FINOS Fintech Open Source Foundation

Introducing FINOS Common Cloud Controls

A Financial Cloud Controls Standard

June 2024

THE LINUX FOUNDATION

Contents

- Public Cloud
  - Benefits and Challenges
  - Risks (US, UK, EU, Singapore)
  - Thematic Challenges
- The Need For A Standard
- CCC
  - Problem Statement
  - How Does It Work?
  - Taxonomies, Attacks and Controls
- Project Structure
  - Steering Committee
  - Working Groups
  - CTA

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

US Treasury: "CSPs lack transparency and Documentation"

February 2023

"...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."

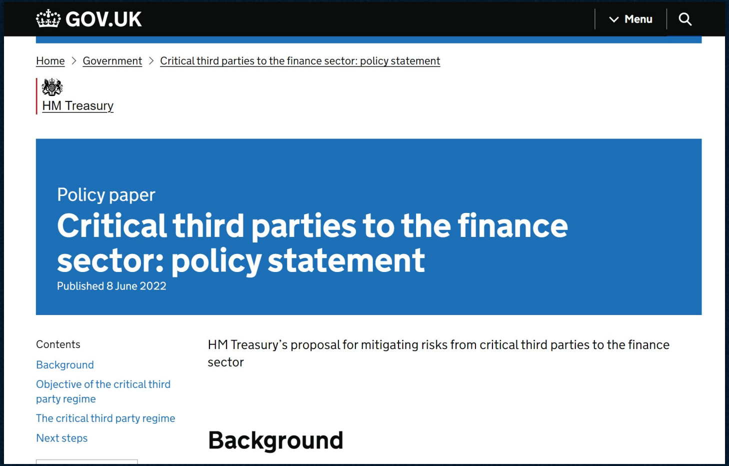
[Link]

The Financial Services Sector's Adoption of Cloud Services

U.S. Department of the Treasury

Cloud Risks Highlighted by United Kingdom HM Treasury

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



GOV.UK

Home > Government > Critical third parties to the finance sector: policy statement

HM Treasury

Policy paper

Critical third parties to the finance sector: policy statement

Published 8 June 2022

Contents

Background

Objective of the critical third party regime

The critical third party regime

Next steps

HM Treasury's proposal for mitigating risks from critical third parties to the finance sector

Background

"(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"**

Link

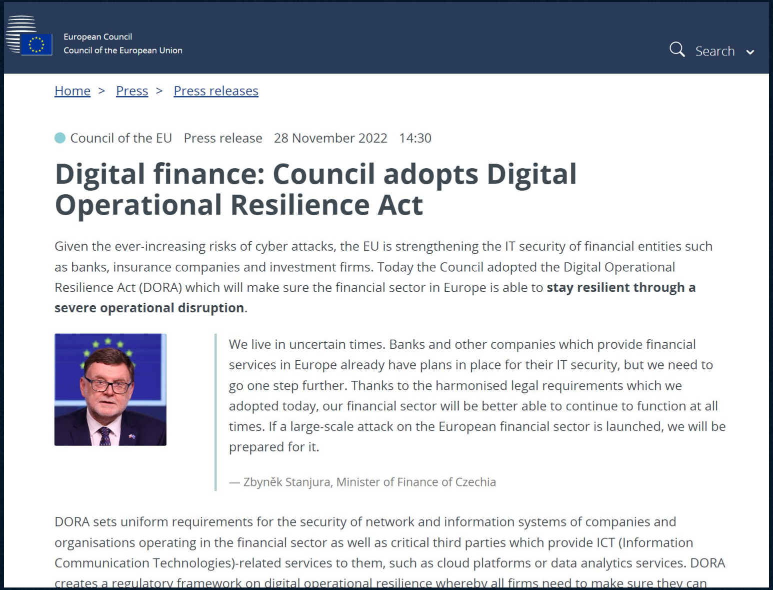
Cloud Risks Highlighted by the European Union

