

# Key Ecosystem Challenges

**CRYPTO-  
CURRENCY**

...

**CBDC**

...

**DIGITAL FIAT  
CURRENCY**

## Protecting Digital Currencies

Presented by:  Jacques Francoeur B.A.Sc., M.A.Sc., MBA  
**Chief Scientist & Founder**, Security Inclusion Now USA



USA Delegate (2018,19,20) Security Expert & Contributor  
International Telecommunications Union Standardization, Study Group 17: Security  
Expert Network Member World Economic Forum, Blockchain Security

# Today's State of Global Protection

## Wealth<sup>1</sup>

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

## Internet Connected<sup>2</sup>

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

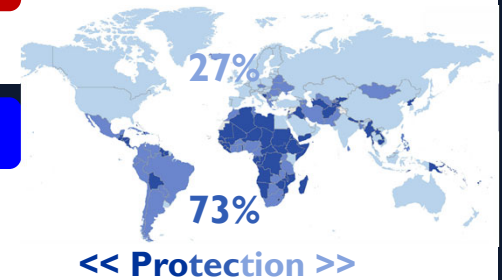


## 2019 Global Risks Report<sup>3</sup> According to the World Economic Forum

Identifies **Cyber** as the **4<sup>th</sup>** greatest risk facing the world

## How well are we Protected? According to the 2018 ITU Global Cybersecurity Index<sup>4</sup>

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



## Security spending<sup>5</sup> 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>

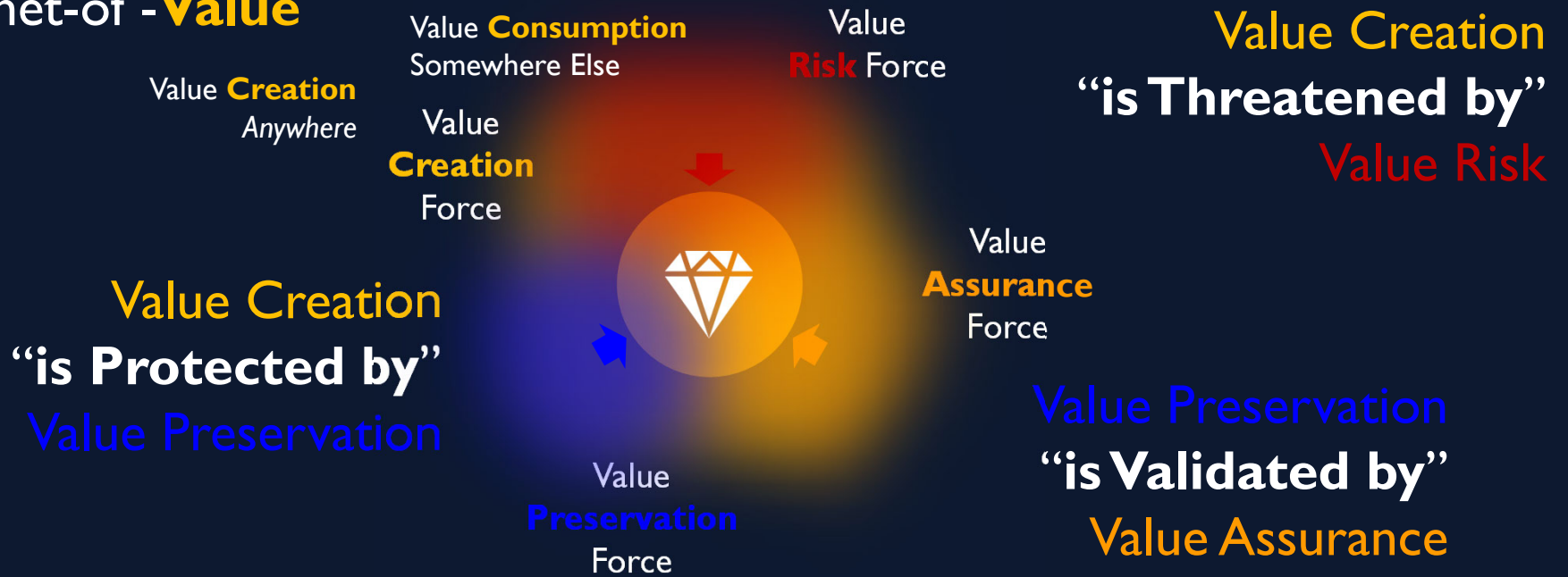
3: [http://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2019.pdf](http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf)

4: Global Cybersecurity Index (GCI) 2018 [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](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>

