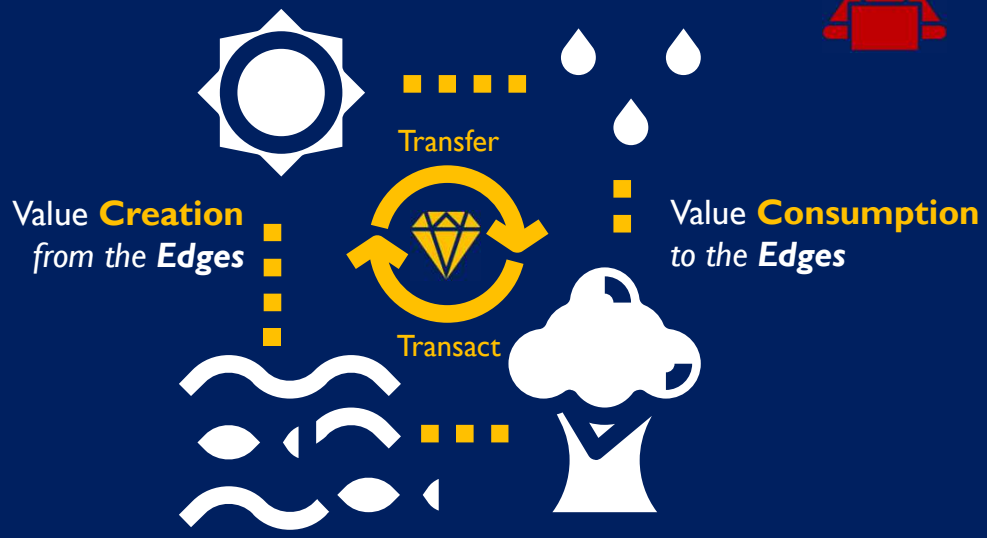
Ecosystem

Value **Creation** *from the **Edges***

Value **Consumption** *to the **Edges***

Financial Inclusion

Value **Stolen** *Anytime from Anywhere*



Value **Creation** *from the **Edges***

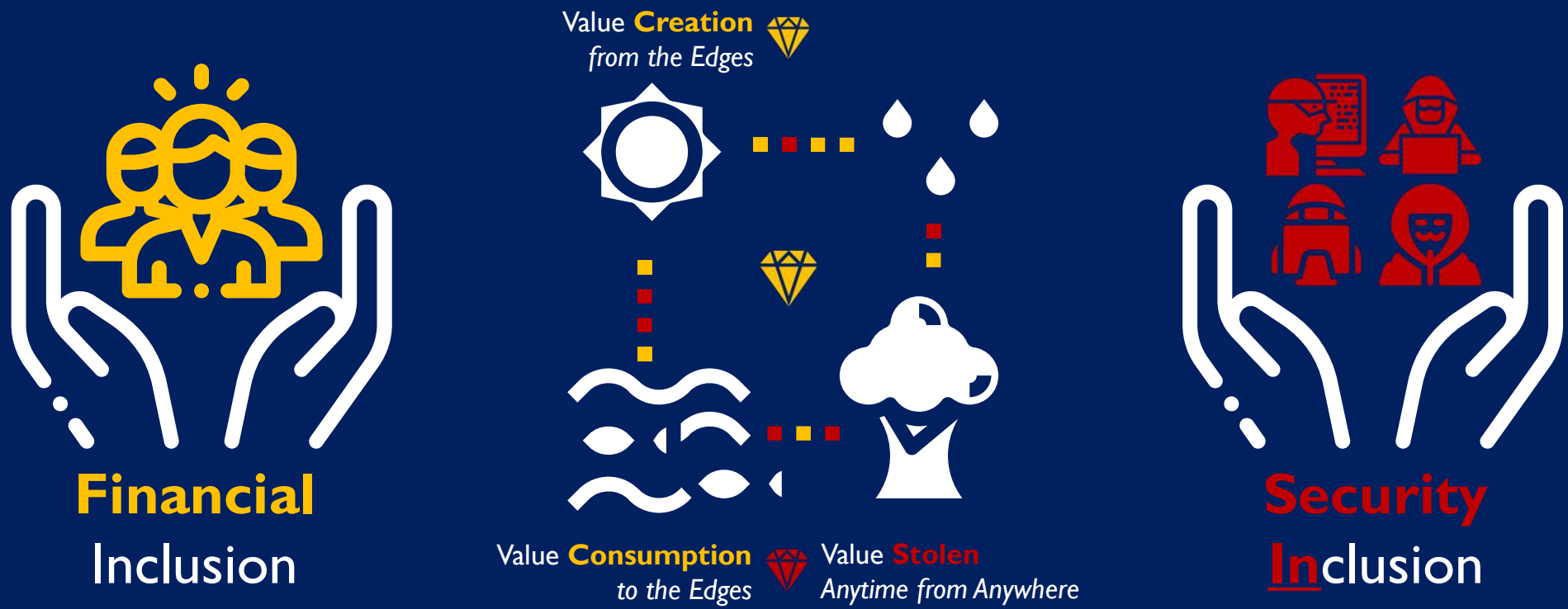
Value **Consumption** *to the **Edges***

DC Wild, Wild West

Loss of **Confidence**

Digital Currency: Standards, Laws, Regulations

Loss of **Confidence** <<< Value **Consumption**



For Digital Currency, the Need for **Assurance**

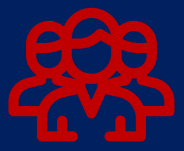
Value **Creation** *from the **Edges***

Value **Consumption** *to the **Edges***

Financial Inclusion

I created Value!

I purchased Value!



Who?

Identification for **Attribution,** Ownership
- Identifiers
- Access
- Authorization

Control = Ownership

What Value was **created?**

What Value was **purchased?**

What?

