

FINOS Common Cloud Controls Open Standard: Project overview



Fintech
Open Source
Foundation



Table of Contents

- Executive Summary
- Background
- Problem statement
- Challenges we're addressing
- Why get involved
- Participation guidelines

Executive Summary

- **Common Cloud Controls Project (CCC)** it's an open standard, originally proposed by Citi, currently undergoing formation with the support of 20+ FINOS Members aiming to develop a unified set of cybersecurity controls for common services across the major cloud service providers (CSPs)
- **Problems we're trying to solve**
 - Lack of unified set of mitigations and controls for FSIs deploying on common cloud services
 - Risks arising from fragmented, complex and often conflicting regulatory landscape
 - Regulators are increasingly concerned about systemic risks of cloud concentration & vendor lock-in
- **CCC will be an open standard/specification, with logical controls and tests**
 - Evidencing could be open source (e.g. via [Compliant Financial Infrastructure](#) project)
 - But could also be simply that CSPs evidence compliance against controls
 - Focus on maximum common denominator: common services only (not trying to cover the full spectrum)
- **The Common Cloud Controls Project would be able to stand up a certification program**
 - Update over time as CSPs update services & threats evolve
 - Tests should be open source to avoid any single entity being a “kingmaker”
 - Existing FINOS [Compliant Financial Infrastructure](#) project can support this effort

Background: Public Cloud Adoption by Financial Services

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

Benefits



Agility &
Scalability



Cost
Optimization



Codified
Controls



Accelerated
Innovation



Geographic
Availability



Resilience

Challenges



Shared
Responsibility



Scarcity of
Skills



Regulatory
Environment

Regulatory landscape: 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



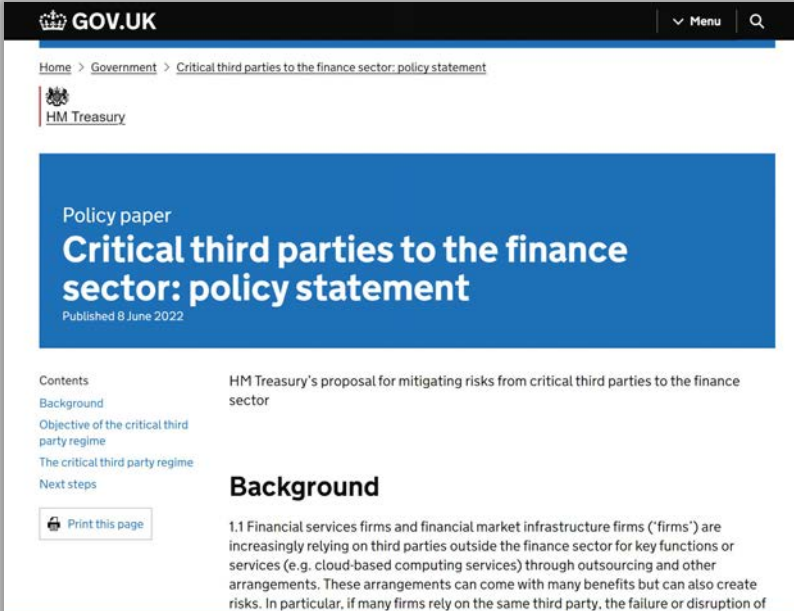
[Link](#)

Regulatory landscape: UK HM Treasury

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

June 2022

[Link](#)



The screenshot shows the HM Treasury website page for the policy statement. The page has a blue header with the GOV.UK logo and a navigation menu. Below the header, there is a breadcrumb trail: Home > Government > Critical third parties to the finance sector: policy statement. The main content area features a large blue banner with the text 'Policy paper Critical third parties to the finance sector: policy statement' and 'Published 8 June 2022'. Below the banner, there is a table of contents with links to 'Background', 'Objective of the critical third party regime', 'The critical third party regime', and 'Next steps'. A 'Print this page' button is also visible. The 'Background' section is currently selected and shows the beginning of the text: '1.1 Financial services firms and financial market infrastructure firms (“firms”) are increasingly relying on third parties outside the finance sector for key functions or services (e.g. cloud-based computing services) through outsourcing and other arrangements. These arrangements can come with many benefits but can also create risks. In particular, if many firms rely on the same third party, the failure or disruption of

