

Introducing FINOS

Common Cloud Controls

A Financial Cloud Controls Standard

Gabriele Columbro

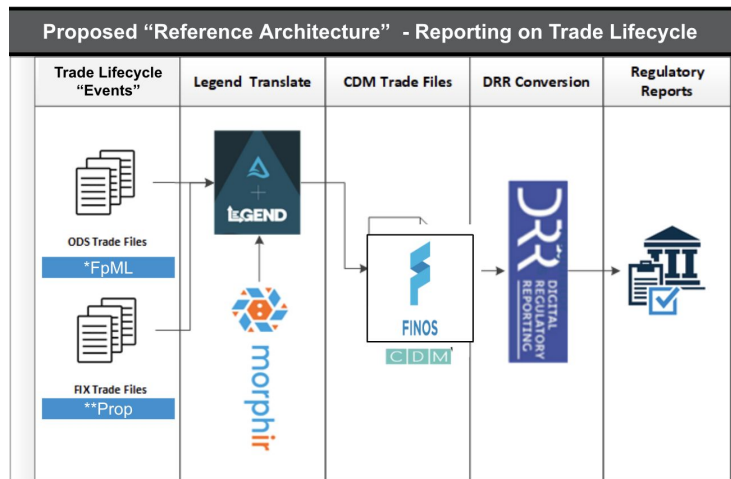
General Manager, Linux Foundation Europe
Executive Director, FINOS



Financial firms are “regulator success” driven

As it enables mutualization of interpretation of both technology (e.g. cloud, OSS) regulation and financial regulations (e.g. LCR and DRR)

**OPEN
REG
TECH**



**OPEN
REG
TECH**

US LCR



COMPLIANT FINANCIAL
INFRASTRUCTURE

(New)



**OPEN
SOURCE**
READINESS
by **FINOS**



**FINOS
COMMON
CLOUD
CONTROLS**

Public Cloud Adoption by Financial Services

Public Cloud Placement offers *significant* benefits to Financial Services... as well as some *unique challenges*

Benefits



Agility &
Scalability



Cost
Optimization



Codified
Controls



Accelerated
Innovation



Geographic
Availability



Resilience

Challenges



Shared
Responsibility



Scarcity of
Skills



Regulatory
Environment

Cloud Risks Highlighted by US Department of the Treasury

“...commonly held view among many U.S. financial institutions as well as industry stakeholders and academics that existing **CSPs’ efforts did not fully satisfy financial institution risk management needs.**”

“**Concentration** could expose many financial services clients to the same set of physical or cyber risks (e.g., from a region-wide outage).”

“**Unbalanced contractual terms** could limit individual financial institutions’ ability to measure and mitigate risks from cloud services, which could result in unwarranted risk across the sector.”