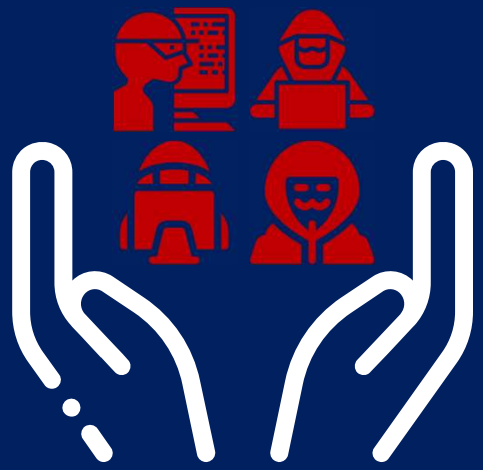
Cryptography for
- Immutability
- Confidentiality
- Authenticity
- Attribution
- Proofs
- Distributed Trust

I own Value!

Transact Away!

Assurance for:
- Trust
- Liability
- Warranties

Value **Stolen** *Anytime from Anywhere*



Security **In**clusion

The International Telecommunications Union - Standardization

193
Member States

150
Academia

170
Associates

550
Sector Member

a

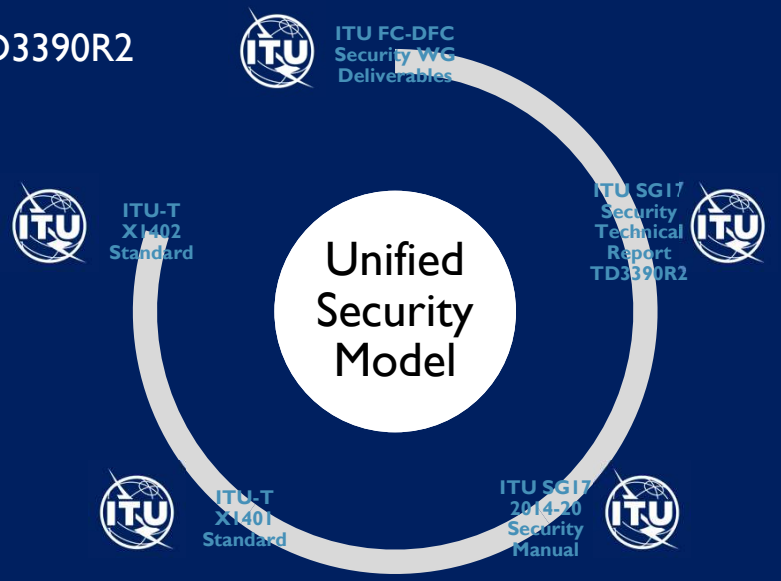
United Nations

specialized agency for Information & Communication Technologies, based in Geneva Switzerland

On the path to Standardization

Unified Security Model published by ITU Study Group 17: Security:

- ITU Focus Group – Cryptocurrencies & Digital Fiat Currency: Protection Assurance for Digital Currencies
- ITU SG17 Security: Technical Report Unified Security Model SG17-TD3390R2
- ITU SG17 Security Manual 2020: Section 11.5 Unified Security Model
- ITU-T X1401 Annex Security Threats to Distributed Ledger Technology Standard
- ITU-T X1402 Annex Security Framework for Distributed Ledger Technology Standard



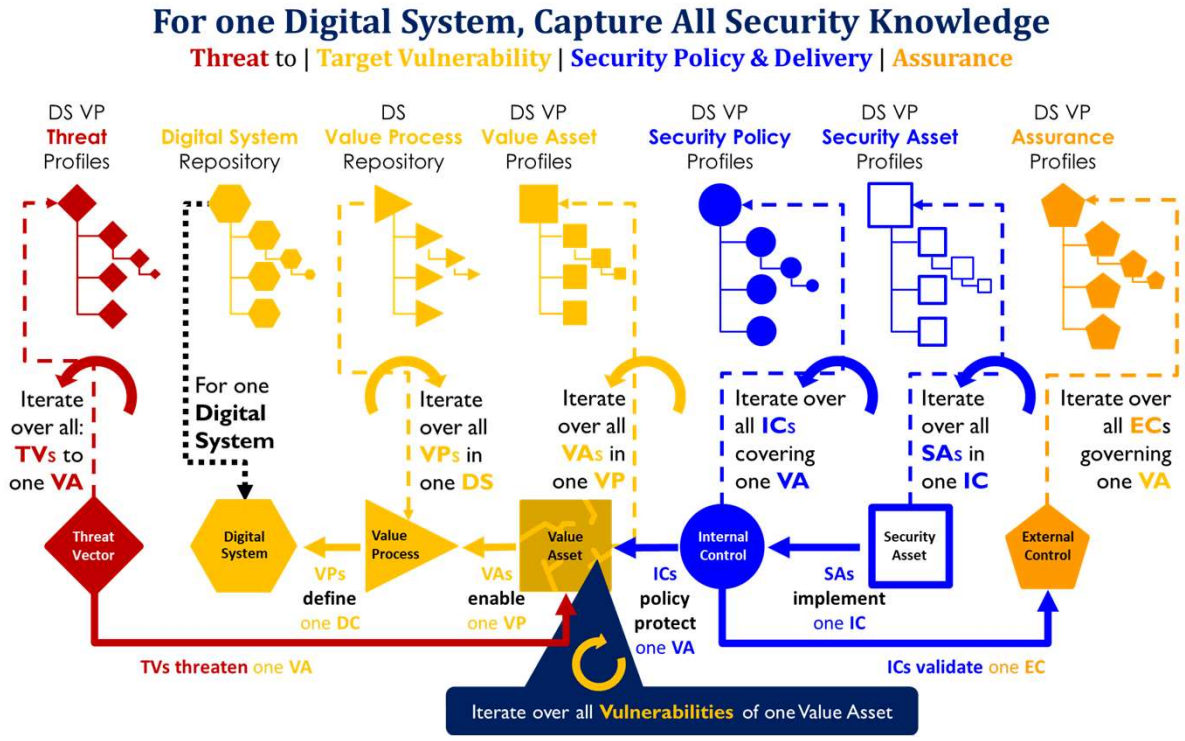
International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03 November 2020)

TR-USM
Unified security model (USM) – A neutral integrated system approach to cybersecurity



Target Evaluation Completeness Mechanism

For one Vulnerability of one Value Asset to
One Digital System Attack Surface

Scope: One Digital System

One Digital System Attack Surface Profile

Anchor: **One** Digital System — Iterate — **All** Value Processes of one Digital System