“(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**”

Regulatory landscape: 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 a press release from the European Council, dated 28 November 2022. The title is "Digital finance: Council adopts Digital Operational Resilience Act". The text explains that the EU is strengthening the IT security of financial entities to address the risks of cyber attacks. It mentions that the Council adopted the Digital Operational Resilience Act (DORA) to ensure the financial sector can stay resilient through severe operational disruption. A quote from Zbyněk Stanjura, Minister of Finance of the Czechia, states that banks and other companies already have plans in place for their IT security, and the harmonised legal requirements will further improve their ability to function during a large-scale attack. The bottom of the page notes 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 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

[Link](#)

Regulatory landscape: Monetary Authority of Singapore

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

June 2021



Monetary Authority
of Singapore

[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... and concentration risks (...)**

And hot of the press: White House RFI - July 2023

[Link](#)



THE WHITE HOUSE



[Administration](#) [Priorities](#) [The Record](#) [Briefing Room](#) [Español](#) [MENU](#)

JULY 19, 2023

Fact Sheet: Office of the National Cyber Director Requests Public Comment on Harmonizing Cybersecurity Regulations

 › [ONCD](#) › [BRIEFING ROOM](#) › [PRESS RELEASE](#)

[RFI Cybersecurity Regulatory Harmonization](#)

Today, the White House Office of the National Cyber Director (ONCD) is announcing a request for information (RFI) on cybersecurity regulatory harmonization and regulatory reciprocity. The RFI builds on the commitment the Administration made in the National Cybersecurity Strategy to “harmonize not only regulations and rules, but also assessments and audits of regulated entities.” The RFI advances one of the 69 initiatives that were

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...
- ...but our regulators are increasingly moving towards establishing and enforcing technical standards

Why is this important to FINOS members?

- Financial services companies are responsible for institutional risk management, not vendors.
- FINOS members have the institutional knowledge to develop an *appropriate* Cloud standard, and the critical mass to work with regulators and CSPs to drive adoption of a standard that benefits all.

What is being proposed?

- The proposed *Common Cloud Controls Project* would be 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”

Addressing (some of) these Challenges

Our regulators have identified some consistent thematic challenges as an industry we can help to address

- | | |
|---|--|
| Cloud Concentration : | <i>The inability to move workloads between Cloud Service Providers</i> |
| Inconsistency of cyber controls: | <i>Missing or misconfigured controls results in increased Cyber risk</i> |
| Scarcity of skilled workforce: | <i>CSP implementations vary greatly; competition for talent is intense; complex skill set requirements</i> |

And ultimately, we could help address...

- | | |
|--|--|
| Fragmentation & complexity of regulatory landscape: | <i>Focus by multiple regulatory agencies simultaneously creates risk to Financial Services firms</i> |
|--|--|

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
- Mitigate cloud concentration risks and vendor lock-in

- **CSPs**

- Collaboratively define a standard in accordance to 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

- **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

How to get involved?

- Project will kick-off in early August 2023 and undergo an initial members-only formation stage ahead of open sourcing
- If you are a FINOS member, please reach out to membersuccess@finos.org
- If you are not a FINOS Member, you can join [here](#) or express your interest to learn more [here](#)

References

Asset	Entity	TYPE	DATE
The Financial Services Sector's Adoption of Cloud Services	U.S. Department of the Treasury	Regulatory Report	Feb 2023
Critical third parties to the finance sector: policy statement	UK HM Treasury	Policy Statement	June 2022
DORA	EU Council	Legislation	June 2022
Addressing the technology and cyber security risks associated with public cloud adoption	Monetary Authority of Singapore	Recommendation / Advisory	June 2021
A new threat to financial stability lurks in the cloud (Feb 16 2023)	Financial Times	Press	Feb 2023