cloud security alliance®

Charter 2021

Open Certification Framework - OCF Working Group

Release 3: 03/01/2021

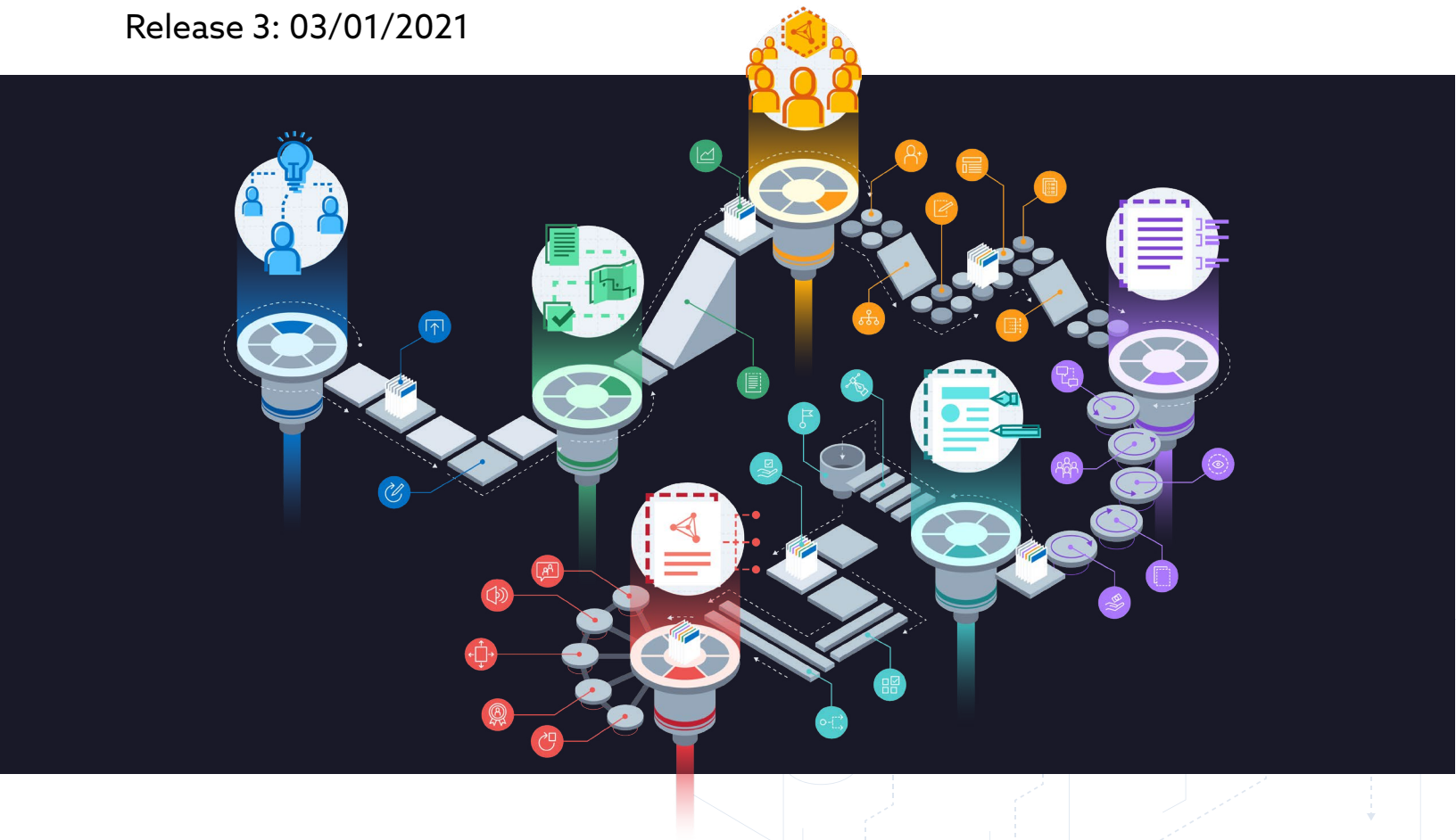

Table of Contents

Working Group Executive Overview

Mission

The mission of the Open Certification Framework Working Group is to develop, maintain, review, update, support the development and deployment of all the certification and attestation schemes included in the CSA Security Transparency Assurance Risk (STAR) Program. The OCF WG focuses on information security and privacy certification schemes for processes and products in the areas of cloud computing and mobile.

Working Group Scope and Responsibilities

The Cloud Security Alliance has identified gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. Consumers do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection and privacy capabilities and service portability.

The CSA Open Certification Framework (OCF) is an industry initiative to allow global, trusted independent evaluation of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification and/or attestation according to the Cloud Security Alliance's industry leading security guidance and control framework.