Scope: One Value Process

One Value Process Attack Surface Profiles

Anchor: **One** Value Process — Iterate — **All** Value Assets of one Value Process

Scope: One Value Asset

One Value Asset Attack Surface Profile

Anchor: **One** Value Asset — Iterate — **All** Vulnerabilities of one Value Asset

Scope: One Value Asset Vulnerability

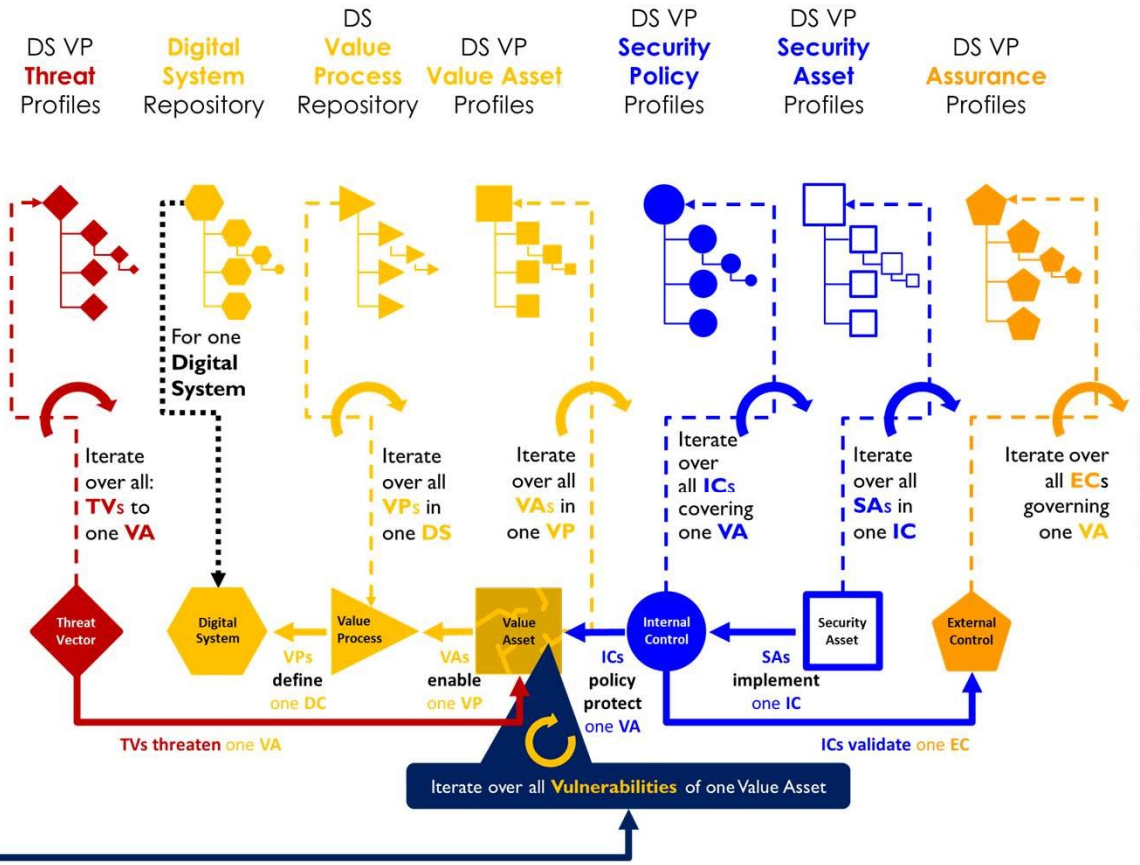
Single Expression: One Vulnerability

Anchor: **One** Value Asset Vulnerability:

For one Digital System, Capture All Security Knowledge

For one Vulnerability of one Value Asset, iterate over all vulnerabilities in all Value Assets,
all Value Assets in all Value Processes in one Digital System

Threat to | **Target Vulnerability** | **Security Policy & Delivery** | **Assurance**