US Treasury: CSPs lack transparency and documentation

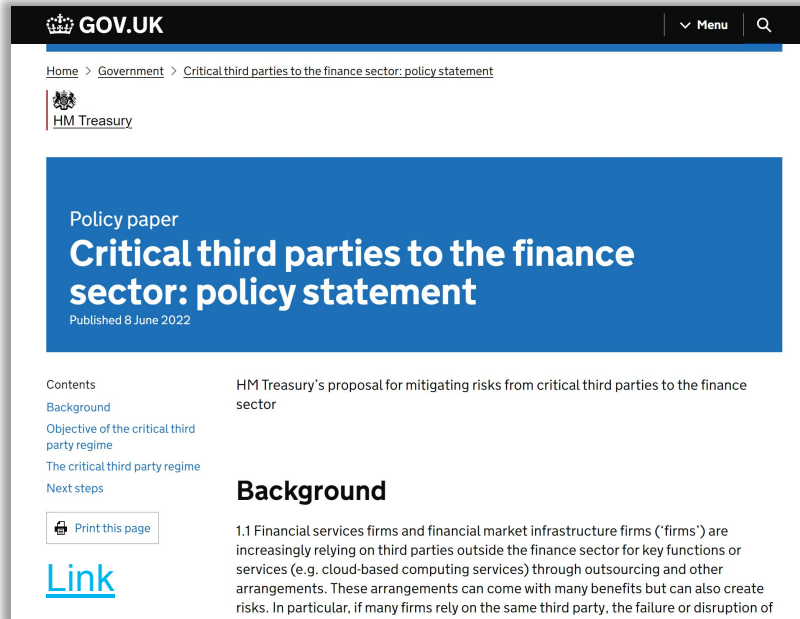
February 2023



Cloud Risks Highlighted by United Kingdom HM Treasury

UK: Hard for FIs to obtain resiliency guarantees from “critical third parties” such as CSPs

June 2022



“(Financial) firms are required to ensure their contractual arrangements with third parties allow them to comply with this **operational resilience framework**, which includes **requirements on areas such as data security, business continuity and exit planning**

...no single firm can manage risks originating from a concentration in the provision of critical services by one third party to multiple firms

...significant information and power asymmetries between certain third parties and firms, which may prevent firms from obtaining **adequate assurances that their contractual arrangements achieve an appropriate level of operational resilience**”

Cloud Risks Highlighted by the European Union

“DORA sets **uniform requirements for the security of network and information systems** of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, **such as cloud platforms**

European supervisory authorities ... **will develop technical standards for all financial services institutions to abide by**”

EU: Resiliency rules set for FIs and CSPs with “uniform requirements”



The screenshot shows the official press release from the European Council. The header includes the European Council logo and navigation links. The main title is 'Digital finance: Council adopts Digital Operational Resilience Act'. Below the title, a summary states that the EU is strengthening IT security for financial entities. A quote from Zbyněk Stanjura, Minister of Finance of Czechia, is included, along with a small portrait photo of him. At the bottom, a paragraph explains that DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector, as well as critical third parties providing ICT services, such as cloud platforms or data analytics services.

European Council
Council of the European Union

Home > Press > Press releases

Council of the EU Press release 28 November 2022 14:30

Digital finance: Council adopts Digital Operational Resilience Act

Given the ever-increasing risks of cyber attacks, the EU is strengthening the IT security of financial entities such as banks, insurance companies and investment firms. Today the Council adopted the Digital Operational Resilience Act (DORA) which will make sure the financial sector in Europe is able to **stay resilient through a severe operational disruption**.



We live in uncertain times. Banks and other companies which provide financial services in Europe already have plans in place for their IT security, but we need to go one step further. Thanks to the harmonised legal requirements which we adopted today, our financial sector will be better able to continue to function at all times. If a large-scale attack on the European financial sector is launched, we will be prepared for it.

— Zbyněk Stanjura, Minister of Finance of Czechia

DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can

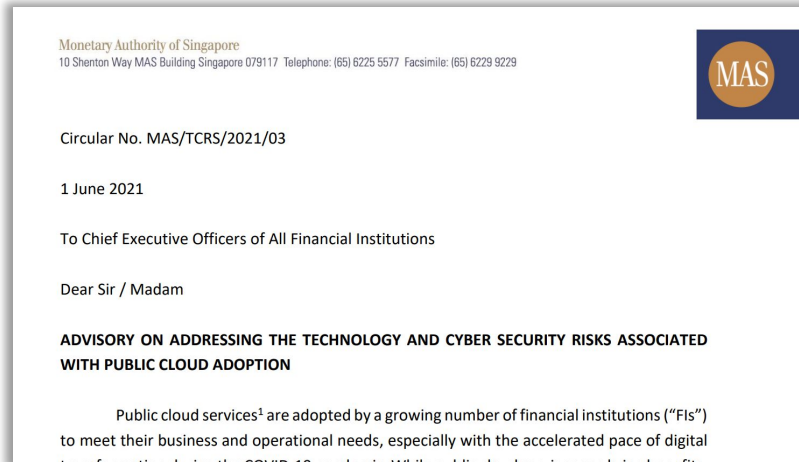
Risks Highlighted by the Monetary Authority of Singapore

