Cloud Security Initiative for the Financial Sector Charter

Introduction

The Cloud Security Alliance (CSA) and the Cyber Risk Institute (CRI) have teamed up on a new initiative to provide the financial community with new resources to map and integrate CSA’s Cloud Controls Matrix (CCM) and CRI’s Financial Services Cybersecurity Profile (Profile).

The CSA’s CCM is considered the standard for cloud security assurance and compliance. Similarly, the CRI Profile is emerging as the leading cybersecurity assessment for the financial services industry. The integration of the two best practices will provide a new cybersecurity assurance framework to satisfy the requirements of financial institutions adopting cloud computing technologies.

This activity will be performed by an ad-hoc created Working Group composed by members of the CSA Financial Services Stakeholder Platform (FSSP), CSA CCM Working Group and CRI and BITS designated members. This group will be called the “Cloud Security Initiative for the Financial Sector Working Group”.

Purpose

The Cloud Security Initiative for the Financial Sector Working Group will work to:

- define the scope, objectives, and technical specification of the CSA-CRI Cloud Security Framework for Financial Services (from now on the CSA-CRI Framework)
- define the value proposition and Go-To-Market (GTM) strategy of the FI Cloud Security Framework.

More specifically the Cloud Security Initiative for the Financial Sector Working Group will:

- discuss a mapping and gap analysis between the CRI Profile and the CSA CCM V4.
- Suggest how to integrate input from the CRI Profile into the CCM V4 Implementation Guidelines.
• Suggest how to integrate input from the CRI Profile into the CCM V4 Auditing Guidelines.
• Validate and/or develop a new framework that integrates CCM V4 and CRI Profile.
• In case the CRI Profile requirements would exceed the CCM V4 requirements, suggest how to integrate the missing requirements/controls into an updated version of the CCM.
• Define, if required, additional documentation and guidelines in order to facilitate the implementation of the CSA-CRI Cloud Security Framework.
• Create awareness material to educate Cloud Service Providers (CSPs) and Financial Sector Regulators.

Work towards consensus among its members on any suggested goals, alternatives, improvements or changes.

Member Profile Requirements
• Familiar with best practices and control frameworks such as the Cloud Control Matrix (CCM), the CRI Financial Services Cybersecurity Profile.
• Working in the Financial Services Industry and a subject matter expert (SME) in sector-specific security needs and requirements, or be a SME with expertise in the Financial Services Industry.

Decision Making
The primary decision-making mechanism is based on consensus. In case consensus is not reached, the group leaders / co-chairs will escalate the matter to the CSA and CRI/BITS executive teams.

Project Outcome
The process will be considered a success if:
• The scope, objective and technical specification of the – FI Cloud Security Framework for Financial Services has been defined
• The Cloud Security Initiative for the Financial Sector Working Group completes the mapping and integration of the CSA’s Cloud Controls Matrix (CCM) to the CRI Financial Services Cybersecurity Profile (“the Profile”) to create a “FI-Cloud Security Framework” for the financial services industry and suggest how to integrate input from the CRI Profile into the CCM V4 Auditing Guidelines
• The value proposition and Go-To-Market (GTM) strategy has been defined
• The industry is engaged in a meaningful way in evaluating the proposed integration and improvements in reviewing and commenting on the key processes and strategy;
Awareness materials to educate CSPs and Financial Sector Regulators have been created

A roadmap for possible future collaboration has been defined

Recommendations and decisions fit into the context of the overall industry and recognize and respect the unique aspects and needs of the cloud community specifically the Financial Services Sector;

Appropriate CSA, CRI and BITS staff is involved throughout the process to avoid surprises that lead to delays.

**Description of Sub-Working Groups**

1. **The Framework Working Group**: Ad hoc group that will meet 4-8 times for 1-2 hours per meeting in early 2021 to ensure that Boston Consulting Group’s addition of the Cloud Security Alliance’s (CSA) Cloud Control Matrix (CCM) to the Profile includes the correct overall architecture (i.e. do the columns in the Profile capture the right elements?)
   a. This will generally include Deputy CISOs, Deputy CIOs, and/or GRC officials from financial institutions, cloud service providers, and potentially trade associations.