EU: "Resiliency rules set for FIs and CSPs with 'uniform requirements'"

"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"**

Link



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

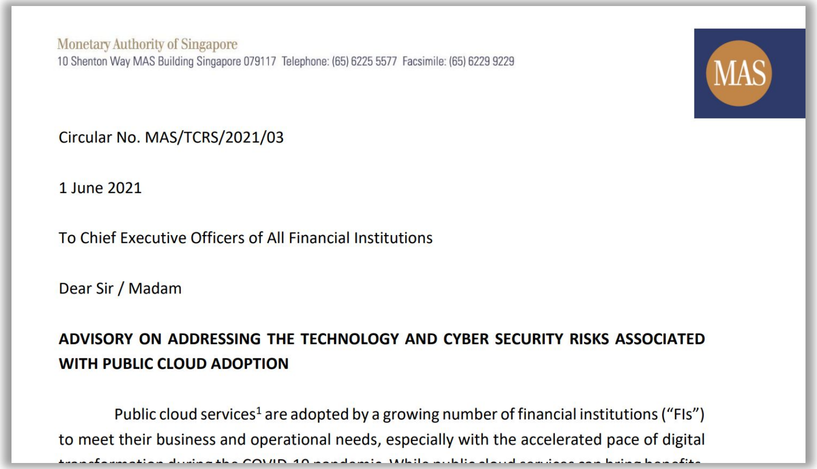
DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics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



Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117 Telephone: (65) 6225 5577 Facsimile: (65) 6229 9229

Circular No. MAS/TCRS/2021/03

1 June 2021

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE TECHNOLOGY AND CYBER SECURITY RISKS ASSOCIATED WITH PUBLIC CLOUD ADOPTION

Public cloud services[1] are adopted by a growing number of financial institutions ("FIs") to meet their business and operational needs, especially with the accelerated pace of digital transformation during the COVID-19 pandemic. While public cloud services can bring benefits

Link

"…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 (…)"**

FINOS Addressing Some of the Key Challenges

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

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.

Ultimately, this allows us to address:

Fragmentation & Complexity of Regulatory Landscape

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

The need for a Financial Services 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".

FINOS

FINOS Common Cloud Controls (CCC) aims to describe consistent controls for compliant public cloud deployments in the financial services sector. This project seeks to address the challenges of cybersecurity, resiliency, and compliance in cloud services across major cloud service providers (CSPs).

FINOS

1. Defining Best Practices Around Cloud Security

CCC aims to standardize cloud security controls for the banking sector. Provides a common set of controls that CSPs can implement to meet the requirements of financial services firms. Collaborative effort ensures robust and representative controls.

2. One Target For CSPs to Conform To

Prevents CSPs from needing to conform to multiple standards set by different financial services firms. Aims to provide a single, unified target for CSPs.

FINOS

3. Sharing The Burden Of A Common Definition

CCC reduces the burden of compliance for CSPs by providing a common definition of controls. Controls are cloud-agnostic, allowing CSPs to implement them within their own infrastructure.

3. Sharing The Burden Of A Common Definition

CCC reduces the burden of compliance for CSPs by providing a common definition of controls. Controls are cloud-agnostic, allowing CSPs to implement them within their own infrastructure.

FINOS

4. A Path Towards Common Implementation

CCC works in tandem with FINOS' **Compliant Financial Infrastructure** project, which provides financial services firms with a one-stop shop for secure cloud infrastructure deployment.