Singapore: Focus on poor cyber hygiene... and lock-in/concentration



June 2021

Monetary Authority
of Singapore



“...Common key risks and control measures that FIs should consider before adopting public cloud services:

- Implementing **strong controls in areas such as Identity and Access Management (IAM), cyber security, data protection and cryptographic key management (...)**
- Misconfigurations or poor cyber hygiene could result in unauthorized access to the cloud metastructure (...)
- **Managing cloud resilience, outsourcing, vendor lock-in and concentration risks (...)**”

A problem in search of a solution...
(not the other way around)

Announcing...



**FINOS
COMMON
CLOUD
CONTROLS**

CCC Addresses these key challenges

Regulators have identified some consistent thematic challenges as an industry we can help to address through FINOS Common Cloud Controls

Cloud Vendor Lock-in

The inability to move workloads between Cloud Service Providers.

Inconsistency of cyber controls

Missing or misconfigured controls results in increased cyber risk.

Scarcity of skilled workforce

CSP implementations vary greatly; competition for talent is intense; complex skill set requirements.

And ultimately, we could help address...

Fragmentation & Complexity of Regulatory Landscape

Focus by multiple regulatory agencies simultaneously creates risk to Financial Services firms.

The need for a FinServ Public Cloud Standard...

Why is this important?

- CSP differentiation makes regulatory, operational and cyber resilience complicated, bespoke and costly.
- Our regulators are increasingly moving towards establishing and enforcing technical standards.

Why is this important to FINOS members?

- The buck stops with the banks! CSPs are not responsible for institutional risk management, we are!
- FINOS banking members have the institutional knowledge to develop an appropriate Cloud standard, and the critical mass to work with CSPs to drive adoption.

What is being done?

- *FINOS Common Cloud Controls (FINOS CCC)* is an industry standard that describes consistent controls for a *subset of CSP services* that are common across CSPs and are fundamental to most solutions.
- CSPs would certify themselves against the standard in a machine-verifiable way.
- Various regulators can map their requirements to a single consistent standard, a public cloud regulatory “Rosetta Stone”.

...is broadly recognized!



July 28th



July 19th

FINOS Common Cloud Controls – What is it?

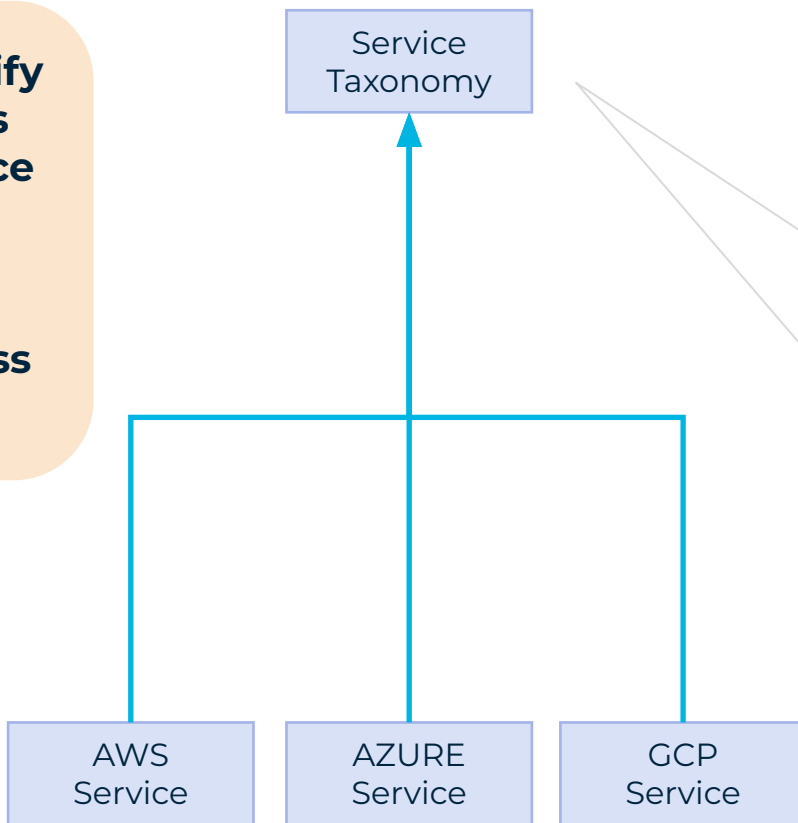
The FINOS Common Cloud Controls standard consists of the following:

- 1. Cloud Services Taxonomy :** a consistent taxonomy for **common critical services** provided by a specific CSP to facilitate identification and classification of similar services across CSPs.
- 2. Service Specific Data Flow Diagram :** a high-level data flow of a generic service, providing sufficient details to understand common attack vectors in the service. This will necessitate the creation of a consistent nomenclature and iconography for cloud services and their dependent components
- 3. Threat Catalogue :** a consistent taxonomy of common threat techniques, and associated mitigations, that may occur across services exploiting potential weaknesses. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) is leveraged and extended where necessary.
- 4. Logical Controls Description :** a logical control that provides a mitigation to a specific threat that a service has to address. The **Open Security Controls Assessment Language** (OSCAL) is a machine-readable data format used to define a control policy. This is a NIST standard that is maturing with controls now available to define the NIST 800-153 cloud standard.

FINOS Common Cloud Controls – Putting it all Together

Each CSP must first classify their applicable services against a Common Service Taxonomy.

This identifies potential service alternatives across CSPs



Exploring collaborations with

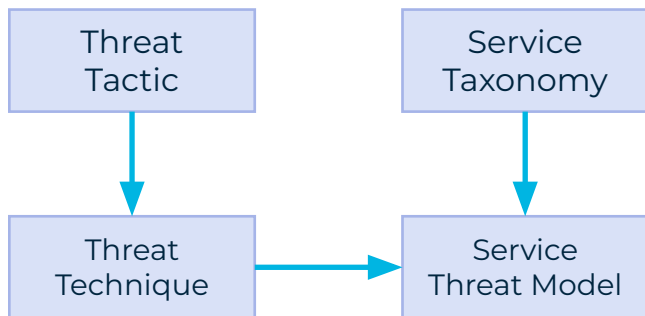


FOCUS



**FinOps
Foundation**

FINOS Common Cloud Controls – Putting it all Together



Leveraging the MITRE ATT&CK Framework and common architecture approach, a Threat Model for the generalized service is created