# The **Struggle** to Protect

Internet-of -**Value**



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

# Internet-of-Value Ecosystem

*Supply*

*Demand*

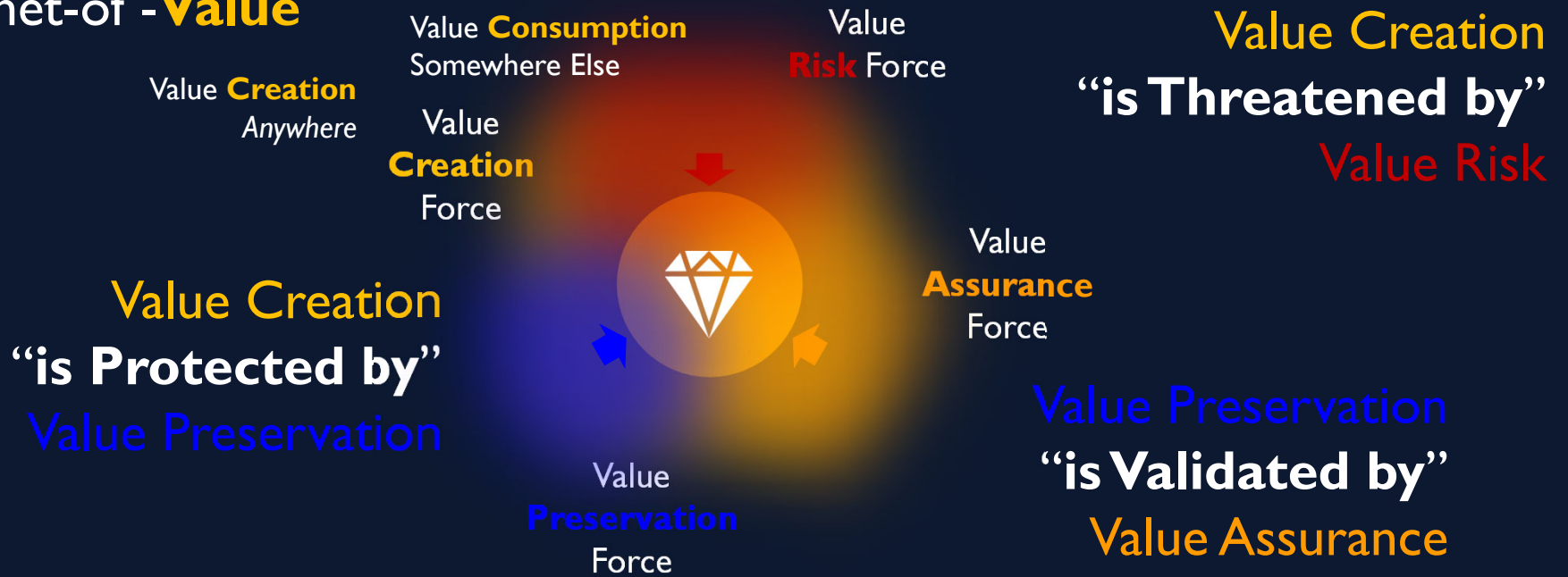


## Digital Currency

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

# The **Struggle** to Protect

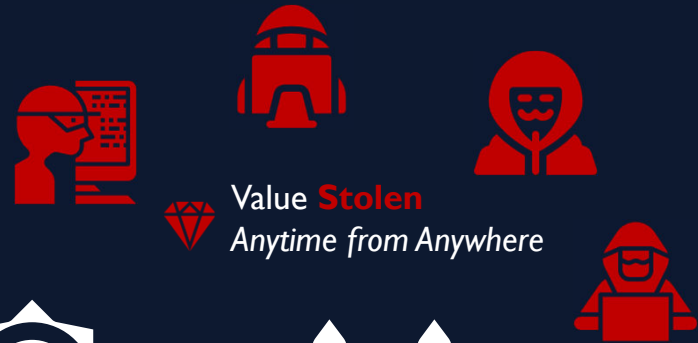
Internet-of -**Value**



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

# Digital Currency: Standards, Laws, Regulations Ecosystem

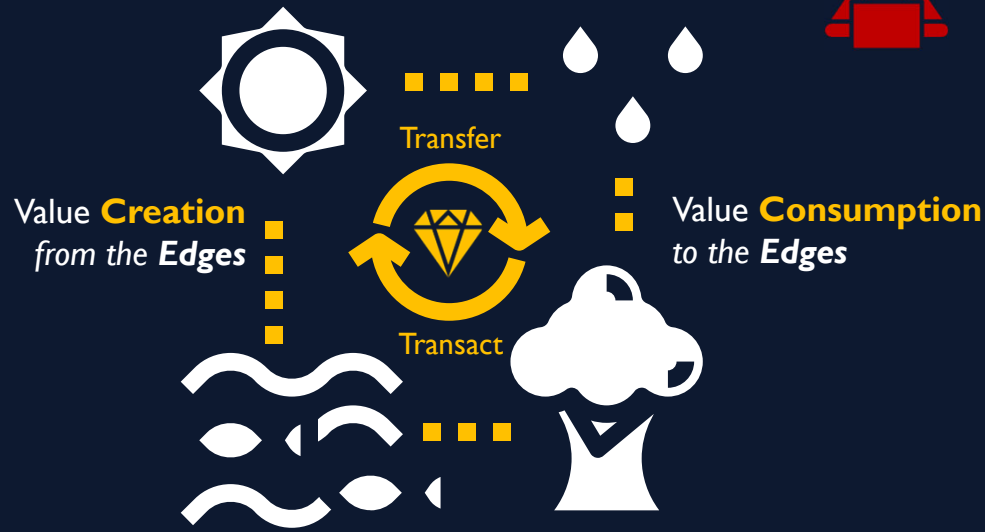
Value **Creation** from the **Edges**  Value **Consumption** to the **Edges**



Value **Stolen** Anytime from Anywhere



**Financial Inclusion**



**DC**  
Wild, Wild West



Loss of **Confidence**



# Digital Currency: Standards, Laws, Regulations

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

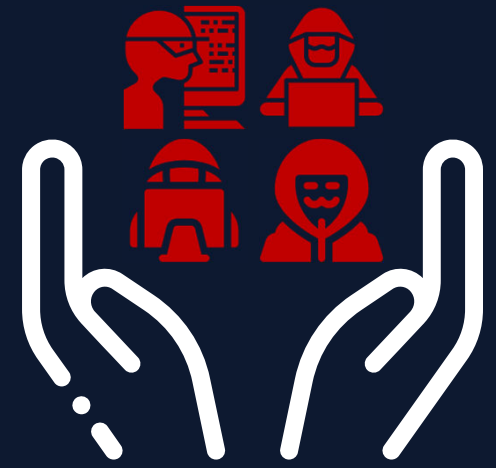


**Financial**  
Inclusion

Value **Creation**   
from the Edges



Value **Consumption**  Value **Stolen**  
to the Edges Anytime from Anywhere



**Security**  
Inclusion

# For Digital Currency, the Need for Assurance

Value **Creation**  Value **Consumption**  
from the Edges to the Edges



**Financial**  
Inclusion

I created Value!

I purchased Value!



**Who?**

**What** Value was created?

**What** Value was purchased?



**What?**

I own Value!




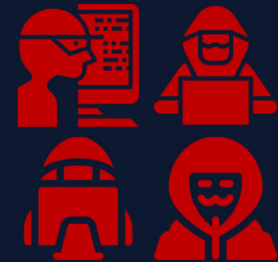
**Transact** Away!

Identification for Attribution, Ownership

- Identifiers
- Access
- Authorization

**Control = Ownership**

 Value **Stolen**  
Anytime from Anywhere



**Security**  
Inclusion

Cryptography for

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

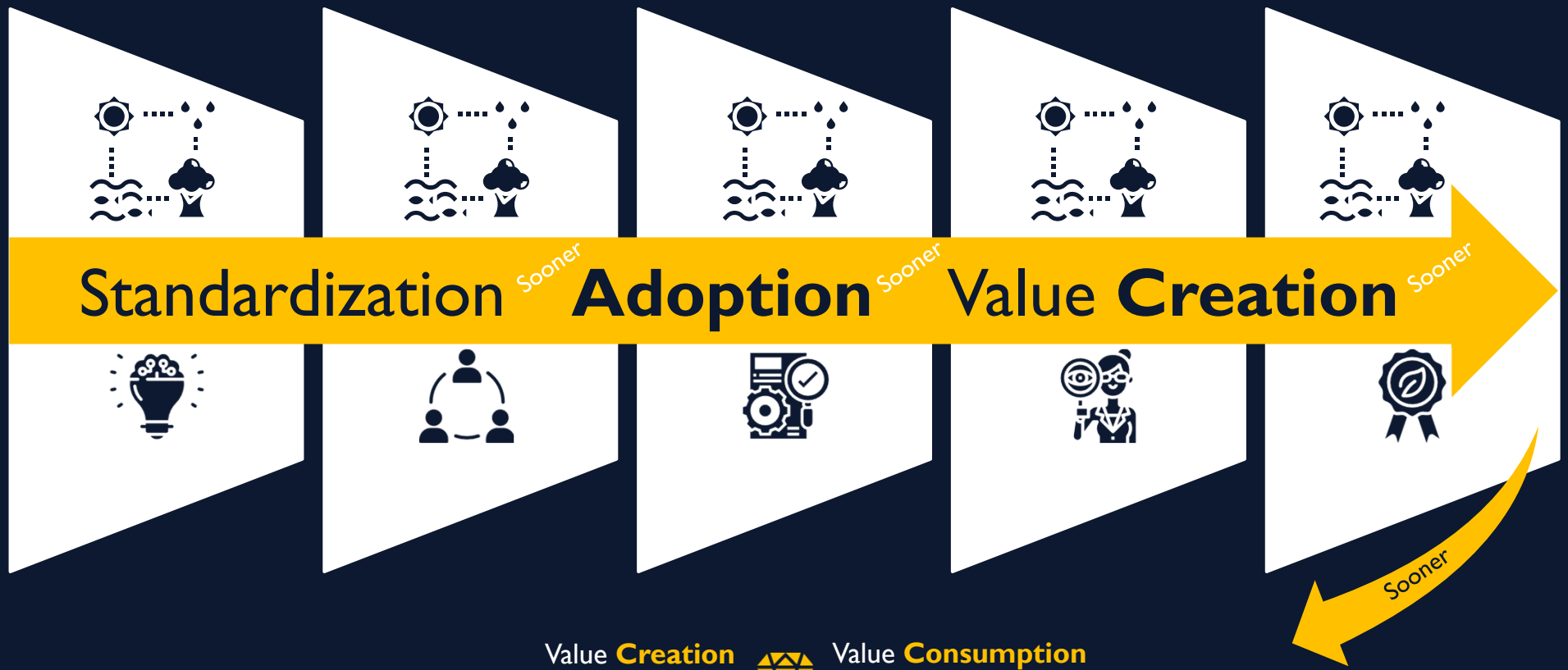
Assurance for:

- Trust
- Liability
- Warranties



# The Need for **Standardization**

... of performance and security specifications

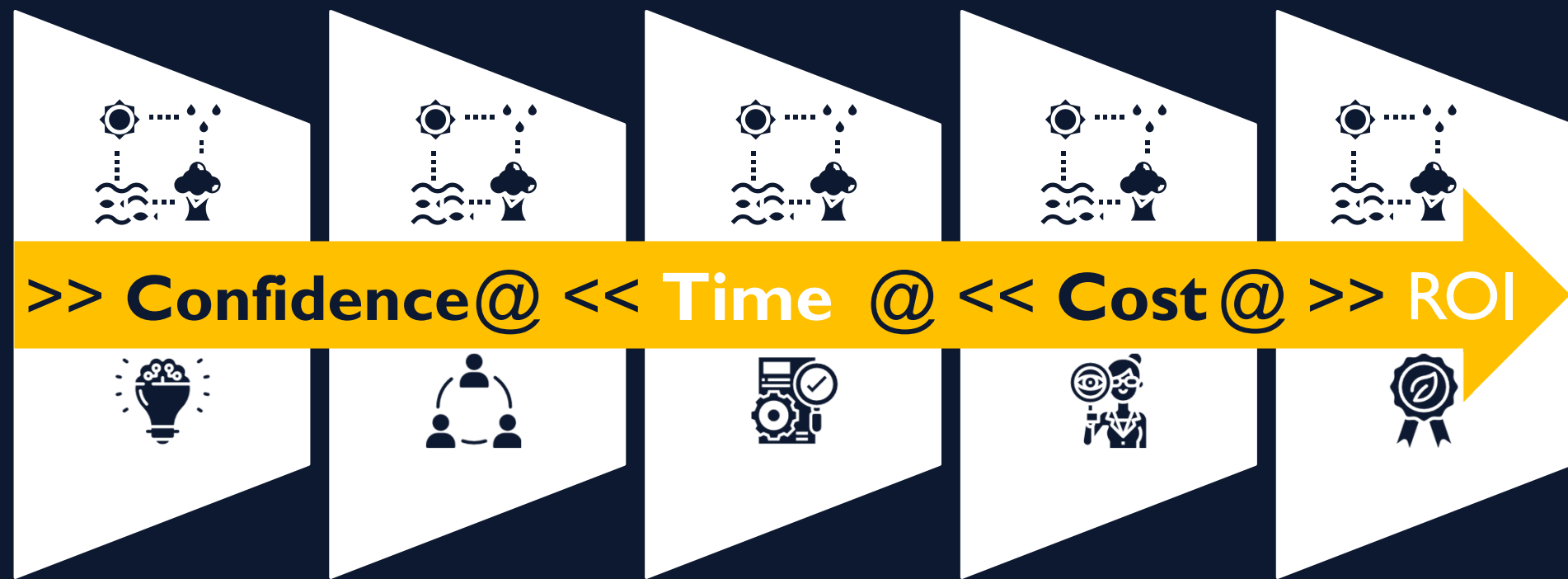


Value **Creation**  
Anywhere – from the **Edges**

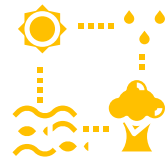


Value **Consumption**  
Somewhere Else – to the **Edges**

# Need for **Hyper** – Standardization, **Time to**



# Need for Expert **Collaboration**



**Collaboration**



Drive **ecosystem-wide** consensus on Digital Currency:

- **Requirements & Specifications**
  - Performance, Security & Resilience
- **Measurement Metrics & Methods**
- **Models & Templates for Reuse**

# Need for Speed – Time to Validation

Domain Experts propose suitable specifications - input into **Validation**



- Outcome - **standardized**
- **Common** specifications & requirements
  - **Consistent** measurement methods & metrics
  - **Comparable** models, templates & evaluations

# Need for Speed – Time to Validation

Validation process:

- **Common** specifications & requirements
- **Consistent** measurement methods & metrics
- **Comparable** models, templates & evaluations