2. **Validation Working Group**: Ad hoc group that will meet 4-8 times for 1-2 hours per meeting in mid-2021 to ensure the resulting mapping produced by the Integration Strategy Group and the associated technical details are accurate (i.e. do the rows in the Profile contain the right information?).
   a. This will generally include Deputy CISO/Deputy CIO/GRC delegates who understand the technical requirements and details of cybersecurity and cloud controls, as well as whether the controls are the responsibility of the financial institution, cloud provider, or both.

3. **Education and Policymaker Team**: Ad hoc group that will meet 2-3 times for 1-2 hours per meeting in mid-2021 to develop consistent messaging to be used during promotion of the resulting Profile with Cloud controls to regulators and industry.
   a. This will generally include a variety of policy, communications, and government relations officials.

**Terms of membership**
Members agree to volunteer until the completion of the review process and possibly through the improvement process.

A member’s position on the Cloud Security Initiative for the Financial Sector may be declared vacant if the member:

- Resigns from the Cloud Security Initiative for the Financial Sector (this should be in writing and forwarded to the CSA, CRI and BITS leads).
- Fails to attend more than two meetings or send a designee without prior notice.
- In a case where a member’s position is declared vacant, the CSA, CRI and BITS can appoint an alternative representative from the same area of expertise to fill the position.

**Group Operating Guidelines**

**Convening of Meetings**
- Meetings will be held at the time and place agreeable to the Cloud Security Initiative for the Financial Sector. It is anticipated that CSA, BITS, and CRI will have an initial organizing call discuss how to handle issues of a specific nature that might delay or disrupt development progress, the CSA CCM v4.0, and STAR certification.
- The first organizing call for all group members would take place in early April. It would consist of 2 half hour sessions. A primer on the Profile for those that are not familiar and then a follow-on meeting to discuss the work and working group constructs.
- Cloud Security Initiative for the Financial Sector members will be informed of meetings through email or other electronic means, at least one to two weeks prior to the meeting, if practicable.

Estimated time investment from members
- The time commitment for the various groups is described above in the description of sub-working groups.

**Communication**
- Meetings will be advertised in the CSA Circle Community.
- Project documents and notices will be posted within a dedicated Circle Community.
- Email: CSA and CRI Project coordinators should be copied on all correspondence, and if the project coordinator chooses to open a dialogue via email, all Cloud Security Initiative for the Financial Sector members will be copied.

**Conduct of meetings**
- Meetings will be open to all.
- Meetings will be facilitated by CRI, BITS and CSA coordinators.
- Informed alternates are acceptable and encouraged if the Cloud Security Initiative for the Financial Sector members cannot attend.
- After all meeting agenda items have been addressed, time will be provided for non-agenda items to be addressed if time permits.
Meetings will end with a clear understanding of expectations and action items for next steps.

Meetings are expected to be one hour. Extension of time, in 15-minute increments, will require the consent of the majority of members attending that meeting.

The CRI, BITS and CSA coordinators will keep a record of meeting attendees, key issues raised, and actions required.

The previous meeting record and a meeting agenda will be forwarded to members of the Cloud Security Initiative for the Financial Sector at least one week before the next meeting.

**Roles and Responsibilities**

Cloud Security Initiative for the Financial Sector is an advisory group to the CSA's CTO Office and the CRI:

Cloud Security Initiative for the Financial Sector members agree to:
- Provide specific industry local expertise, including identifying emerging local and global issues;
- Review project documents and comment promptly;
- Attend all meetings possible and prepare appropriately;
- Gather information/feedback from their constituents as practicable before each meeting;
- Articulate and reflect the interests that working group members bring to the table;
- Maintain a focus on solutions that benefit the entire project objectives.

The CSA CRI, and BITS Group Coordinators agree to:
- Provide Cloud Security Initiative for the Financial Sector members the opportunity to collaborate with other agencies and groups on making recommendations for the project;
- Effectively manage the scope and, schedule;
- Keep Cloud Security Initiative for the Financial Sector members informed of progress;
- Provide technical expertise;
- Brief local decision makers and produce briefing materials and reports;
- Provide early notification of Cloud Security Initiative for the Financial Sector meetings and provide ten working days to review and comment on technical reports and other documents;
- Manage logistics for meetings; and
• Explain the reasons when deviations are taken from Cloud Security Initiative for the Financial Sector recommendations.