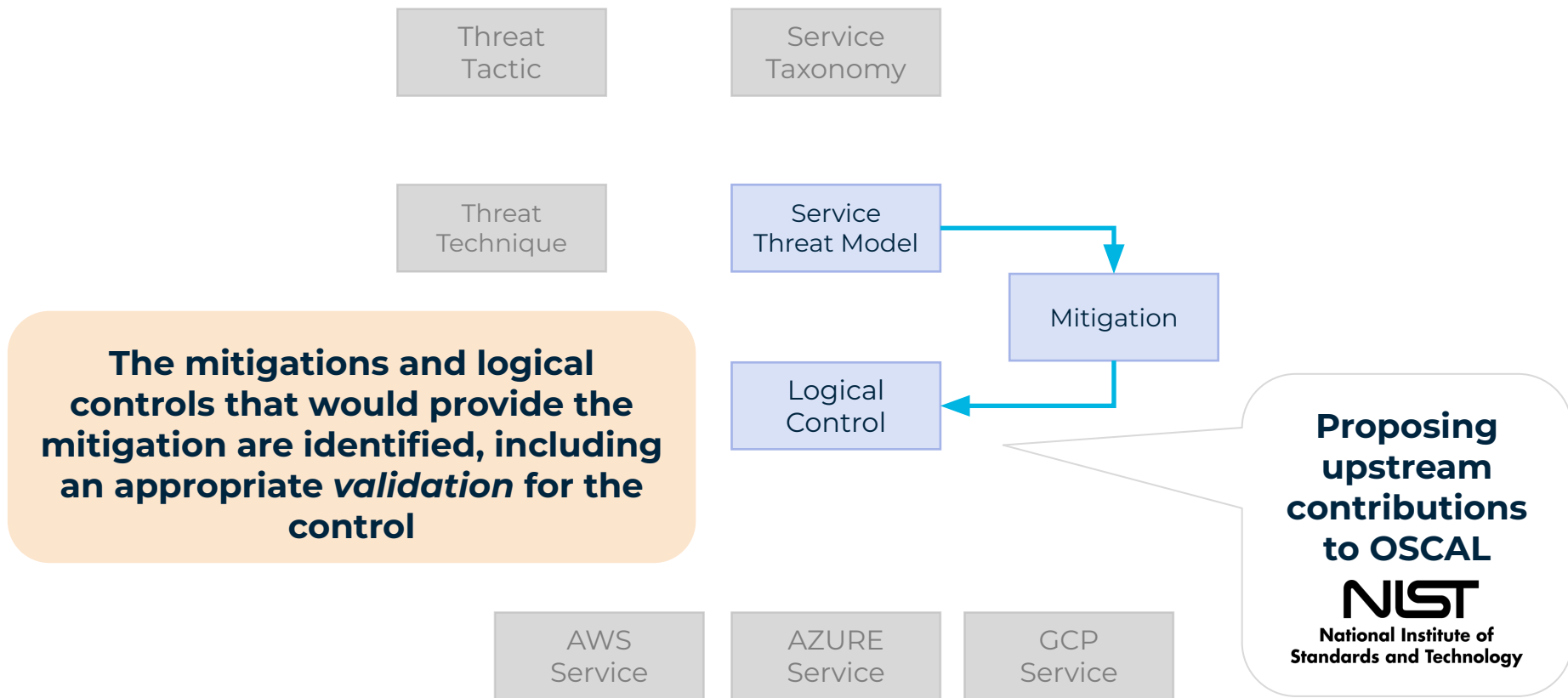
MITRE
ATT&CK™

AWS
Service

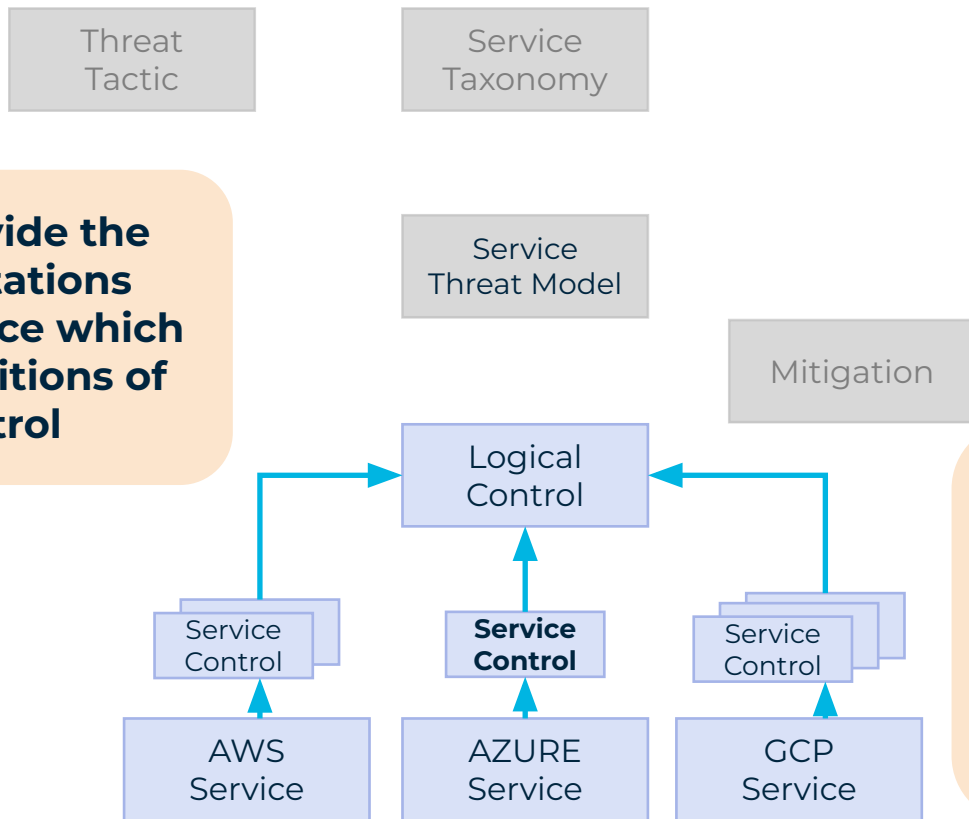
AZURE
Service

GCP
Service

FINOS Common Cloud Controls – Putting it all Together