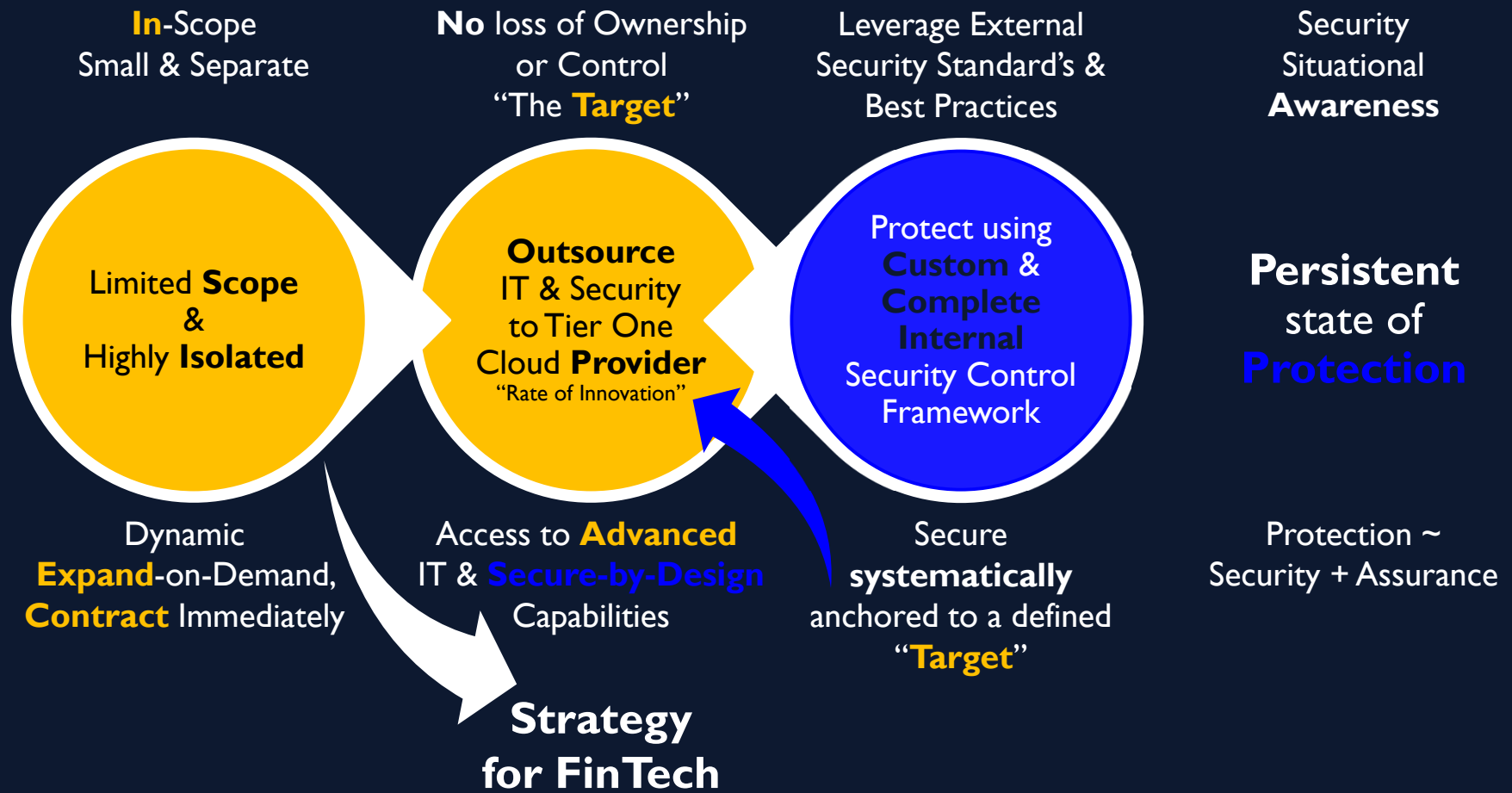


## **Standardized**

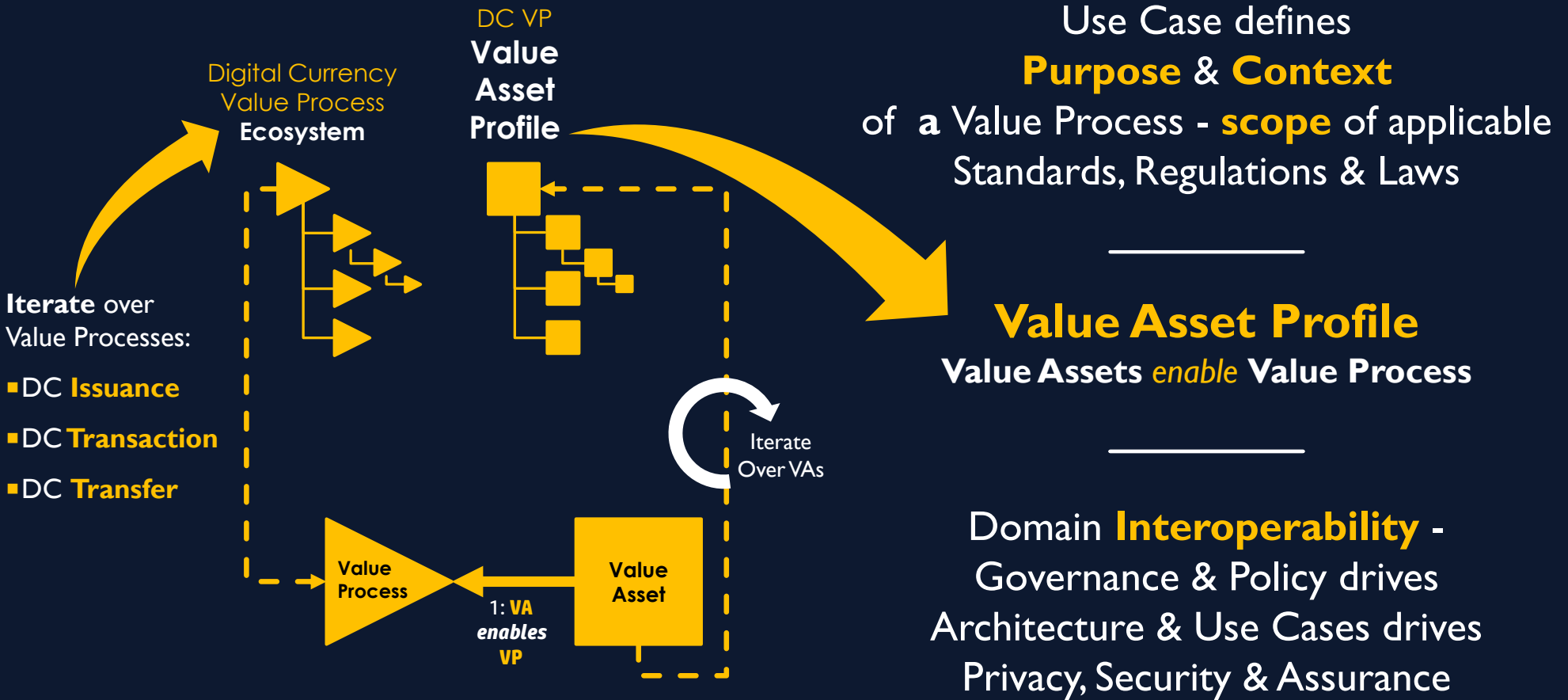
- Models
- Measurement Metrics
- Evaluation Methods

*that will ensure*  
**Repeatability w/ High Confidence**  
*for a basis of*  
**Performance & Protection**  
**Assessments & Benchmarking**  
*across the Ecosystem*