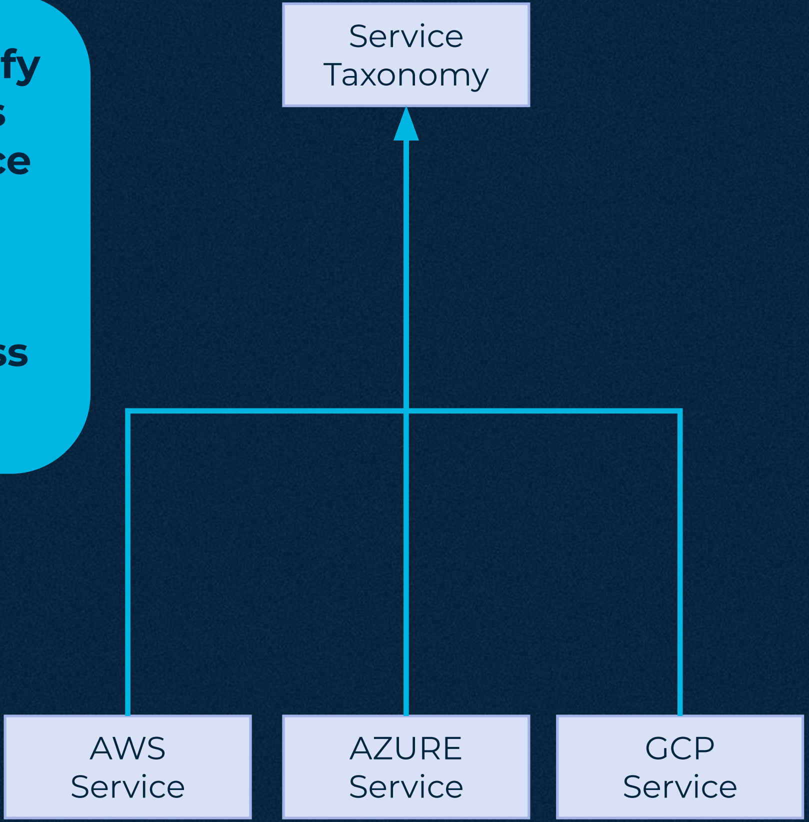
5. A Path Towards Certification

CCC Envisions offering certification for CSPs who conform to the CCC standard in the future.

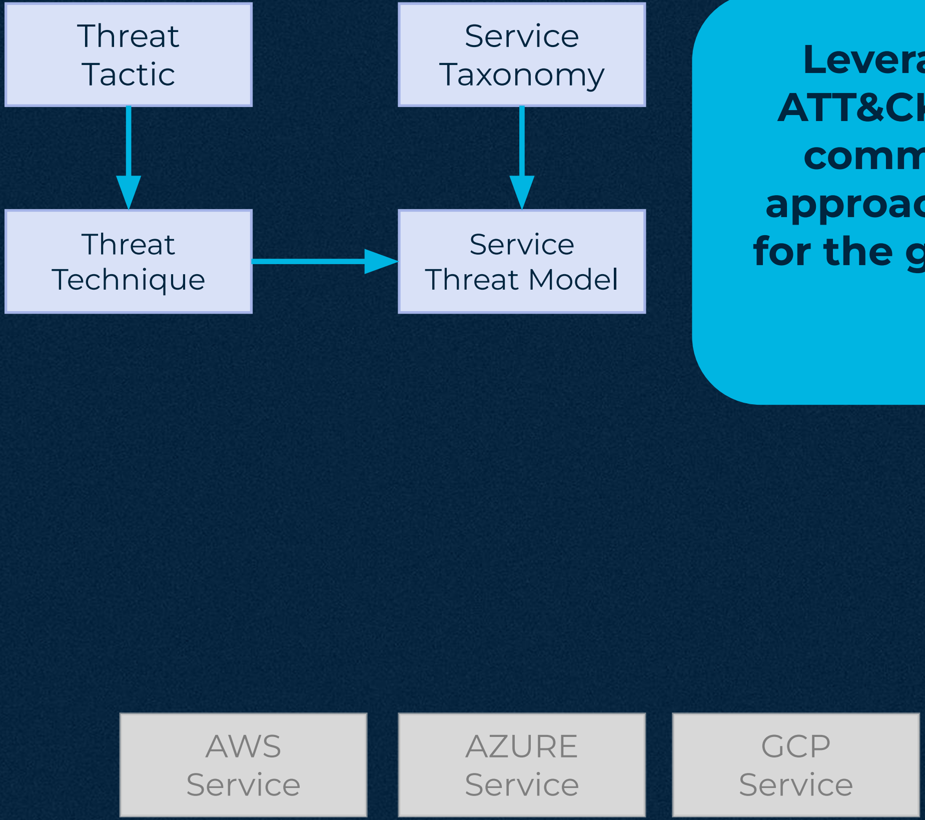
FINOS Common Cloud Controls – Putting it all Together