Genesis Cybersecurity Program

Based on the

Unified Security Model

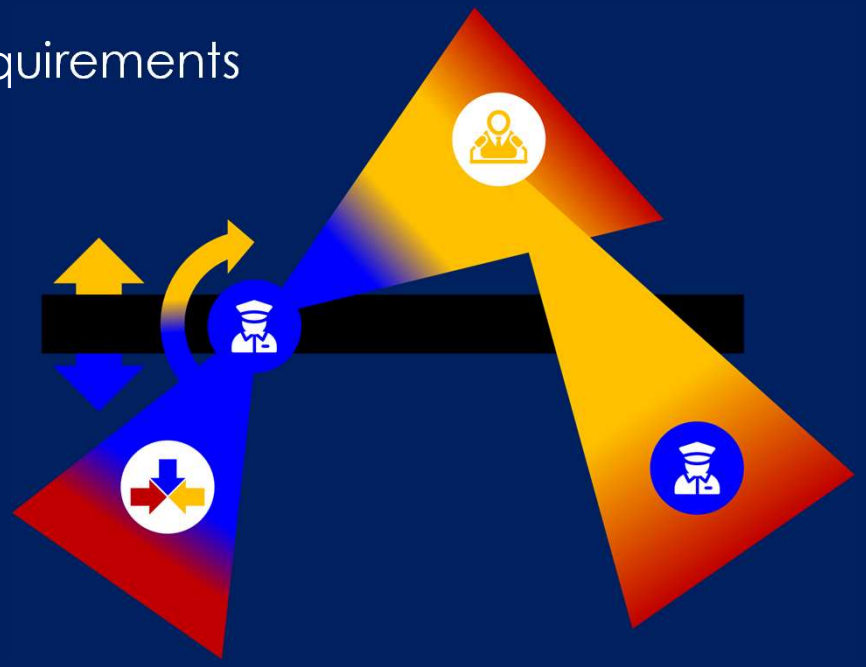
and modeling tool

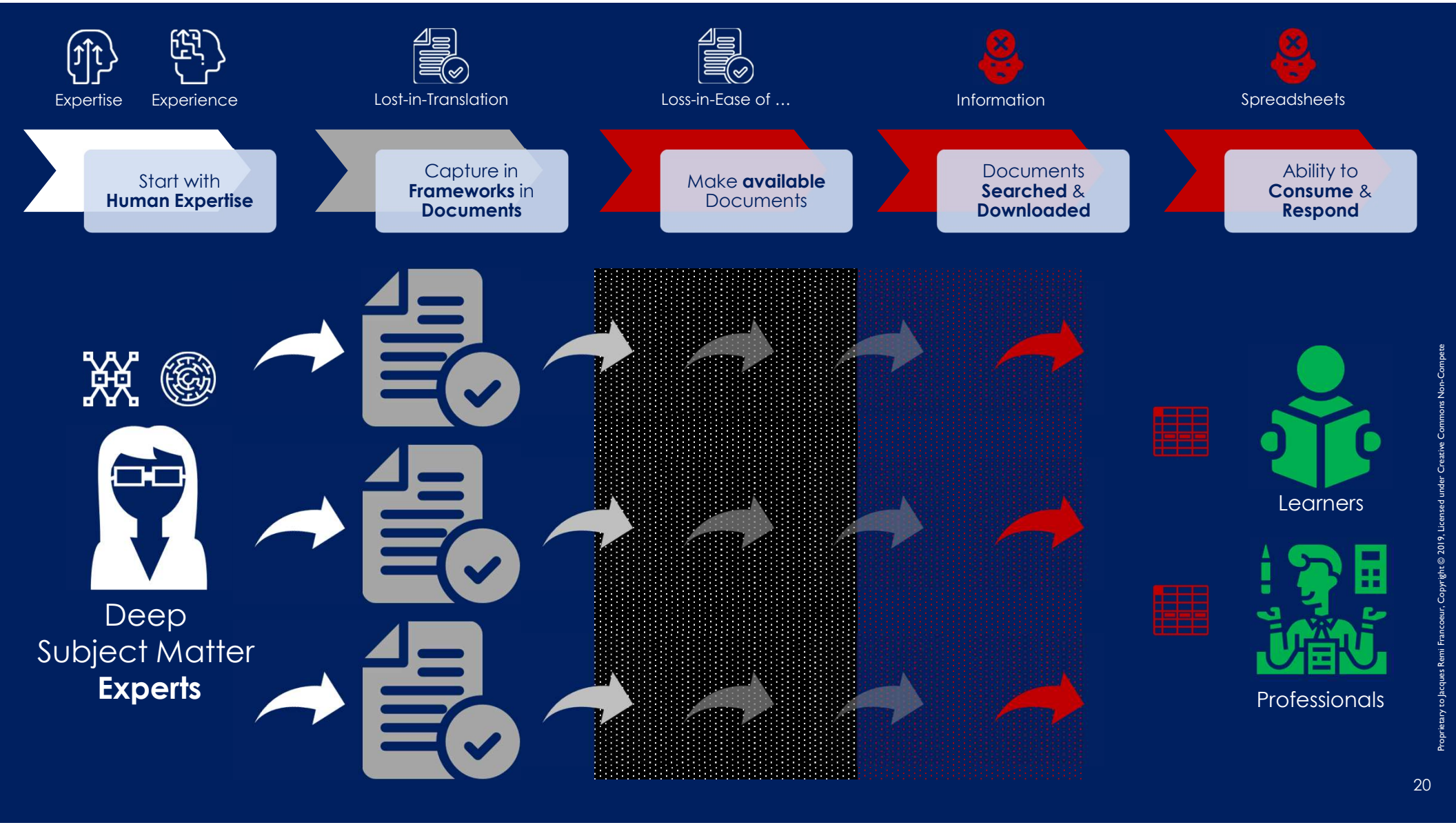
for

Institutionalizing Local & Sustainable Security Modeling & Training Capability

CHALLENGE: COMMUNICATE - **WHAT TO WHOM**

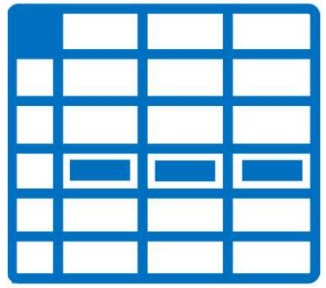
- **Do**: Explain | Present | Demonstrate | Assert
- **What**: **State-of-Control** & its fulfilment to Enterprise Objectives & Compliance Requirements
- To **Whom:**
  - To **Yourself** (CISO)
  - To **Enterprise** (Board, EC, etc.)
  - To **Auditors**
  - To **Regulators**
  - To **Examiners**
  - To **Certifiers**
- **When**, on a periodic basis
- **Why**, meet fiduciary duty-of-care to customers, investors, partners