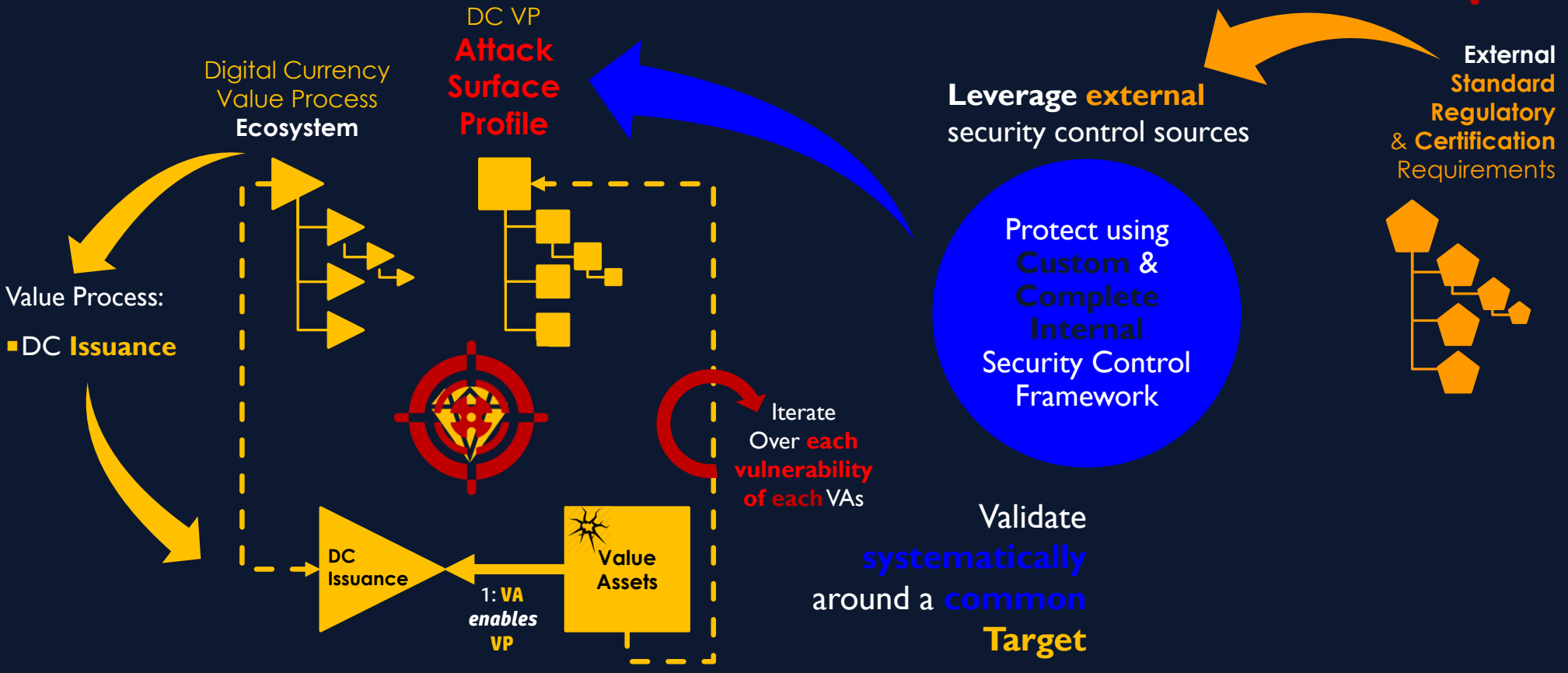
# The **Need** to be: Top Tier



# The **Need** for a **Common** Reference

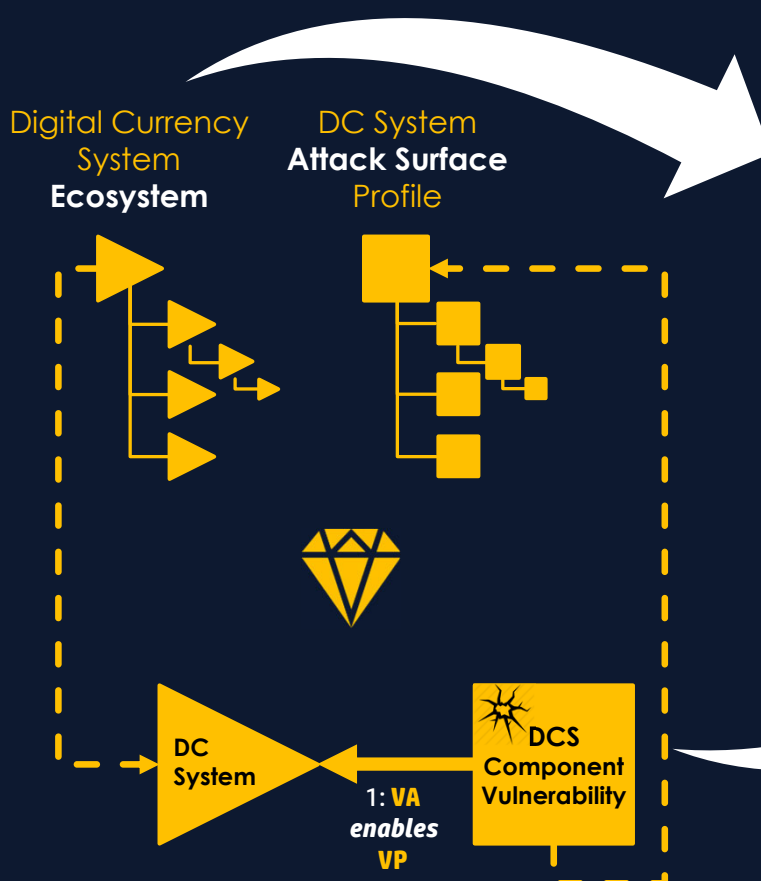


# The **Need** to be Target Specific





# The **Need** to adopt **Nomenclature**



Level	DIGITAL CURRENCY TARGET NOMENCLATURE	Acroynm
0	Digital Currency System <b>Ecosystem</b>	DCSE
-1	Digital Currency <b>System</b>	DCS
-2	DCS Component <b>Domain</b>	DCS-CD
-3	DCS Component <b>Class</b>	DCS-CC
-4	DCS <b>Component</b>	DCS-CO
-5	DCS Component <b>Vulnerability</b>	DCS-CV

**DC-#**  
**Target Level**  
**Nomenclature**  
 "Classification System"

# + Threat & Protection Nomenclature

Level	DIGITAL CURRENCY TARGET NOMENCLATURE	Acronym
0	Digital Currency System <b>Ecosystem</b>	DCSE
-1	Digital Currency <b>System</b>	DCS
-2	DCS Component <b>Domain</b>	DCS-CD
-3	DCS Component <b>Class</b>	DCS-CC
-4	DCS <b>Component</b>	DCS-CO
-5	DCS Component <b>Vulnerability</b>	DCS-CV

LEVEL	DCS RISK Nomenclature	DCS TARGET Nomenclature	DCS PROTECTION Nomenclature
0	DCS <b>ECOSYSTEM</b> RISK (DCSE-R)	DCS <b>Ecosystem</b> (DCSE)	DCS <b>ECOSYSTEM</b> PROTECTION (DCSE-P)
-1	DC <b>SYSTEM</b> RISK (DCS-R)	DC <b>System</b> (DCS)	DC <b>SYSTEM</b> PROTECTION (DCS-P)
-2	DCS THREAT <b>DOMAIN</b> (DCS-R-TD)	DCS Component <b>Domain</b> (DCS-CD)	DCS SECURITY <b>DOMAIN</b> (DCS-P-SD)
-3	DCS THREAT <b>CLASS</b> (DCS-R-TC)	DCS Component <b>Class</b> (DCS-CC)	DCS SECURITY <b>CLASS</b> (DCS-P-SC)
-4	DCS COMPONENT <b>THREATS</b> (DCS-R-CT)	DCS <b>Component</b> (DCS-CO)	DCS <b>COMPONENT</b> SECURITY (DCS-P-CS)
-5	DCS COMPONENT <b>VULNERABILITY</b> ATTACK (DCS-R-CVA):	DCS Component <b>Vulnerability</b> (DCS-CV)	DCS COMPONENT <b>VULNERABILITY</b> ATTACK COUNTERMEASURE (DCS-P-CVAC):

# + Stack Nomenclature

- #.1 Application
- #.2 Service
- #.3 Protocol
- #.4 Network
- #.5 Data
- #.6 Physical

LEVEL	DCS RISK Nomenclature	DCS TARGET Nomenclature	DCS PROTECTION Nomenclature
0	DCS ECOSYSTEM RISK (DCSE-R)	DCS Ecosystem (DCSE)	DCS ECOSYSTEM PROTECTION (DCSE-P)
-1	DC SYSTEM RISK (DCS-R)	DC System (DCS)	DC SYSTEM PROTECTION (DCS-P)
-2	DCS THREAT DOMAIN (DCS-R-TD)	DCS Component Domain (DCS-CD)	DCS SECURITY DOMAIN (DCS-P-SD)
-3	DCS THREAT CLASS (DCS-R-TC)	DCS Component Class (DCS-CC)	DCS SECURITY CLASS (DCS-P-SC)
-4	DCS COMPONENT THREATS (DCS-R-CT)	DCS Component (DCS-CO)	DCS COMPONENT SECURITY (DCS-P-CS)
-5	DCS COMPONENT VULNERABILITY ATTACK (DCS-R-CVA)	DCS Component Vulnerability (DCS-CV)	DCS COMPONENT VULNERABILITY ATTACK COUNTERMEASURE (DCS-P-CVAC)