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

This identifies potential service alternatives across CSPs

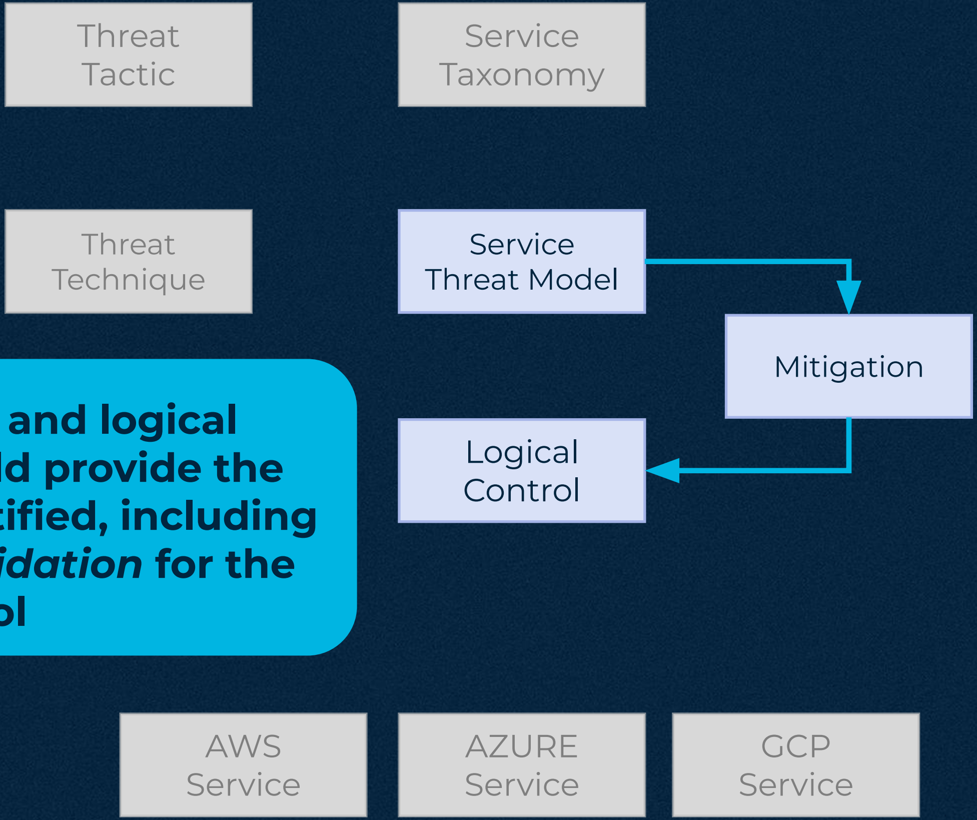


FINOS Common Cloud Controls – Putting it all Together



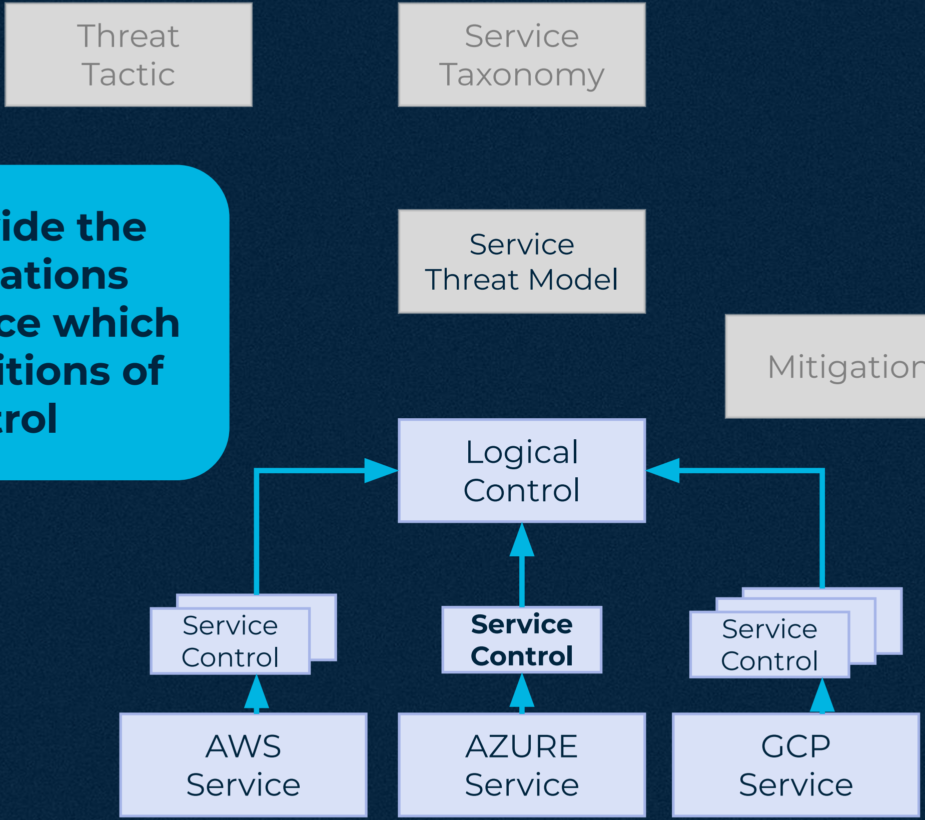
Leveraging the MITRE ATT&CK Framework and common architecture approach, a Threat Model for the generalized service is created

FINOS Common Cloud Controls – Putting it all Together



The mitigations and logical controls that would provide the mitigation are identified, including an appropriate *validation* for the control

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

Steering Committee

In March 2024, CCC elected a steering committee to oversee project governance, consisting of community and financial services seats.

FINOS CCC Maintainer	Representing	Seat
Jon Meadows	citi	FSI
Oli Bage	LSEG	FSI
Simon Zhang	BMO	FSI
Paul Stevenson	Morgan Stanley	FSI
Robert Griffiths	Scott Logic	Community
Eddie Knight	sonatype	Community
Adrian Hammond	Red Hat	Community

Contributing Organizations

citi

sonatype

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Red Hat

