FINOS Common Cloud Controls Open Standard: Project overview
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
Public Cloud Placement offers *significant* benefits to Financial Services... 
...as well as some *unique challenges, especially with Regulators*
“...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.”
“(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”
“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”
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**
Fact Sheet: Office of the National Cyber Director Requests Public Comment on Harmonizing Cybersecurity Regulations

JULY 19, 2023

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:

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud Concentration</strong></td>
<td>The inability to move workloads between Cloud Service Providers</td>
</tr>
<tr>
<td><strong>Inconsistency of cyber controls</strong></td>
<td>Missing or misconfigured controls results in increased Cyber risk</td>
</tr>
<tr>
<td><strong>Scarcity of skilled workforce</strong></td>
<td>CSP implementations vary greatly; competition for talent is intense; complex skill set requirements</td>
</tr>
<tr>
<td><strong>Fragmentation &amp; complexity of regulatory landscape</strong></td>
<td>Focus by multiple regulatory agencies simultaneously creates risk to Financial Services firms</td>
</tr>
</tbody>
</table>

And ultimately, we could help address...
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

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