The Evolution of STAR

Introducing Continuous Auditing

cloud security alliance®

Acknowledgments

Lead Authors:

Alain Pannetrat
Daniele Catteddu
John DiMaria
John Yeoh
Pete Chronis

CSA Global Staff:

Stephen Lumpe (cover)
Stephen Smith (layout)

Table of Contents

Introduction

The Cloud Security Alliance's (CSA) Security, Trust, Assurance, and Risk (STAR) Registry is a repository that allows Cloud Service Providers (CSPs) to share security, compliance, and privacy controls with current and potential customers. To register with STAR, CSPs must document controls using CSA's Consensus Assessments Initiative Questionnaire (CAIQ), which reflects the cloud security and privacy requirements defined in CSA's Cloud Controls Matrix (CCM).

STAR has three different transparency and assurance levels. STAR Level 1 allows CSPs to self-attest to the security, compliance, and privacy controls in their environment. STAR Level 2 allows organizations to build off of other industry certifications and standards, extending the scope to include controls specific to the cloud. Level 2 requires controls validation as part of a SOC (STAR Attestation), ISO 27001 (STAR Certification), or C-STAR: For the Greater China Market based on GB/T 22239-2008 and GB/Z 28828-2012. While Level 1 provides control transparency, Level 2 offers cloud customers assurance via a third-party independent assessment by a qualified auditor, validating the implementation of CCM controls applicable in the scope of the service.

While STAR Levels 1 and 2 offer significant levels of transparency and assurance, some cloud customers require even greater levels of trust and accountability. For the most demanding cloud technology use cases, CSA created the STAR Level 3 program, further extending the scope of Level 2 to demonstrate continuous, automated, security, compliance, and privacy control effectiveness. CSA Continuous Auditing Certification (aka STAR Level 3) is the most rigorous assurance tier in the STAR program. Level 3-certified services providers can demonstrate that critical security controls are monitored and validated continuously, providing customers with the ultimate level of transparency and assurance.

Value Proposition

Continuous security controls auditing and certification delivers best-in-class security transparency and assurance to customers. Those who adopt continuous controls auditing and certification can expect to:

- Gain market advantage, delivering best-in-class security to customers that may help improve trust, increasing customer acquisition and retention.
- Help reduce cybersecurity risk by creating a mechanism to detect and remediate control deficiencies quickly – allowing you to better protect your company and your customers.
- Reduce customer acquisition and retention costs by streamlining vendor security questionnaires and third-party audits. Leveraging CSA's STAR program CAIQ, registry and audit guidance cuts overhead and allows you to deliver the transparency your customers need.
- Deliver services to meet the needs of the most demanding customers and provide assurance against the most rigorous regulatory frameworks.

How Does STAR Level 3 Work?

Continuous certification combines a Star Level 2 "point-in-time" certification and a continuous assessment (Star Level 3), both validated by an independent third-party auditor. Continuous auditing gives the strongest level of assurance – validating that security controls are functional and operating effectively.

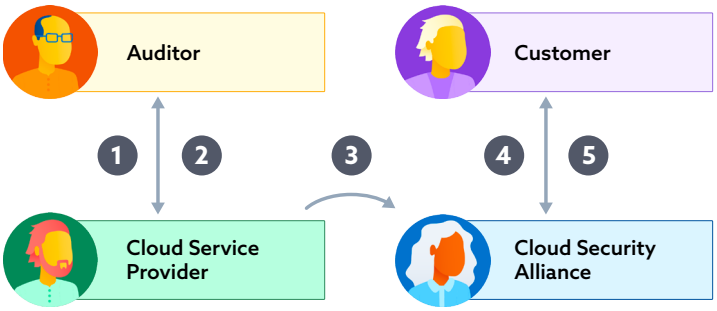

Figure 1 – STAR Level 3 Certification Process

(1) Cloud Service Provider (CSP) delivers the controls scope and measurement scheme to the auditor

(2) Auditor issues report validating scope of the STAR Level 3 (L3) controls and measurement scheme, begins monitoring control results, solicits root cause on exceptions

(3) CSP registers L3 audit report with CSA and begins transmitting control results and exception reports

(4) CSA reviews documentation and posts approved candidates to STAR Registry, begins storing control results

(5) Prospective and existing customers check STAR Registry

Roles and Responsibilities

The CSP is the sponsor of the continuous auditing process. The CSP must be able to map its internal controls into the CCM and continuously provide control performance measurement data to be leveraged in the audit, and is responsible for addressing the results of the auditing process.