**THREAT | TARGET | PROTECTION**  
Nomenclature

Isolate one row  
- Protocols

0 DIGITAL CURRENCY SYSTEM							
ID	Domain	DCS RISK Nomenclature		DCS TARGET Nomenclature		DCS Protection Nomenclature	
-1		DCS-Risk	DCS-R	Digital Currency System (DCS)		DCS-Protection	DCS-P
-2		THREAT DOMAIN (TD)		COMPONENT DOMAIN (CD)		SECURITY DOMAIN (SD)	
-2.1	Application	Application TD	DCS-R-ATD	Application CD	DCS-X-ACD	Application SD	DCS-P-ASD
-2.2	Service	Service TD	DCS-R-STD	Service CD	DCS-X-SCD	Service SD	DCS-P-SSD
-2.3	Protocol	Protocol TD	DCS-R-PTD	Protocol CD	DCS-X-PCD	Protocol SD	DCS-P-PSD
-2.4	Network	Network TD	DCS-R-NTD	Network CD	DCS-X-NCD	Network SD	DCS-P-NSD
-2.5	Data	Data TD	DCS-R-DTD	Data CD	DCS-X-DCD	Data SD	DCS-P-DCSD
-2.6	Physical	Physical TD	DCS-R-PhTD	Physical CD	DCS-X-PhCD	Physical SD	DCS-P-PhSD
-3		THREAT CLASS (TC)		COMPONENT CLASS (CC)		SECURITY CLASS (SC)	
-3.1	Application	Application TC	DCS-R-ATD-ATC	Application CC	DCS-X-ACD-ACC	Application SC	DCS-P-ASD-ASC
-3.2	Service	Service TC	DCS-R-STD-STC	Service CC	DCS-X-SCD-SCC	Service SC	DCS-P-SSD-SSC
-3.3	Protocol	Protocol TC	DCS-R-PTD-PTC	Protocol CC	DCS-X-PCD-PCC	Protocol SC	DCS-P-PSD-PSC
-3.4	Network	Network TC	DCS-R-NTD-NTC	Network CC	DCS-X-NCD-NCC	Network SC	DCS-P-NSD-NSC
-3.5	Data	Data TC	DCS-R-DTD-DTC	Data CC	DCS-X-DCD-DCC	Data SC	DCS-P-DCSD-DCSC
-3.6	Physical	Physical TC	DCS-R-PhTD-PhTC	Physical CC	DCS-X-PhCD-PhCC	Physical SC	DCS-P-PhSD-PhSC
-4		COMPONENT THREAT (CT)		COMPONENT (CO)		COMPONENT SECURITY (CS)	
-4.1	Application	Application CT	DCS-R-ATD-ATC-ACT	Application Component	DCS-X-ACD-ACC-AC	Application CS	DCS-P-ASD-ASC-AST
-4.2	Service	Service CT	DCS-R-STD-STC-SCT	Service Component	DCS-X-SCD-ACC-SC	Service CS	DCS-P-SSD-SSC-SST
-4.3	Protocol	Protocol CT	DCS-R-PTD-PTC-PCT	Protocol Component	DCS-X-PCD-ACC-PC	Protocol CS	DCS-P-PSD-PSC-PST
-4.4	Network	Network CT	DCS-R-NTD-NTC-NCT	Network Component	DCS-X-NCD-ACC-NC	Network CS	DCS-P-NSD-NSC-NST
-4.5	Data	Data CT	DCS-R-DTD-DTC-DCT	Data Component	DCS-X-DCD-ACC-DC	Data CS	DCS-P-DCSD-DCSC-DCST
-4.6	Physical	Physical CT	DCS-R-PhTD-PhTC-PhCT	Physical Component	DCS-X-PhCD-ACC-PhC	Physical CS	DCS-P-PhSD-PhSC-PhST
-5		COMPONENT VULNERABILITY ATTACK (CVA)		COMPONENT VULNERABILITY (CV)		CVA COUNTERMEASURE (CVAC)	
-5.1	Application	Application CVA	DCS-R-ATD-ATC-ACT-ACVA	Application CV	DCS-X-ACD-ACC-AC-ACV	Application CVAC	DCS-P-ASD-ASC-AST-ACVAC
-5.2	Service	Service CVA	DCS-R-STD-STC-SCT-SCVA	Service CV	DCS-X-SCD-ACC-SC-SCV	Service CVAC	DCS-P-SSD-SSC-SST-SCVAC
-5.3	Protocol	Protocol CVA	DCS-R-PTD-PTC-PCT-PCVA	Protocol CV	DCS-X-PCD-ACC-PC-PCV	Protocol CVAC	DCS-P-PSD-PSC-PST-PCVAC
-5.4	Network	Network CVA	DCS-R-NTD-NTC-NCT-NCVA	Network CV	DCS-X-NCD-ACC-NC-NCV	Network CVAC	DCS-P-NSD-NSC-NST-NCVAC
-5.5	Data	Data CVA	DCS-R-DTD-DTC-DCT-DCVA	Data CV	DCS-X-DCD-ACC-DC-DCV	Data CVAC	DCS-P-DCSD-DCSC-DCST-DCVAC
-5.6	Physical	Physical CVA	DCS-R-DTD-DTC-DCT-DCVA	Physical CV	DCS-X-PhCD-ACC-PhC-PhCV	Physical CVAC	DCS-P-PhSD-PhSC-PhST-PhCVAC

# + Protocol Threat Vectors

-5.3.1	<b>Consensus Mechanism Threats</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT-</b>
-5.3.1.1	<b>51% Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- 51A</b>
-5.3.1.2	<b>Timestamp Manipulation Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- TMA</b>
-5.3.1.3	<b>Bribing Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- BA</b>
-5.3.1.4	<b>Selfish Mining Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- SMA</b>
-5.3.1.5	<b>Chain Hopping Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- CHA</b>
-5.3.1.6	<b>Block Withholding Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- BWA</b>
-5.3.1.7	<b>Double-Spending Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>CMT- DSA</b>
-5.3.2	<b>Smart Contract Threats</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>SCT</b>
-5.3.2.1	<b>Timestamp Dependence Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>SCT- TDA</b>
-5.3.2.2	<b>Mishandled Exceptions Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>SCT- MEA</b>
-5.3.2.3	<b>Integer Overflow Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>SCT- OIA</b>
-5.3.2.4	<b>Predictable Random Number Attack</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>SCT- PRNA</b>
-5.3.3	<b>Virtual Machine Threats</b>	DCS-R-PTD-PTC-PCT-PCVA:	<b>VMT</b>

**ITU-T**  
TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1401**  
(11/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Distributed ledger  
technology security

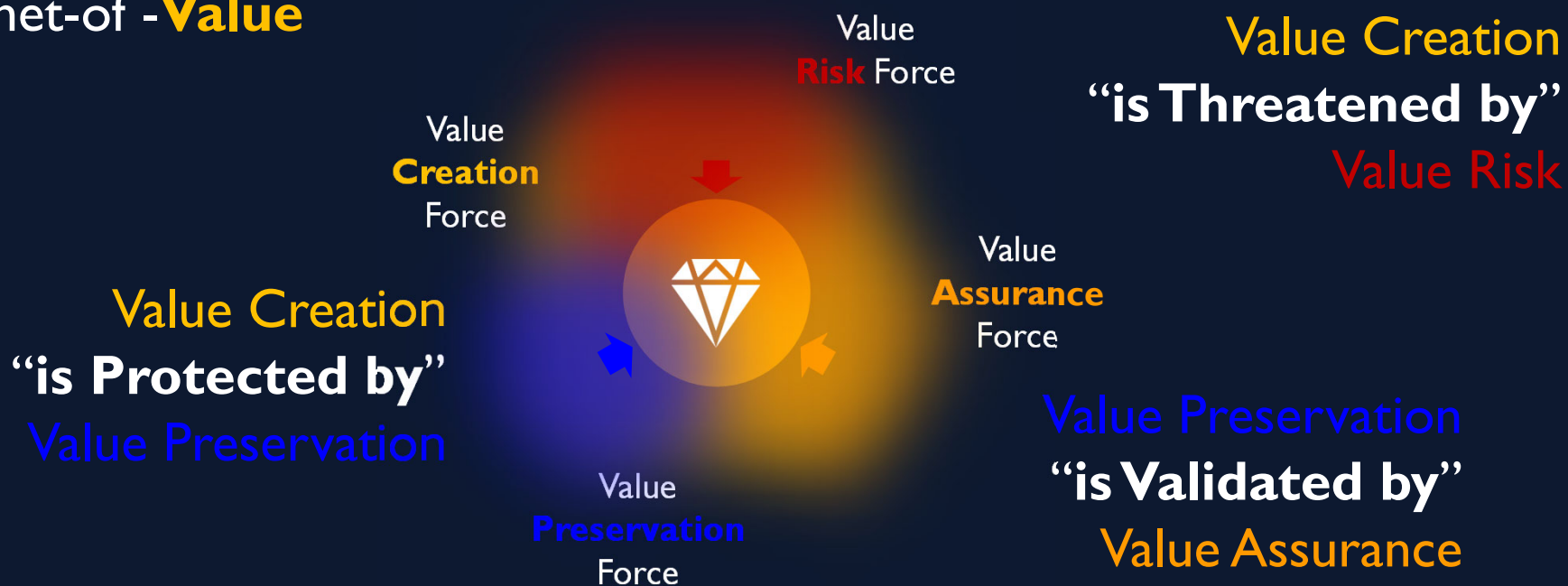
**Security threats to distributed ledger  
technology**