FINOS Common Cloud Controls – Putting it all Together

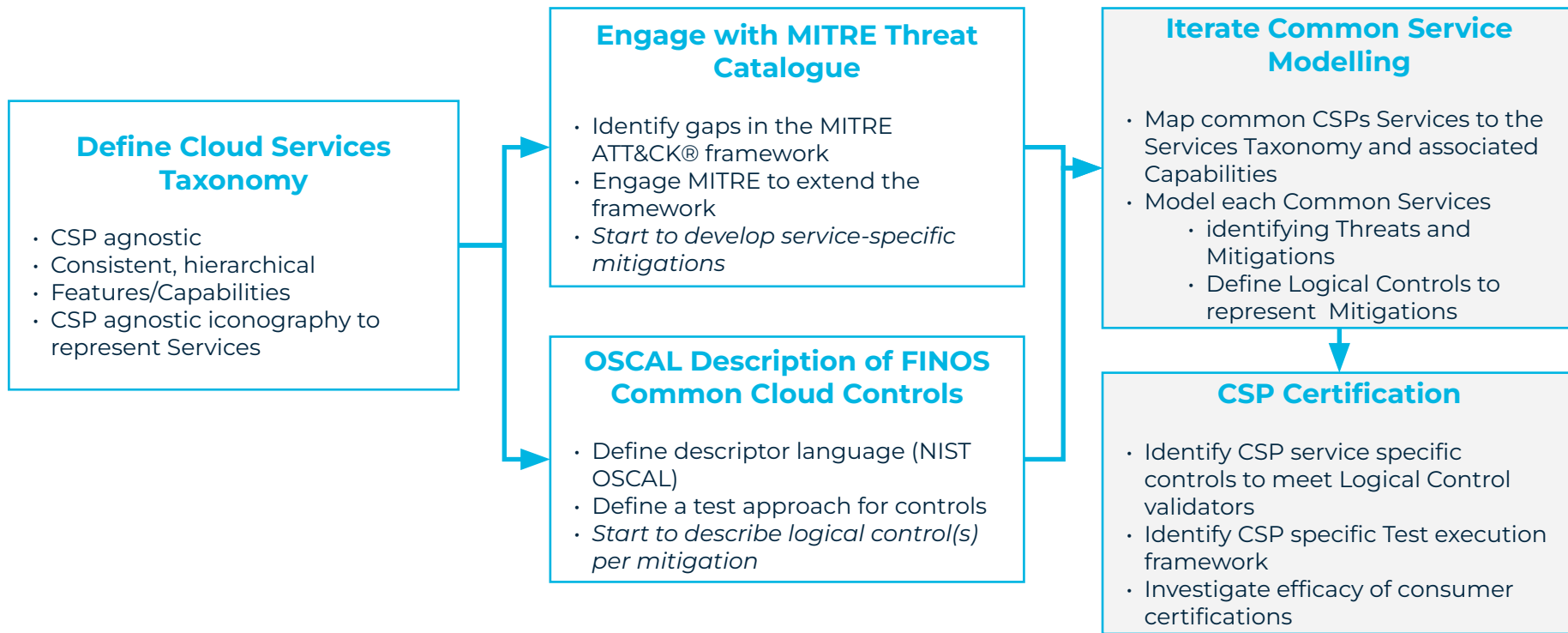


Each CSPs can provide the control implementations specific to their service which can satisfy the conditions of the logical control