Independent auditing firms and auditors serve as the trusted third party, recognized and qualified by CSA, and are either an ISO-accredited certification body or a certified public accountant (e.g., AICPA member). Auditors perform the certification of attestation audit and provide findings to the CSP. Auditors also validate the controls scope, metrics used, and method of data measurement and validate data integrity.

CSA, with input from its members, establishes the STAR program guidelines and rules for auditors. CSA provides guidelines on the establishment of a suitable scope for the Level 3 program and defines reporting policies, maintains the STAR registry, and certifies CSPs into the program.

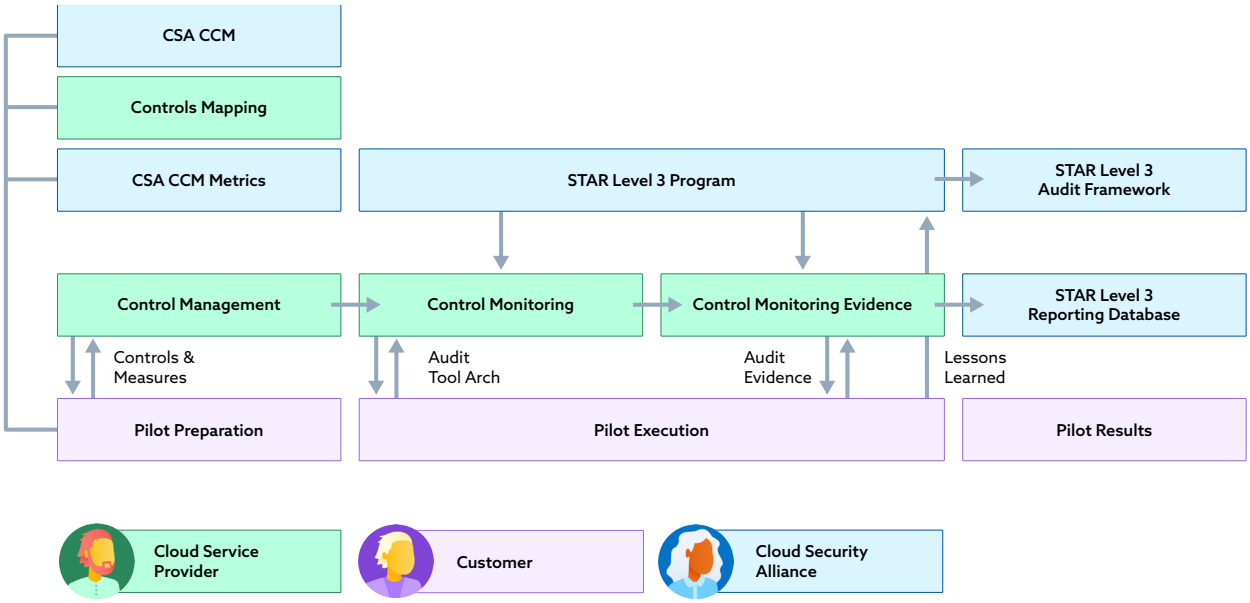

Figure 2 – STAR Level 3 Data Flow and Roles and Responsibilities

Continuous Auditing Foundations

Continuous auditing differs in control validation frequency compared to traditional "point-in-time" certifications and "over a period of time" attestations, which are a linear process producing one output result at the end; continuous auditing measures a control with a higher frequency. Intervals between checks are regulated by a policy that takes into consideration the technical nature of the control and the risk level. Suitable architecture must be designed to facilitate and record automated and non-automated assessments.

Continuous audits are separated into a "preparation phase" and the four "execution phases" (see Figure 3). The preparation phase produces specifications, which are the input for the continually executed subsequent phases.

Continuous auditing requires an architecture that allows for constant data gathering and processing. Defined objectives, attributes, metrics, frequencies, and scope are utilized in the execution phases to analyze the control measurement data and the manual assessments to assess the state of compliance.