Recommendation ITU-T X.1401

International Telecommunication Union

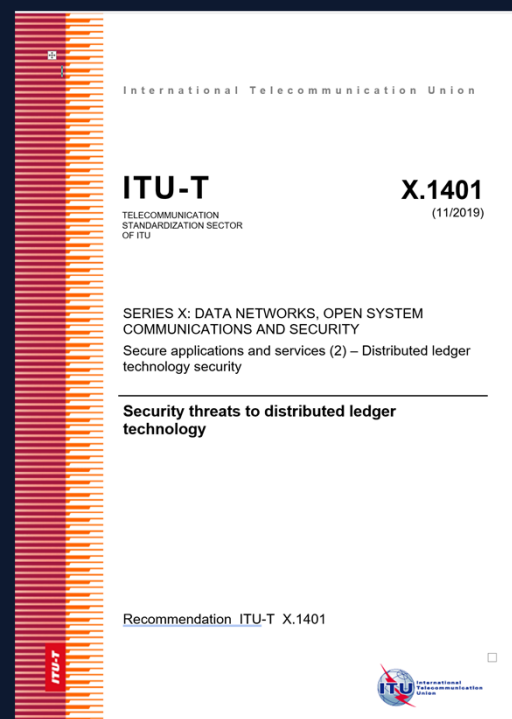
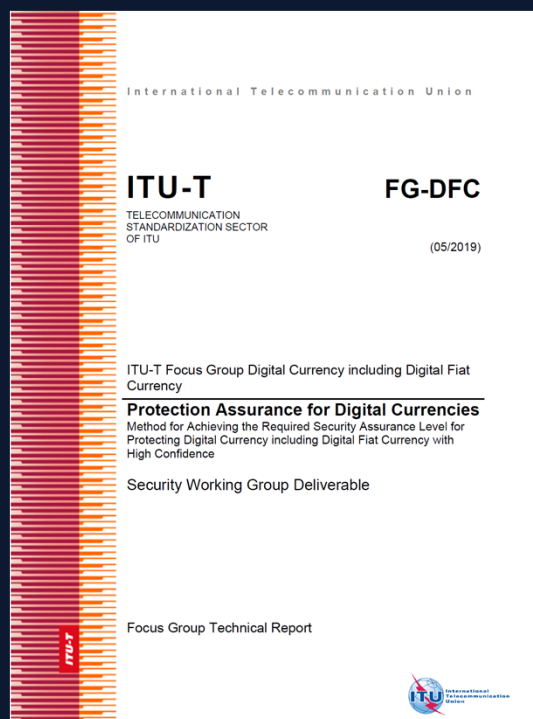
# The **Struggle** to Protect

Internet-of -**Value**



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

# Rethink to a Relational Model



Institutionalize Relationships

# Better Standardized Input - Better Output

Using

- **Common** specifications & requirements
- **Consistent** measurement methods & metrics
- **Comparable** models, templates & evaluations



**Standardized**

- **Models**
- **Measurement Metrics**
- **Evaluation Methods**

*that will ensure*

**Repeatability w/ Confidence**

*a basis of*

**Performance & Protection**

**Assessments & Benchmarking**

*across the Ecosystem*

Feeds **Standardized** “Creation & Issuance” Process

# Please walk away with

Realize This	Demand This	Accept This	Do This	Remember This
Current approaches and methods are too costly & complex - <b>not sustainable</b>	It is time for <b>interoperable</b> -by-Design!  From Massively <b>Heterogenous</b> to Massively <b>Interoperable</b>	DC use cases will need <b>trust standards</b> that are <b>logically</b> “ <b>higher</b> ” than other human use cases – <b>money</b>	<b>Participate</b> in the discussion and development of Standards	Participating enables one to <b>influence</b> and <b>shape</b> the future, do not miss the <b>opportunity</b>





# JACQUES FRANCOEUR

SILICON VALLEY SECURITY INDUSTRY THOUGHT LEADER: 34+ YOЕ



Please reach out  
to join forces with



USA Delegate (2018,19,20) Security Expert  
& Contributor

International Telecommunications Union (ITU),  
Standardization, Study Group 17: Security

Chief Scientist, Security Inclusion Now USA  
<https://www.linkedin.com/in/innoonewetrust/>  
Jacques@SecurityInclusionNow.org





# JACQUES FRANCOEUR

SILICON VALLEY SECURITY INDUSTRY THOUGHT LEADER: 34+ YOE



**Jacques  
Francoeur**

M.A.Sc., B.A.Sc, MBA

jacques@securityinclusionnow.org

<https://www.linkedin.com/in/innoonetrust/>

MBA: Concordia University  
M.A.Sc: University of Toronto  
Institute for Aerospace Studies  
B.A.Sc.: University of Toronto,  
Engineering Science,  
Aerospace Engineering

## **Chief Scientist & Founder**

**Security Inclusion Now**, Silicon Valley

**USA Delegate** (2018,19,20) **Security Expert & Contributor**  
**International Telecommunications Union (ITU)**, Standardization,  
Study Group 17: Security

**Chair: Security & Assurance** Working Group  
**Digital Currency Global Initiative**, ITU

## **Technical Director**

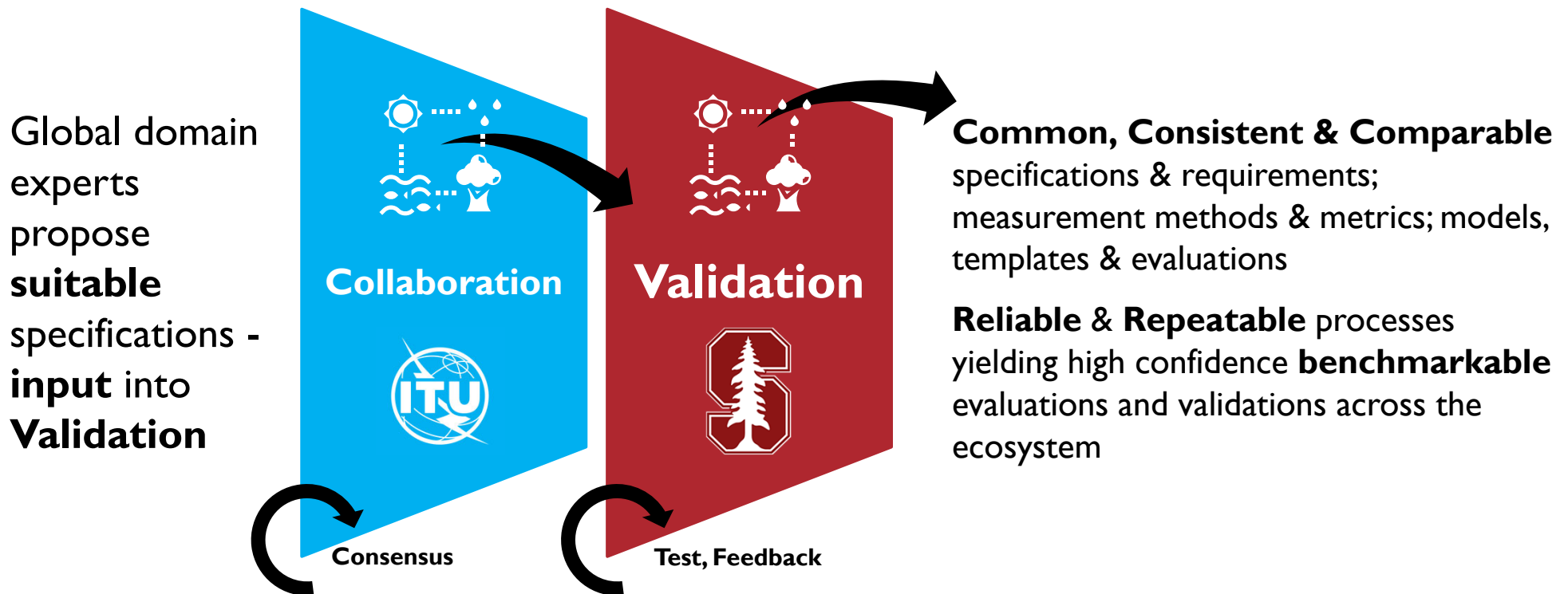
**Future of Digital Currency Program**, Stanford University  
Stanford Center for Blockchain Research, School of Engineering

## **Expert Network Member**

**World Economic Forum**, Blockchain Security

# Digital Currency Global Initiative

## & the Stanford Future of Digital Currency Program



**Spheric Shield™** | jacques.francoeur@sphericsecurity.com | ADMIN | Direct Mode

**TARGET ANALYSIS** | VALUE PROCESS LINKING

Value Processes of **DLT**

is enabled by **VALUE ASSET**

**THREAT ANALYSIS** | THREAT VECTOR LINKING

Threat Vectors of **BLOCKCHAIN**

threatens **VALUE ASSET**

**SECURITY ANALYSIS** | INTERNAL CONTROL LINKING

Internal Controls of **NIST CS...**

could policy protect **VALUE AS...**

**STANDARDS & REGULATIONS** | EXTERNAL CONTROL LINK MANA...

External Controls of **ISO 270...**

is validated by ...