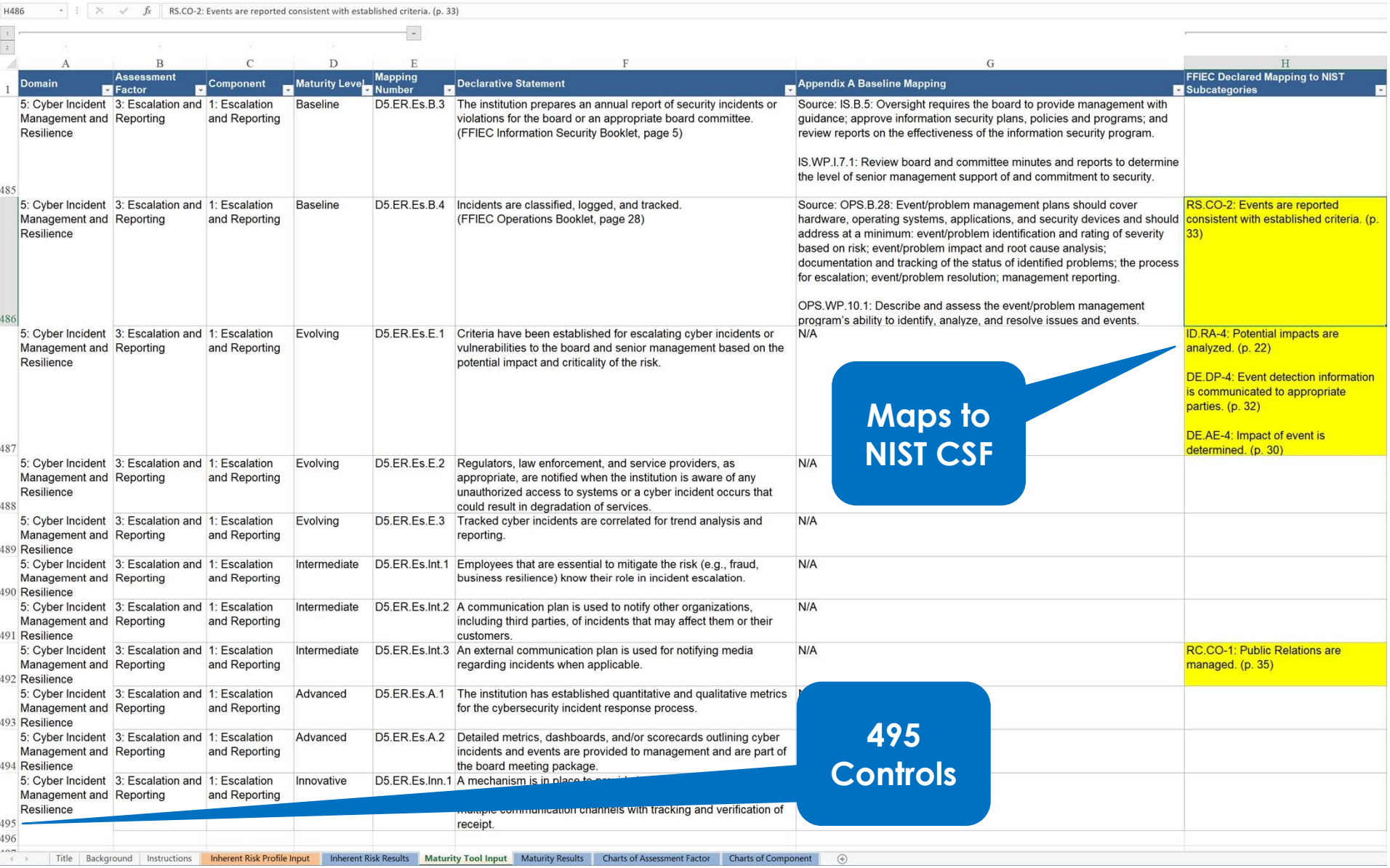


Financial Services Sector Coordinating Council

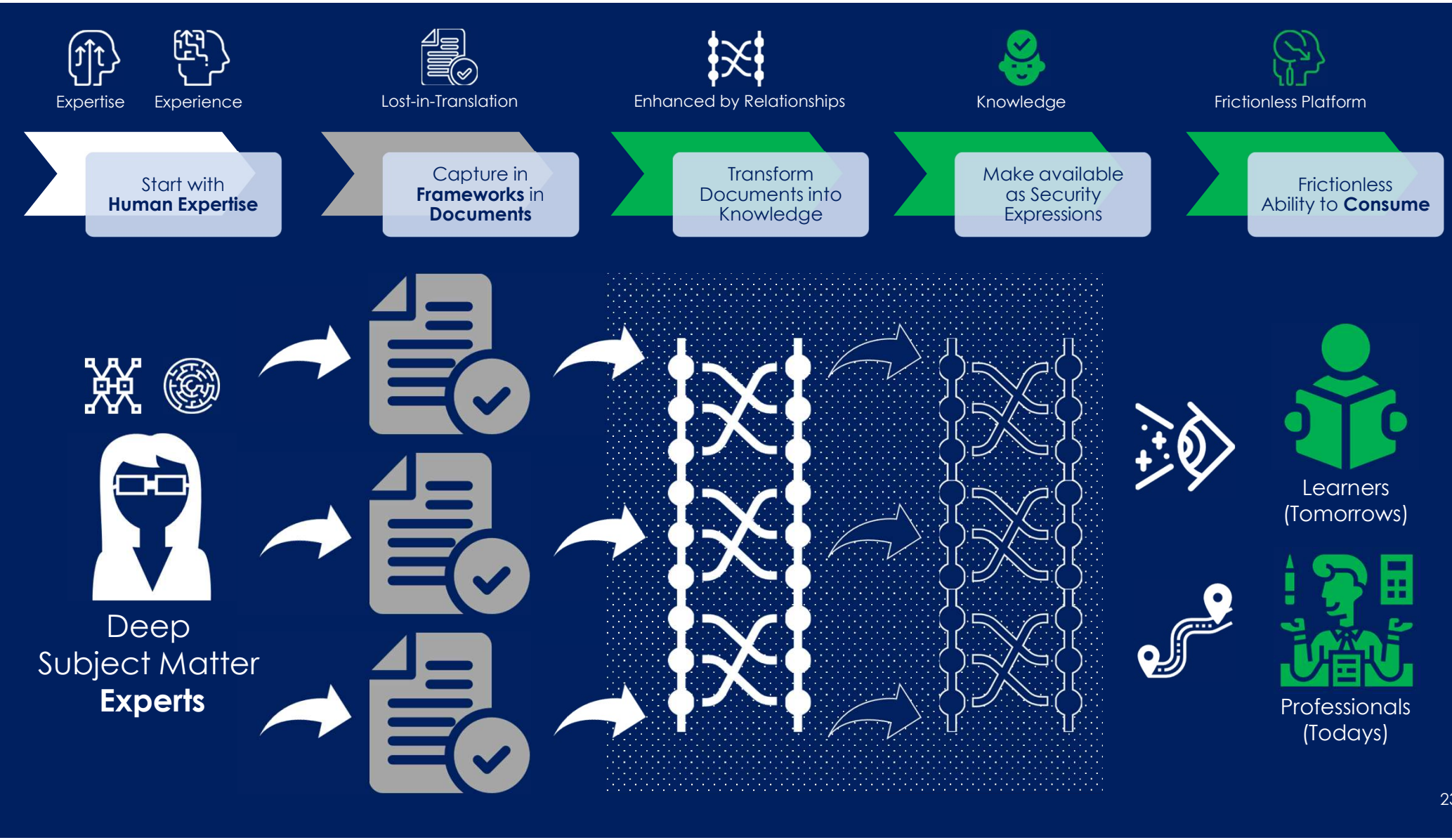
for Critical Infrastructure Protection and Homeland Security