Scott Logic

Google

DICTUM MEUM PACTUM LSEG

Microsoft

JupiterOne

controlplane

Morgan Stanley

BMO

GitLab

SYMPHONY SOFTWARE FOUNDATION

Container Solutions

Goldman Sachs

CCC Working Groups

In May 2024, CCC formed new working groups and elected WG leaders to spearhead progress in several key areas

Working Group	When	Chair	Mailing List
Security	4PM UK, 1st and 3rd Thursday each month	Michael Lysaght, Citi	ccc-security
Delivery	4:30PM UK, 1st and 3rd Thursday each month	Damien Burks, Citi	ccc-delivery
Communications / All Hands	5PM UK, 1st and 3rd Thursday each month	Alex St Pierre	ccc-communications
Taxonomy	4:30PM UK, 2nd and 4th Thursday each month	Sonali Mendis, Scott Logic	ccc-taxonomy
Community Structure	5PM UK, 2nd and 4th Thursday each month	Stevie Shiells, Scott Logic	ccc-structure
Duplication Reduction	5:30PM UK, 2nd and 4th Thursday each month	Jared Lambert, Microsoft	ccc-duplication

calendar.finos.org

Find CCC meetings to join. Beginners are advised to start with **CCC Communications WG**.

github.com/finos/common-cloud-controls

Browse our GitHub repo and see what’s being worked on.