...with these services considered compliant to the FINOS CCC standard for that service

Delivering FINOS Common Cloud Controls

FINOS Common Cloud Controls has been launched within FINOS with the following working groups



After 3 months of formation FINOS CCC has **133 participants** and is maintained by **Citi, Goldman Sachs, Morgan Stanley, BMO, NIST, Google, Red Hat, Control Plane** and **Compliance Cow**.

Morgan Stanley



BMO



Goldman Sachs



Red Hat

Google Cloud



controlplane



ComplianceCow

NIST

Hot off the press: CCC is “open” for business

finos.org/common-cloud-controls-project



**.MONEY
20/20**
AN ASCENTIAL COMPANY

USA
OCTOBER 23-26
LAS VEGAS

Clear Skies Ahead: Solving Cloud Migration Issues Through Open Source

Panel

Speakers



Gabriele (Gab) Columbro

Executive Director
The Fintech Open Source
Foundation (FINOS)



David Stone

Office of the CISO
Google



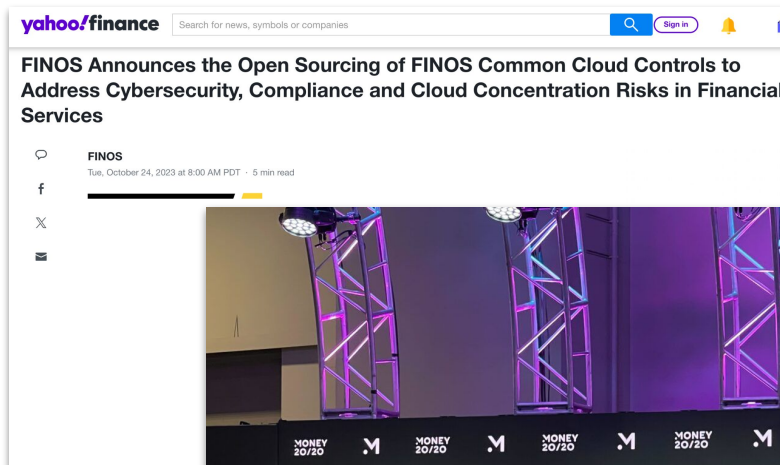
Rohan Deshpande

Head of App Foundry
Goldman Sachs

When

Tuesday 24, 13:30 - 14:10
(40min)

The Briefing Room, Money
Hall



Why would you want to be involved?

- **Financial Institutions**

- Regulators and self-regulatory bodies have already expressed interest in this, get ahead of the game
- Addresses a common, strategic issue as FSIs move workloads in the cloud, with a multi-cloud strategy
- Get the opportunity to define compliance requirements without forcing structural changes in the shared responsibility model
- Reduce cloud concentration risks and vendor lock-in

- **CSPs**

- Regulators and self-regulatory bodies have already expressed interest in this: maintain the shared responsibility model
- Participate actively in the definition of financial cloud compliance with your customers: no single vendor can own this space, when ultimately responsibility is on regulated entities
- First mover advantage during early stage formation phase

- **SaaS tech vendors / Consulting firms**

- Influence definition of the standard which will create a level playing field
- Reduce regulatory friction/risk, by building your product on a widely accepted set of requirements defined by FSIs
- Become an expert early on an industry wide technology

Join FINOS to collaborate on FINOS Common Cloud Controls

Common Cloud Controls solves consistent thematic challenges identified by the regulators through open source

- ✓ Cloud Concentration
- ✓ Inconsistent cyber controls
- ✓ Scarcity of skilled workforce

... and ultimately ...

Fragmentation & complexity of regulatory landscape



Read the FINOS
Press Release 



Connect with FINOS to Find Out More

