Enterprise Authority to Operate

Small and mid-sized Vendors

With optional Premium Consultancy

Working Group Charter

Release 1.0 as of 24 April 2023

# Mission Statement

The mission of the Enterprise Authority to Operate (EATO) Working Group is to develop, maintain, review, update, support and deploy of a concentrated assessment and certification and attestation scheme catering to small and mid-sized vendors / service providers, with the aim of enabling such vendors to achieve a certification accepted also by larger Corporate Clients, including such clients in tightly regulated industries such as Finance.

The EATO targets a comprehensive assessment of risks inherent in Anything as a Service (XaaS) products with underlying Cloud based infrastructure or platform, with particular focuses on information security and privacy, but also covering Business Continuity, Data Retention, Archiving, and vendor / service provider controls and risks.

The EATO Working Group defines and sets auditing requirements and minimum standards required to be achieved to pass the EATO assessment and certification.

The EATO Working Group defines and scopes consultancy services to small and mid-sized vendors / service providers, to enable such vendors to derive and implement architectures and designs compliant with the information security and privacy certification schemes defined by the Enterprise Authority To Operate Working Group.

The mandate to consultancy services will be scoped to guide vendors to build their services adhering to Security by Design principles which lead to compliance with the Enterprise Authority To Operate requirements, and with this, enable vendors to achieve assurance and certification according to the Enterprise Authority To Operate control requirements.

All services and deliverables as defined by the Enterprise Authority To Operate Working Group will become part of the Cloud Security Alliance products and can be delivered by the Cloud Security Alliance itself or by licensed service partners explicitly nominated, empowered and agreed by the Cloud Security Alliance.

# Working Group Background, Scope with Objectives and Key Results, Impact and Outcomes, Outputs

## Background

The CSA EATO Working Group has identified gaps within the understanding and implementation of small to mid-sized Cloud based XaaS regarding data protection and information security, particularly when processing sensitive data of highly regulated industries, inhibiting market adoption of such services. As consuming Corporate Customers are typically large size, global and have to abide by multiple and tight regulations, such Corporate Customers either cannot adopt these Cloud based XaaS or have to perform individual heavy weight Risk & Cloud Control Assessments which lead to complex remediation requirements towards the vendor and their services. This results in redundant cost and effort intensive assessments and remediation processes, both to the vendor and the several potential Corporate Customers.

## Scope

## Objectives and Key Results

* Establish an industry standard controls and assessment framework for XaaS catering to customer firms in highly regulated industries
* Establish a global, trusted independent assessment service of small and mid-sized Cloud based XaaS providers against the industry standard enhanced controls framework.
* Establish a trusted and independently certified remediation consultancy service enabling XaaS Providers to change design of their services implementing security by design.
* Provide a trusted certification to subscribing firms enabling to reduce cost and risk.

## Impact and Outcomes

* Improvement of information security by design across XaaS Providers:
  + By incentivizing to conduct an assessment, and only one instead of many
  + Reducing cost for XaaS Providers for the assessment
  + Focusing effort on remediation against one central / combined set of findings instead of many disparate and potentially conflicting requirements
* Efficiency gains for Subscribing Firms as there is only one central assessment instead of one each per each firm wanting to use the XaaS Providers’ services
* Reduction of cost and effort for Subscribing Firms using a shared trusted assessment
* Globally accepted and trusted Certificate which also covers effective remediation performed and validated.