The objective of the program will be to harmonize with existing third-party certifications and audit standards to avoid duplication of effort and cost.

The CSA OCF is based upon the technical best practices and control frameworks defined within relevant CSA's Working Group, such as for instance the Cloud Control Matrix (CCM), the Consensus Assessment Initiative Questionnaire (CAIQ), the Level Agreement research initiatives, as well as the IoT Control Framework.

The CSA OCF will support several tiers, recognizing the varying assurance requirements and maturity levels of providers and consumers. These will range from the CSA Security, Trust Assurance and Risk registry (STAR) self-assessment to high-assurance specifications that are continuously monitored.

Discussions and decisions/changes proposed by the OCF and its working groups are considered privileged and confidential and are not to be made public until either the proposed changes have been finalized or a vote has been taken and so documented.

Working Group Membership

Eligible members of the OCF WG are:

- CSA enterprise customer corporate members (Enterprise Users)
- CSA solution provider corporate members (CSPs)
- International, Regional, National Regulatory Bodies, Agencies and Institutions (European Commission, European Data Protection Board (EDPB), ENISA, BSI Germany, METI, IDB – IDA, NIST, FedRAMP, USA DoD, USA FTC, etc)

- SDOs & other organizations (e.g. ISO/IEC / JTC 1 / SC27, SC38, ITU-T, ETSI, W3C, ISACA, AICPA, JIPDEC, JASA, etc)
- Representatives of relevant research project not directly run under the auspices of the CSA, but relevant to the activities of the OCF WG (e.g. EU-SEC.)
- Representative of trade and users associations (e.g. EuroCIO, DigitalEurope, ECSO, etc.)

Working Group Structure

Co-Chairs

The working group will be led by co-chairs in addition to the selected leadership. Co-chairs must be members of the CSA, unless the CSA Executive Team has granted an exception. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research. Responsibilities of the co-chair include:

- Define the work plan for each year (e.g., meetings and expected deliverables)
- Ensure progress of work according to the work plan
- Report to the CSA Executive Team on execution risks and suggest possible solutions
- Convene meetings when necessary and act as Chairperson of OCF.
- Ensure deliverables are adequately resourced and Led
- Ensure that guidance provided in the current OCF charter is followed
- Ensure that relevant documents are circulated to OCF members

Committees

The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.

Sub-Work Groups

Ad hoc sub-work groups composed of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

Alignments with Other Groups

The OCF working group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work, on demand basis. The list other groups that the OCF working group will be working closely with includes, but is not limited to:

CSA Cloud Control Matrix Working Group:

- Specifically collaborating on the implementation of CCM related controls across the 3 levels of assurance and transparency of STAR

- CSA PLA Working Group:
- Specifically collaborating on the development of a scheme to certify organization against the
- requirements included in the PLA Code of Practice v3.1.
- IoT Matrix
- Evaluate the extension of the STAR program to IoT (i.e. implementation of a certification for Edge
- Computing and IoT devices)
- International Standardization Council (ISC):
- Specifically collaborating on the identification of international standardization opportunities for
- the STAR program components as well as relevant input from SDOs that could serve to improve the program.
- Additional groups:
  - ENISA
  - ISO/IEC SC 27 and SC 38
  - NIST
  - AICPA
  - The German Federal Office for Information Security (BSI)
  - GSA/FedRAMP
  - GAIA-X
  - CCCS -Canadian Centre for Cyber Security
  - IMDA Singapore
  - CMMC - DOD

Operations

Advisory

The CSA Working Group will be advised by various SMEs and councils including but not limited to the International Standardization Council (ISC) and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle

The CSA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives: https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

Peer Review

We will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The working group will hold conference calls no less than bi-monthly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

Decision-making Procedures

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1. The voting procedures are as follows:
   a. By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
   b. By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2. The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3. In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

Actions/Activities

The list of actions includes:

- Completion of revised strategy for the OCF Level 3 – STAR Continuous Certification.
- Completion and implementation of the Privacy Certification (currently based on the
- Code of Conduct for GDPR Compliance.
- Produce awareness materials for the various STAR Program target audiences.
- Evaluate the feasibility of an IoT extension of STAR.
- Evidenced Based Self-Assessment Pilot Program

Each of the above mentioned actions will have one or more associated deliverables. The final list of deliverables will be included in the STAR Program annual work plan.

Deliverables will be governed by CSA's intellectual property rights policy.

Duration

This charter will be valid until 30 April 2022 and it will be updated to reflect any changes in the OCF WG objectives and priorities.

Charter Revision History

Date	Authored and Approved by
November 2015	OCF WG
March 2016	OCF WG
Sept 2017	OCF WG
April 2019	OCF WG
March 2020	OCF WG
January 2021	OCF WG