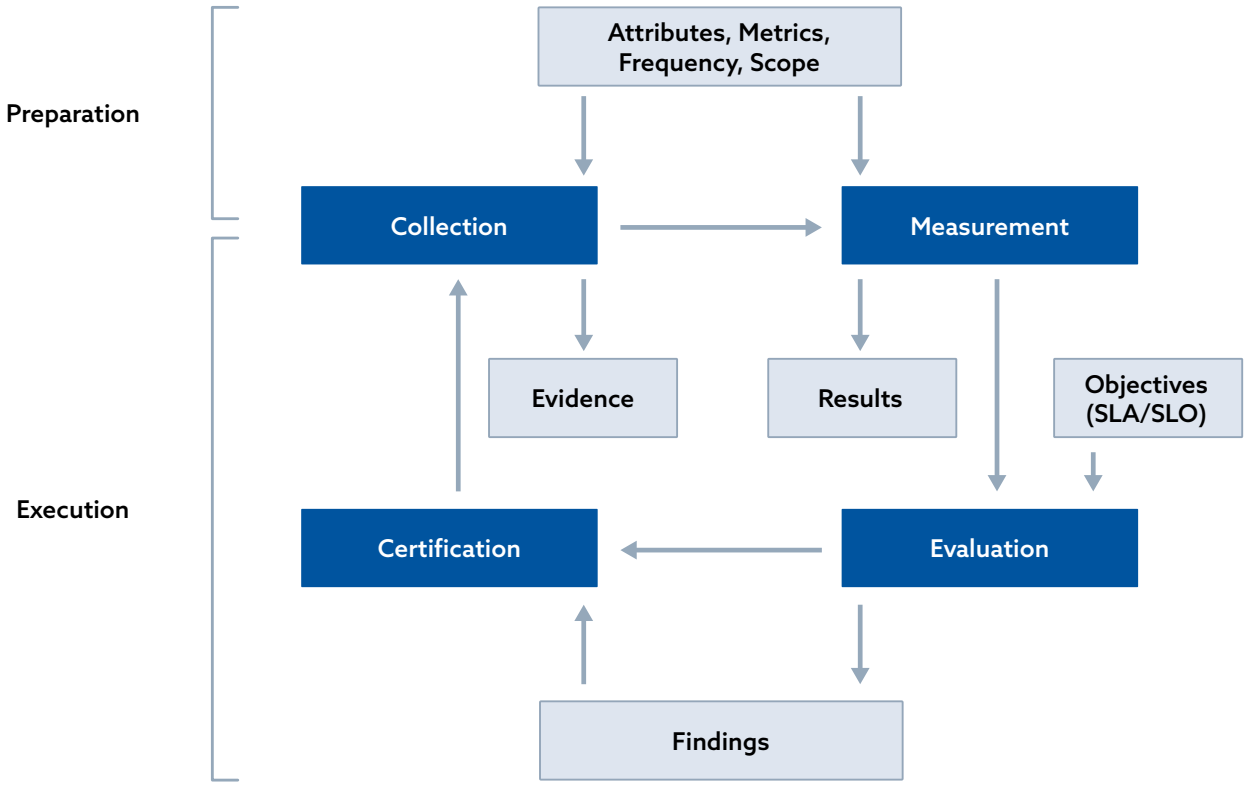

Figure 3 – Continuous Audit Model

Preparing for the Continuous Audit

In the preparation phase, selected control attributes are operationalized and success criteria are selected. This process includes:

- Definition of the scope of the measurement and the service-level objectives (SLO) or Service Quantitative Objectives (SQO) associated with each control;
- Determination of the frequencies at which each objective should be checked; and,
- Definition of attributes and metrics, as well as identification of points where the measurements should be taken.

Control measurements should:

- Be obtained on the infrastructure or service by performing measurements and storing in the evidence store;
- Be performed according to the metric; and,
- Express a qualitative or quantitative assessment of an attribute.

To ensure transparency, this process has to be documented in a way that can be audited.

Executing the Continuous Audit

Collection

The collection phase is the first step of the "execution phase" of an ongoing continuous auditing process. Data is collected for the automated assessment as well as for the non-automated assessment. Data collection is driven by the metric that has been chosen to validate an attribute. Data serves as evidence that the control is operating effectively (or as intended).

Automated assessments can be driven through log analytics, network statistics and monitoring, process statistics, or resource utilization.

Non-automated assessment requires humans to verify the existence and the effectiveness of certain processes and to read documents or examine records.

The frequency at which evidence is collected is influenced by the objective. Evidence must be stored and retained for audit purposes before it is processed.

Measurement

This phase seeks to execute operations designed to qualify or quantify a control attribute. The result can be considered as evidence like the raw data itself and should be treated and stored as the original evidence.

Measurement generally requires data processing to transform the collected raw data into an usable result that can be compared to a known good or objective.