## Outputs

* Controls Framework
  + Based on CCMv4
  + Extending CCMv4 by additional controls
  + Sharpening CCMv4 existing controls
  + With explicit external guidance re what the expected security by design features are
  + Generally, based upon the technical best practices and control frameworks defined within relevant CSA’s Working Groups, 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.
* Assessment and Auditing Framework and Guidance
  + With defined acceptance and evidencing criteria
  + With explicit methodology to derive findings and expected remediation requirements
  + With logic determining breach likelihood, impact and residual risk exposure
* Remediation and Consultancy Guidance
  + Security by Design architecture blueprints for upfront / new implementation guidance
  + Remediation blueprints for most common findings / cloud platforms for existing services
  + Consultancy framework and guidance re what are acceptable designs and compensating controls for partially adequate implementations
  + Criteria for evidencing of findings remediation, confirmation of proof of remediation
  + Logic for re-determining remaining (after remediation) breach likelihood, impact and residual risk exposure
* Certification Framework
  + Definition of acceptance criteria for assessment results and remediation implemented:
    - Findings / likelihood / impact / residual risks
    - Full / partial remediation with translation into remaining residual risks
  + Certification levels and suitability levels: differentiate according to data classification, region, industry, potential further criteria
  + Possible cycles of progressing from lower to higher level / more comprehensive certifications
  + With logic determining final (after remediation) breach likelihood, impact and residual risk exposure
  + With re-certification / certification renewal framework and process
  + With acceptance and accreditation by major standardization bodies
  + With mapping to major auditing frameworks to harmonize with existing third-party certifications and audit standards to avoid duplication of effort and cost
  + *Proposal: Position as a Premium Certificate which goes beyond existing certification schemes because it addresses specific regulatory requirements applicable to tightly regulated industries and applicable to restricted jurisdictions.*
  + *Proposal: Support several tiers, recognizing the varying assurance requirements, in particular also with respect to varying regulatory requirements applicable to Corporate Customers*
* Subscription Model
  + Assessments are financed by subscriptions not auditing fees
  + Remediation consultancy is charged directly by consultancy company to the XaaS Provider
  + Subscribers buy a volume of assessments / certifications (t.b.d., possibly multiple models meaningful to differentiate whether a subscriber wants only to buy the assessment but perform acceptance individually, or whether a subscriber wants only to deal with fully remediated and certified to be fully compliant XaaS Providers)
  + Single case purchase / special purpose / small volume purchases models to be determined

## Licensing of Outputs

The CSA may license either the EATO assessment service, and / or the assurance and certification service, and / or the consultancy service to authorized 3rd parties qualified and vetted by the CSA.

# Working Group Membership

Eligible members of the EATO Working Group are:

* CSA enterprise customer corporate members (Enterprise Users)
* CSA individual members. If CSA individual members represent a corporation, with the aim of the corporation to become CSA corporate member.
* CSA solution provider corporate members (CSPs)
* 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 cooperate members of the CSA, unless the CSA Executive Teams have 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 EATO Working Group.
* Ensure deliverables are adequately resourced and Led
* Ensure that guidance provided in the current EATO charter is followed
* Ensure that relevant documents are circulated to EATO Working Group 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-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.

# Alignment with other Groups

The EATO 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 EATO 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 OCC Working Group:

* Alignment regarding the STAR certification scheme

Charter of Trust Working Group:

* Alignment regarding controls and assessment / certification framework

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

## Decisions

Discussions and decisions/changes proposed by the CSA EATO Working Group and its related CSA 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.

## Advisory

The CSA EATO 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 EATO 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

The CSA EATO Working Group will seek CSA’s help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

# Communication Methods

## Infrastructure & Resource Requirements

The CSA EATO 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.

## Working Group Conference Calls and in-person Meetings

The CSA EATO Working Group will hold in-person meetings and / or conference calls as needed but no less than 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

## Definition of Majority

1. A majority shall consist of more than half of the members present and voting. If multiple participants represent a member, then their votes shall be counted as one vote for the member, not multiple.
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.

## Abstentions of more than fifty Percent

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.

## Voting Procedures

1. The voting procedures are as follows:
   1. 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
   2. 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

* Definition of EATO requirements, controls, questions, and guidance set.
* Derivation of EATO auditing guidelines and minimum acceptance criteria set
* Derivation of EATO assessment and risk / remediation framework and governance
* Completion and implementation of the EATO Certification.
* Produce awareness materials for the various STAR Program target audiences.
* Educational materials.
* 3rd party consultancy requirements.

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 31 Dec 2024 and it will be updated to reflect any changes in the EATO Working Group objectives and priorities.

# Charter Revision History

|  |  |  |
| --- | --- | --- |
| Version and Date | Artefact | Approved by |
| V0.1 / 29 May 2022 | Draft first version created | Draft |
| V0.8 / 08 September 2022 | Feedback from Working Group initial review incorporated, created version for final Working Group review and feedback (pre-CSA Management and Peer review) | Draft |
| V0.9 / 12 October 2022 | Feedback by CSA Management and initial Working Group Members incorporated, in particular eliminated consultancy Business Model from Charter and focused on setting the framework with auditing requirements and requirements towards consultancy. | Draft |
| V1.0 / 24 March 2023 and 24 April 2023 | 24 March 2023:  Modified Name and content to reflect agreements with Jim Reavis and Working Group on 13 March 2023.  24 April 2023:  Further added objectives, impact, outcomes and outputs from Working Group presentation deck as per agreement in the Working Group on 13 March 2023. Extended valid due date of this Charter to 31 Dec 2024 to reflect the time it has taken to start up and operationalize the Working Group. | Final |