**1: VA enables VP**

**2: TV threatens VA**

**3: IC policy protects VA**

**5: IC validates EC**

- Build Management [DLT: DCE-X-APP-DAM-DAD-]
- Test Management [DLT: DCE-X-APP-DAM-DAD-T]
- Software Development [DLT: DCE-X-APP-DAM-D]
- Trust Endorsement Management [DLT: DCE-X-APP-D-]
- Internal Governance [DLT: DCE-X-APP-DAM-TEV]
- External Governance [DLT: DCE-X-APP-DAM-TEH]
- Smart Contract Mechanism [DLT: DCE-X-APP-SCM]
- Account Management [DLT: DCE-X-APP-ACM]
- System Management [DLT: DCE-X-APP-SYM]
- Ledger Management [DLT: DCE-X-APP-LEM]
- Consensus Mechanism [DLT: DCE-X-APP-COM]
  - is enabled by **Proof of Work Consensus Algorithm**
  - is enabled by **Proof-of-Stake Consensus Algorithm**
- Extendible Protocol Communication [DLT: DCE-X-APP-EPC]
- Interface [DLT: DCE-X-APP-INT]
  - Client [DLT: DCE-X-APP-INT-CLI]
  - Wallet [DLT: DCE-X-APP-INT-WAL]
- SERVICE Component Domain (SCD) [DLT: DCE-X-SER]
  - Auditing Service [DLT: DCE-X-SER-AS]
    - Monitoring [DLT: DCE-X-SER-AS-MON]
    - Auditing [DLT: DCE-X-SER-AS-AUD]
  - Smart Contract Service [DLT: DCE-X-SER-SCS]
    - Registration [DLT: DCE-X-SER-SCS-REG]
    - Template [DLT: DCE-X-SER-SCS-TEM]
    - Compiler [DLT: DCE-X-SER-SCS-COM]
    - Virtual Machine Runtime [DLT: DCE-X-SER-SCS-VMR]
  - Account Service [DLT: DCE-X-SER-ACS]
    - Identity [DLT: DCE-X-SER-ACS-INT]
    - Authentication [DLT: DCE-X-SER-ACS-ATE]
    - Authorization [DLT: DCE-X-SER-ACS-AUT]

- threatens **Proof of Work Consensus Algorithm**
- threatens **Proof-of-Stake Consensus Algorithm**
- 51% Attack [BLOCKCHAIN THREAT VECTORS: P.1.1]
  - threatens **Node 333.333.333.333**
- Timestamp Attack [BLOCKCHAIN THREAT VECTORS: P.1.2]
  - threatens **Trusted Time Signature System**
- Bribing Attack [BLOCKCHAIN THREAT VECTORS: P.1.3]
  - threatens **Node 333.333.333.333**
  - threatens **Node 123.456.789.111**
  - threatens **Node 345.637.567.134**
- Selfish Mining Attack [BLOCKCHAIN THREAT VECTORS: P.1.4]
  - threatens **Node 333.333.333.333**
  - threatens **Node 123.456.789.111**
  - threatens **Node 345.637.567.134**
- Chain Hopping Attack [BLOCKCHAIN THREAT VECTORS: P.1.5]
  - threatens **Node 333.333.333.333**
  - threatens **Node 123.456.789.111**
  - threatens **Node 345.637.567.134**
- Block Withholding Attack [BLOCKCHAIN THREAT VECTORS: P.1.6]
  - threatens **Node 333.333.333.333**
  - threatens **Node 123.456.789.111**
  - threatens **Node 345.637.567.134**
- Double-spending Attack [BLOCKCHAIN THREAT VECTORS: P.1.6]
  - threatens **Node 333.333.333.333**
  - threatens **Node 123.456.789.111**
  - threatens **Node 345.637.567.134**
- Smart Contract Attack [BLOCKCHAIN THREAT VECTORS: P.2]
  - threatens **Smart Contract 2785096 of DLT C24DSH**
- Smart Contract 2845 of DLT ABCDEF

- The organization's role in the supply chain is identified and con...
- The organization's place in critical infrastructure and its industr...
- Priorities for organizational mission, objectives, and activities ar...
- Dependencies and critical functions for delivery of critical servic...
- Resilience requirements to support delivery of critical services e...
- Governance [NIST CSF 1.1: ID.GV]
  - Organizational cybersecurity policy is established and commun...
  - Cybersecurity roles and responsibilities are coordinated and ab...
  - Legal and regulatory requirements regarding cybersecurity, inc...
  - Governance and risk management processes address cybersco...
- Risk Assessment [NIST CSF 1.1: ID.RA]
  - Asset vulnerabilities are identified and documented [NIST CSF 1...
  - Cyber threat intelligence is received from information sharing f...
  - Threats, both internal and external, are identified and documen...
  - Potential business impacts and likelihoods are identified [NIST ...
  - Threats, vulnerabilities, likelihoods, and impacts are used to det...
  - Risk responses are identified and prioritized [NIST CSF 1.1: ID.R...
- Risk Management Strategy [NIST CSF 1.1: ID.RM]
  - Risk management processes are established, managed, and ag...
  - Organizational risk tolerance is determined and clearly express...
  - The organization's determination of risk tolerance is informed l...
- Supply Chain Risk Management [NIST CSF 1.1: ID.SC]
  - Cyber supply chain risk management processes are identified, e...
  - Suppliers and third party partners of information systems, com...
  - Contracts with suppliers and third-party partners are used to in...
  - Suppliers and third-party partners are routinely assessed using...
  - Response and recovery planning and testing are conducted wit...
- PROTECT [NIST CSF 1.1: PR]
  - Identity Management, Authentication and Access Control [NIST CSF ...
  - Identities and credentials are issued, managed, verified, revoke...

- is maintained by **Cybersecurity roles and responsib...**
- is validated by **Privileged users understand their rol...**
- is validated by **Third-party stakeholders (e.g., suppli...**
- is validated by **Senior executives understand their r...**
- is validated by **Physical and cybersecurity personnel**
- is validated by **Roles and responsibilities for detecti...**
- is validated by **Personnel know their roles and orde...**
- Information security coordination [ISO 27001 13: 6.1.2]
  - is validated by **Access permissions and authorization**
- Protections against data leaks are im...
- is validated by **Protections against data leaks are im...**
- Allocation of information security responsibilities [ISO 27001 13: ...]
  - is validated by **Incidents are reported consistent wit...**
- Authorization process for information processing facilities [ISO ...]
  - is validated by **Cyber threat intelligence is received f...**
  - is validated by **Voluntary information sharing occur...**
  - is validated by **Public relations are managed [NIST C...**
- Confidentiality agreements [ISO 27001 13: 6.1.5]
  - is validated by **A System Development Life Cycle to r...**
- Contact with authorities [ISO 27001 13: 6.1.6]
  - is validated by **Contact with special interest groups [ISO 27001 13: 6.1.7]**
  - is validated by **Independent review of information security [ISO 27001 13: 6.1.8]**
- External parties [ISO 27001 13: 6.2]
  - is validated by **Identification of risks related to external parties [ISO 27001 13: ...]**
  - is validated by **Remote access is managed [NIST CSF ...]**
  - is validated by **Addressing security when dealing with customers [ISO 27001 1: ...]**
  - is validated by **Remote access is managed [NIST CSF ...]**
  - is validated by **Addressing security in third party contracts [ISO 27001 13: 6.2.3]**
- Asset Management [ISO 27001 13: 7]
  - is validated by **Responsibility for assets [ISO 27001 13: 7.1]**
  - is validated by **Inventory of assets [ISO 27001 13: 7.1.1]**