Title: Accelerating Cloud Security and Compliance for FSI: The Synergy Between FINOS CCC and CFI Projects

Introduction

In the rapidly evolving landscape of financial services, regulatory compliance and security are paramount. The FINOS Common Cloud Controls (CCC) project aims to address these concerns by creating a comprehensive cloud services taxonomy and a threat-informed security control catalog specifically tailored to the financial services industry. The objective of the CCC project is to provide a standardized framework that can be universally applied across various cloud services, ensuring that financial institutions can efficiently manage security and compliance risks. In this talk, we will explore the interface between the CCC project and the FINOS Compliant Financial Infrastructure (CFI) project, which focuses on accelerating the development, deployment, and adoption of compliant infrastructure services.

By developing a standardized cloud services taxonomy and threat-informed security control catalog, the CCC project aims to provide a critical foundation for the CFI project's efforts to accelerate the adoption of compliant infrastructure services. In this talk, we will demonstrate how the integration of these projects will streamline regulatory compliance, enhance security, and promote the widespread adoption of cloud services in the financial sector, ultimately benefiting financial institutions and their customers.

This collaboration between the CCC and CFI projects exemplifies the power of open-source initiatives in addressing industry-wide challenges. By leveraging the collective expertise of the FINOS community, these projects will deliver solutions that are robust, scalable, and aligned with the evolving needs of the financial services industry.

In this talk, we will detail how the interface between the CCC and CFI projects is expected to create a cohesive framework for managing cloud security and compliance in the financial services industry.

Integration of Taxonomy and Controls

We will discuss how the cloud services taxonomy and security control catalog being developed by the CCC project will serve as a foundational element for the CFI project. The taxonomy will provide a standardized definition of cloud services, which the CFI project can use to categorize its infrastructure services. The security control catalog will inform the development of IaC templates and compliance documentation, ensuring that they align with the latest threat intelligence and regulatory requirements.

Vetted Infrastructure as Code

We will show how the IaC templates developed by the CFI project will be informed by the security controls catalog from the CCC project. By leveraging these controls, the IaC templates

will be pre-configured to meet regulatory and security requirements, reducing the burden on financial institutions to manually configure and validate their infrastructure. This integration will accelerate the deployment of compliant infrastructure services and promote the adoption of secure cloud practices.

Assessments/Validation

We will demo a set of validators that can be used with an IaC template to be integrated in a non-prod CI/CD pipeline to verify compliance before deployment. This will provide a high level assurance that their IaC is effective and performs as expected. By using such validators the financial institutions deploying the infrastructure can be certain that their services meet the industry standard compliance and regulatory requirements.