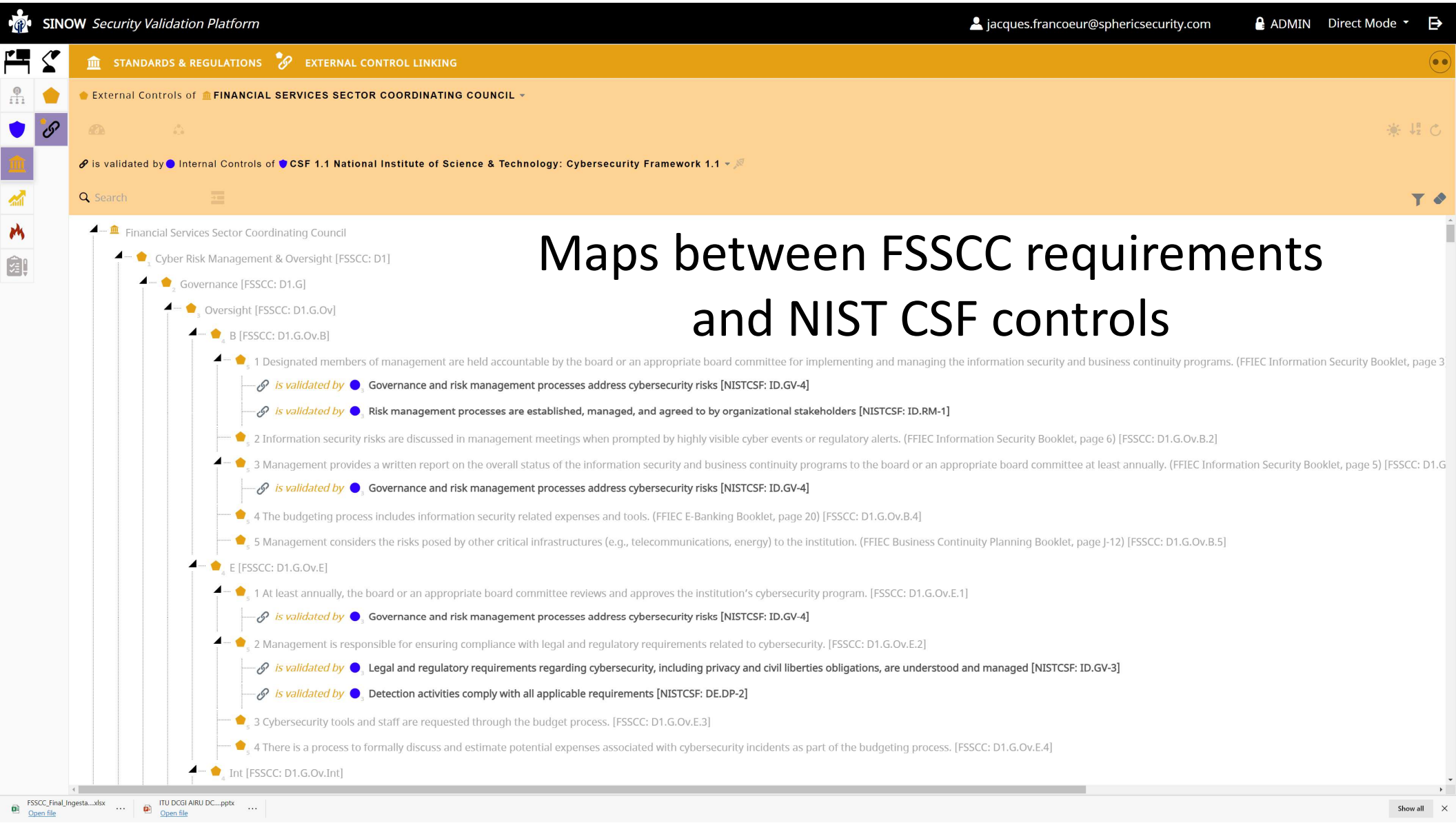


Domain	Domain Maturity	Assessment Factor	Assessment Factor Maturity	Component	Baseline	Evolving	Intermediate	Advanced	Innovative	Assessed Maturity Level
1: Cyber Risk Management & Oversight	Incomplete	1: Governance	Incomplete	1:Oversight	0%	0%	0%	0%	0%	Incomplete
				2: Strategy / Policies	0%	0%	0%	0%	0%	Incomplete
				3: IT Asset Management	0%	0%	0%	0%	0%	Incomplete
		2: Risk Management	Incomplete	1: Risk Management Program	0%	0%	0%	0%	0%	Incomplete
				2: Risk Assessment	0%	0%	0%	0%	0%	Incomplete
				3: Audit	0%	0%	0%	0%	0%	Incomplete
		3: Resources	Incomplete	1: Staffing	0%	0%	0%	0%	0%	Incomplete
		4: Training & Culture	Incomplete	1: Training	0%	0%	0%	0%	0%	Incomplete
				2: Culture	0%	0%	0%	0%	0%	Incomplete
2: Threat Intelligence & Collaboration	Incomplete	1: Threat Intelligence	Incomplete	1: Threat Intelligence and Information	0%	0%	0%	0%	0%	Incomplete
		2: Monitoring & Analyzing	Incomplete	1: Monitoring and Analyzing	0%	0%	0%	0%	0%	Incomplete
		3: Information Sharing	Incomplete	1: Information Sharing	0%	0%	0%	0%	0%	Incomplete
3: Cybersecurity Controls	Incomplete	1: Preventative Controls	Incomplete	1: Infrastructure Management	0%	0%	0%	0%	0%	Incomplete
				2: Access and Data Management	0%	0%	0%	0%	0%	Incomplete
				3: Device / End-Point Security	0%	0%	0%	0%	0%	Incomplete
				4: Secure Coding	0%	0%	0%	0%	0%	Incomplete
		2: Detective Controls	Incomplete	1: Threat and Vulnerability Detection	0%	0%	0%	0%	0%	Incomplete
				2: Anomalous Activity Detection	0%	0%	0%	0%	0%	Incomplete
				3: Event Detection	0%	0%	0%	0%	0%	Incomplete
		3: Corrective Controls	Incomplete	1: Patch Management	0%	0%	0%	0%	0%	Incomplete
				2: Remediation	0%	0%	0%	0%	0%	Incomplete
4: External Dependency Management	Incomplete	1: Connections	Incomplete	1: Connections	0%	0%	0%	0%	0%	Incomplete
		2: Relationship Management	Incomplete	1: Due Diligence	0%	0%	0%	0%	0%	Incomplete
				2: Contracts	0%	0%	0%	0%	0%	Incomplete
				3: Ongoing Monitoring	0%	0%	0%	0%	0%	Incomplete
5: Cyber Incident Management and Resilience	Incomplete	1: Incident Resilience Planning and Strategy	Incomplete	1: Planning	0%	0%	0%	0%	0%	Incomplete
				2: Testing	0%	0%	0%	0%	0%	Incomplete
		2: Detection, Response, and Mitigation	Incomplete	1: Detection	0%	0%	0%	0%	0%	Incomplete
				2: Response and Mitigation	0%	0%	0%	0%	0%	Incomplete
		3: Escalation and Reporting	Incomplete	1: Escalation and Reporting	0%	0%	0%	0%	0%	Incomplete