Continuously auditing a measurement result quantifies or qualifies an attribute. Interpretation of raw data collected for an attribute is usually defined in the preparation phase, where a measurable value and control objective is identified for each attribute.

For key measurement procedures and guidance, see the EU SEC's Continuous Auditing Certification Scheme.

Evaluation

The evaluation phase seeks to validate whether data collected on the control meets the certification goal set by the CSP. Control measurements are validated against SLOs and SQOs.

Control validation can be performed by:

- Evaluating the attributes:
- Performing a measurement, and/or
- Requesting the latest value from the evidence store.

- Assessing the control status by evaluating all corresponding attributes.
- Evaluating the control status based on the evidence provided for each objective.

Certification

The source of control measurement data must be disclosed to stakeholders. CSPs must disclose:

- How the evidence data was collected, namely by human or automated assessment.
- The frequency at which the result of the assessment gets updated.

The assurance on truthful data involves two traits:

- An ethical statement from the CSP on the truthfulness.
- The implementation of technical safeguards into the data aggregation chain, which must be traceable by the stakeholder.

As part of the certification process, continuous auditing data must be shared with CSA and customers for the process to be trusted. Ultimately, the certification phase involves informing stakeholders about the compliance status of an information system with a set of predefined objectives.

The CSA Open Certification Framework provides three models for continuous auditing. Each of the three models provides a different level of assurance by covering requirements of continuous auditing with various levels of scrutiny.

The three models defined here are represented in Figure 4:

1. Continuous Certification Extended Certification with Continuous Self-Assessment
2. Continuous Self-Assessment

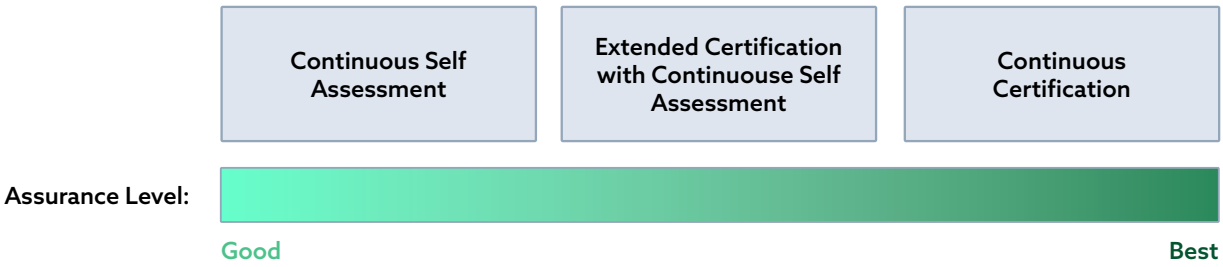

Figure 4 – Continuous Audit Certification Models

Essentially, the proposed framework starts from a simple certification of the timely submission of self-assessment compliance reports and moves up to a continuous certification of control objectives fulfillment. It should be noted that in two of the proposed levels, we rely on traditional "point-in-time" certification as a foundation to create a continuously certified information system by extension.

Conclusion

The CSA Continuous Auditing Certification (aka STAR Level 3) is the most rigorous assurance tier in the STAR program. Level 3-certified services providers can demonstrate that critical security controls are monitored and validated continuously, providing customers with the ultimate level of transparency and assurance. Continuous security controls auditing and certification delivers the best-in-class security transparency and assurance that customers need in an ever-changing threat landscape.

References

European Security Certification Framework (EU-SEC). (2017). Continuous Auditing Certification Scheme. Accessed at https://cdn0.scrvt.com/fokus/44a1bee2dbf28587/cb819c91d951/Whitepaper_CA_FOKUS.pdf

Cloud Security Alliance. (2017). Guidelines for CPAs Providing CSA STAR Attestation v2. Accessed at https://cloudsecurityalliance.org/artifacts/guidelines-for-cpas-providing-csa-star-attestation-v2/

Cloud Security Alliance. (2020). Requirements for Bodies Providing STAR Certification. Accessed at https://cloudsecurityalliance.org/artifacts/requirements-for-bodies-providing-star-certification/.

Cloud Security Alliance. (2020). STAR Certification Guidance Document: Auditing the Cloud Controls Matric (CCM). Accessed at https://cloudsecurityalliance.org/artifacts/star-certification-guidance-document-auditing-the-cloud-controls-matrix-ccm/.

Cloud Security Alliance. (2021). Cloud Controls Matrix and CAIQ v4. Accessed at https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.