Enterprise Authority To Operate (EATO) Certification Framework

Release Date: 07/02/2024

Enterprise Authority To Operate Working Group
Overview and Audience

The Enterprise Authority to Operate (EATO) Framework is an assessment, remediation, and certification framework that targets small and mid-sized Anything-as-a-Service (XaaS) providers. It also targets their entire underlying supply chain who want to offer their services to customers in highly regulated industries or for processing sensitive data.

The EATO Framework is based on CCMv4, has augmented controls to reflect tight regulatory requirements, is comprehensively audited with findings which have to be remediated under independent guidance before the certification is issued.

Cost and effort is reduced by conducting a single assessment / audit / remediation / certification cycle rather than multiple parallel, which is financed by a shared subscription model.

This assessment, audit, remediation and certification scheme focuses on information security and privacy.

Overview

The Enterprise Authority to Operate (EATO) Framework is an assessment, remediation, and certification framework that targets small and mid-sized Anything-as-a-Service (XaaS) providers. It also targets their entire underlying supply chain who want to offer their services to customers in highly regulated industries or for processing sensitive data.

The EATO Framework is based on CCMv4, has augmented controls to reflect tight regulatory requirements, is comprehensively audited with findings which have to be remediated under independent guidance before the certification is issued.

Cost and effort is reduced by conducting a single assessment / audit / remediation / certification cycle rather than multiple parallel, which is financed by a shared subscription model.

This assessment, audit, remediation and certification scheme focuses on information security and privacy.

Audience

C-level

Procurers

Auditors/Certification Bodies

XaaS Providers
The EATO Framework: Helicopter View: How does it look like

The EATO Framework consists of four key steps:

• Assessment and audit of compliance of the XaaS against the EATO controls, resulting in findings.
• Remediation of findings under independent guidance.
• Re-Audit of successful remediation of findings.
• Trusted Certification issued based on confirmed closure of the audit findings.

Subscription model with shared funding of the assessment / audit / re-audit / certification cycle
The EATO Framework: Core Components

The EATO Controls Framework is based on the following components:

A controls set based on the CSA Cloud Controls Matrix (CCM) but augmented to apply more detail and more restrictive controls. These controls aim to satisfy regulatory requirements that highly regulated industry customers must abide by.

1. A comprehensive audited assessment against the controls framework. Additional scrutiny is applied toward risks emanating from non-compliance with controls, with particular focus on information security and data protection. Business continuity, data retention, archiving, and vendor/service provider controls and risks are also covered.

2. The audit requires detailed evidence to support concrete design and implementation of the controls. Documentation is actively reviewed and challenged and where necessary, on-site inspection is added to obtain adequate assurance.

3. The audit also allows individual customers to monitor the operating effectiveness of the controls on an ongoing basis.

4. The audit results in findings which require remediation by implementing design changes in the XaaS solutions. Solution providers are accompanied by competent consultancy during the design and implementation phase.

5. Once findings have been remediated, the audit is repeated for these specific findings to assess successful and effective remediation.

6. Only after verification of successful remediation of earlier findings, the EATO certification is issued.
Relation to the CCM

EATO Controls are based on CCMv4, but they are augmented and tailored

Controls Framework

• **Sharpening CCMv4 existing core controls**: to apply stricter and more detailed information security compliance requirements and evidencing scrutiny, catering to the needs of highly regulated corporate customers.
  
  For example, controls on encryption, temporary privileged access management, and cross-border hosting / processing / access have been tightened to achieve a much stricter information protection standard.

• **Extending CCMv4 by additional controls**: where necessary for highly regulated corporate customers.
  
  For example, controls on a customer-specific keys vaulted in a Hardware Security Module for sensitive data, temporary PAM with strict segregation of duties of privileged roles, localization requirements for cloud hosting and services, cross-border access control / prevention for privileged/support user roles and standard user roles.

• **Combined controls**: simplification of repetitive controls with same content in multiple contexts, to reduce the load of the assessment on the XaaS providers and to focus on the compliance with Core Controls.

• **Dropped controls**: A small number have been dropped, to focus on the compliance with Core Controls.

• **With explicit external guidance** re what the expected security by design features are
Impact and Outcomes

Provide a trusted certification to subscribing firms enabling to reduce cost and risk, by the following:

Improvement of information security by design across XaaS Providers by:

- Incentivize an assessment, and only one instead of many.
- Cut the cost for XaaS Providers for the assessment.
- Focus effort on remediation against one central 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.
What’s next
Definition of Auditing Framework, Implementation Guidance and Pilot

Assessment and Auditing Framework, Implementation 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

Pilot with:

- Customer Firms contributing real life SaaS vendor candidates
- SaaS vendor candidates agreeing to become certified under the new Framework
- Auditor Firm to perform the assessment, audit, and re-audit after remediation completion
- Consultancy Firm to accompany the remediation
- CSA to issue certification
Download

https://cloudsecurityalliance.org/artifacts/enterprise-authority-to-operate-eato-controls-framework