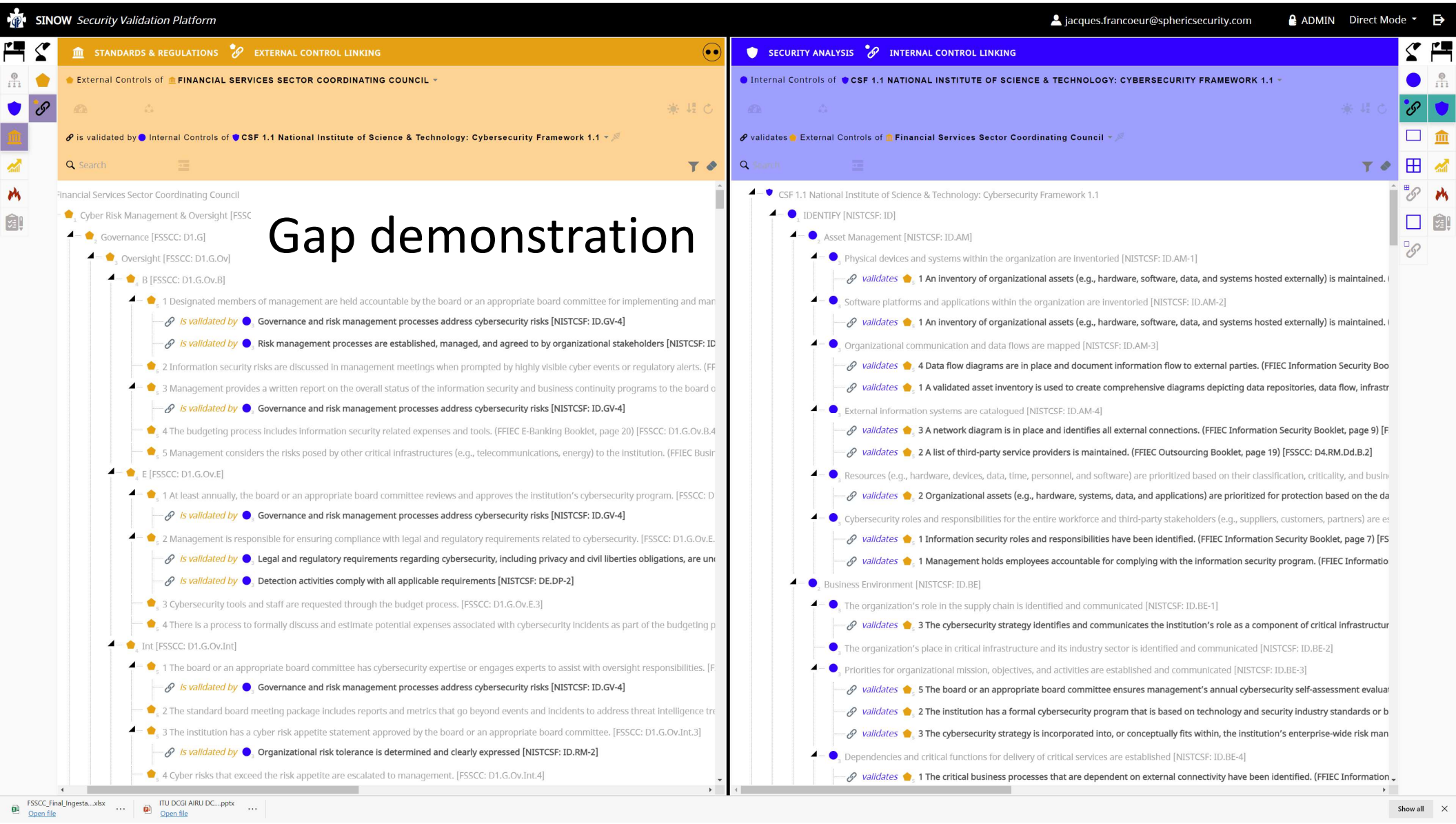


	A	B	C	D	E	F	G	H
1	Domain	Assessment Factor	Component	Maturity Level	Mapping Number	Declarative Statement	Appendix A Baseline Mapping	FFIEC Declared Mapping to NIST Subcategories
485	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Baseline	D5.ER.Es.B.3	The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. (FFIEC Information Security Booklet, page 5)	Source: IS.B.5: Oversight requires the board to provide management with guidance; approve information security plans, policies and programs; and review reports on the effectiveness of the information security program. IS.WP.I.7.1: Review board and committee minutes and reports to determine the level of senior management support of and commitment to security.	
486	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Baseline	D5.ER.Es.B.4	Incidents are classified, logged, and tracked. (FFIEC Operations Booklet, page 28)	Source: OPS.B.28: Event/problem management plans should cover hardware, operating systems, applications, and security devices and should address at a minimum: event/problem identification and rating of severity based on risk; event/problem impact and root cause analysis; documentation and tracking of the status of identified problems; the process for escalation; event/problem resolution; management reporting. OPS.WP.10.1: Describe and assess the event/problem management program's ability to identify, analyze, and resolve issues and events.	RS.CO-2: Events are reported consistent with established criteria. (p. 33)
487	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Evolving	D5.ER.Es.E.1	Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.	N/A	ID.RA-4: Potential impacts are analyzed. (p. 22) DE.DP-4: Event detection information is communicated to appropriate parties. (p. 32) DE.AE-4: Impact of event is determined. (p. 30)
488	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Evolving	D5.ER.Es.E.2	Regulators, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorized access to systems or a cyber incident occurs that could result in degradation of services.	N/A	
489	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Evolving	D5.ER.Es.E.3	Tracked cyber incidents are correlated for trend analysis and reporting.	N/A	
490	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Intermediate	D5.ER.Es.Int.1	Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation.	N/A	
491	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Intermediate	D5.ER.Es.Int.2	A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers.	N/A	
492	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Intermediate	D5.ER.Es.Int.3	An external communication plan is used for notifying media regarding incidents when applicable.	N/A	RC.CO-1: Public Relations are managed. (p. 35)
493	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Advanced	D5.ER.Es.A.1	The institution has established quantitative and qualitative metrics for the cybersecurity incident response process.	N/A	
494	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Advanced	D5.ER.Es.A.2	Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.	N/A	
495	5: Cyber Incident Management and Resilience	3: Escalation and Reporting	1: Escalation and Reporting	Innovative	D5.ER.Es.Inn.1	A mechanism is in place to pro[illegible] multiple communication channels with tracking and verification of receipt.	N/A	
496								





Maps between FSSCC requirements and NIST CSF controls


SINOW Security Validation Platform
jacques.francoeur@sphericsecurity.com
ADMIN
Direct Mode
STANDARDS & REGULATIONS
EXTERNAL CONTROL LINKING
External Controls of FINANCIAL SERVICES SECTOR COORDINATING COUNCIL
is validated by Internal Controls of CSF 1.1 National Institute of Science & Technology: Cybersecurity Framework 1.1
Search
Financial Services Sector Coordinating Council
Cyber Risk Management & Oversight [FSSC
Governance [FSSCC: D1.G]
Oversight [FSSCC: D1.G.Ov]
B [FSSCC: D1.G.Ov.B]
1 Designated members of management are held accountable by the board or an appropriate board committee for implementing and mar
Is validated by Governance and risk management processes address cybersecurity risks [NISTCSF: ID.GV-4]
Is validated by Risk management processes are established, managed, and agreed to by organizational stakeholders [NISTCSF: ID
2 Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FF
3 Management provides a written report on the overall status of the information security and business continuity programs to the board o
Is validated by Governance and risk management processes address cybersecurity risks [NISTCSF: ID.GV-4]
4 The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20) [FSSCC: D1.G.Ov.B.4
5 Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Busir
E [FSSCC: D1.G.Ov.E]
1 At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. [FSSCC: D
Is validated by Governance and risk management processes address cybersecurity risks [NISTCSF: ID.GV-4]
2 Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. [FSSCC: D1.G.Ov.E.
Is validated by Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are un
Is validated by Detection activities comply with all applicable requirements [NISTCSF: DE.DP-2]
3 Cybersecurity tools and staff are requested through the budget process. [FSSCC: D1.G.Ov.E.3]
4 There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting p
Int [FSSCC: D1.G.Ov.Int]
1 The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities. [F
Is validated by Governance and risk management processes address cybersecurity risks [NISTCSF: ID.GV-4]
2 The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence tr
3 The institution has a cyber risk appetite statement approved by the board or an appropriate board committee. [FSSCC: D1.G.Ov.Int.3]
Is validated by Organizational risk tolerance is determined and clearly expressed [NISTCSF: ID.RM-2]
4 Cyber risks that exceed the risk appetite are escalated to management. [FSSCC: D1.G.Ov.Int.4]
Gap demonstration
SECURITY ANALYSIS
INTERNAL CONTROL LINKING
Internal Controls of CSF 1.1 NATIONAL INSTITUTE OF SCIENCE & TECHNOLOGY: CYBERSECURITY FRAMEWORK 1.1
validates External Controls of Financial Services Sector Coordinating Council
Search
CSF 1.1 National Institute of Science & Technology: Cybersecurity Framework 1.1
IDENTIFY [NISTCSF: ID]
Asset Management [NISTCSF: ID.AM]
Physical devices and systems within the organization are inventoried [NISTCSF: ID.AM-1]
validates 1 An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
Software platforms and applications within the organization are inventoried [NISTCSF: ID.AM-2]
validates 1 An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
Organizational communication and data flows are mapped [NISTCSF: ID.AM-3]
validates 4 Data flow diagrams are in place and document information flow to external parties. (FFIEC Information Security Boo
validates 1 A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastr
External information systems are catalogued [NISTCSF: ID.AM-4]
validates 3 A network diagram is in place and identifies all external connections. (FFIEC Information Security Booklet, page 9) [F
validates 2 A list of third-party service providers is maintained. (FFIEC Outsourcing Booklet, page 19) [FSSCC: D4.RM.Dd.B.2]
Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and busin
validates 2 Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the da
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are es
validates 1 Information security roles and responsibilities have been identified. (FFIEC Information Security Booklet, page 7) [FS
validates 1 Management holds employees accountable for complying with the information security program. (FFIEC Informatio
Business Environment [NISTCSF: ID.BE]
The organization's role in the supply chain is identified and communicated [NISTCSF: ID.BE-1]
validates 3 The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructur
The organization's place in critical infrastructure and its industry sector is identified and communicated [NISTCSF: ID.BE-2]
Priorities for organizational mission, objectives, and activities are established and communicated [NISTCSF: ID.BE-3]
validates 5 The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluat
validates 2 The institution has a formal cybersecurity program that is based on technology and security industry standards or b
validates 3 The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk man
Dependencies and critical functions for delivery of critical services are established [NISTCSF: ID.BE-4]
validates 1 The critical business processes that are dependent on external connectivity have been identified. (FFIEC Information
FSSCC_Final_Ingesta....xlsx
Open file
ITU DCGI AIRU DC....pptx
Open file
Show all

Security Control Expressions

Unique

Unambiguous

Precise

“Re-think” how you “see” security

Much is Different

Simplicity

Much is Same