Acknowledgments

Lead Authors

Doug Egan
Stephen Germain

CSA Global Staff

John DiMaria
Stephen Lumpe
Table of Contents

Acknowledgments .............................................................................................................................. 2
Table of Contents ................................................................................................................................ 3
Introduction ........................................................................................................................................ 4
   Abstract ........................................................................................................................................... 4
   Problem Statement ....................................................................................................................... 4
Value Proposition ............................................................................................................................. 6
Conclusion .......................................................................................................................................... 8
Introduction

Abstract

As organizations look to cloud services to process more sensitive and critical data, security and risk management teams require tools to quickly assess and understand the types and rigor of security controls applied by cloud service providers. CSA STAR Attestation is the first cloud-specific attestation program designed to meet this need. CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix.

Problem Statement

Requirements for the cloud can be quite different than non-cloud environments, so a generic approach to security compliance is not a viable solution for providing evidence of assurance in the cloud.

Unique considerations must be given to:

- Understanding the scope of the cloud computing environment.
- Do the current security controls cover the unique aspects of the cloud environment?
- Can the current risk assessment capture the risks correctly?
- Audit trails that prove the effectiveness

Background

As organizations look to cloud services to process more sensitive and critical data, security and risk management teams require tools to quickly assess and understand the types and rigor of security controls applied by cloud service providers. CSA STAR Attestation is the first cloud-specific attestation program designed to meet this need. Based on the CSAs Cloud Controls Matrix (CCM), STAR is the only meta-framework of cloud-specific security controls, mapped to leading standards, that enables third party audit review to give security teams the support and trust they require to enable this move to the cloud.
As a rigorous program based on the SOC2 attestations standards or international equivalents (i.e. ISAE 3000), the STAR Attestation provides for robust reporting on the cloud service provider’s description of its systems and controls, including a description of the service auditor’s tests of controls. The reports are intended to meet the needs of a broad range of users that need to understand the cloud-specific controls of a cloud service provider as it relates to security and the criteria in CCM. Similar to a traditional SOC 2 attestation there are two types of reports:

- Type 1, report on management’s description of a cloud service provider’s system and the suitability of the design of controls (“point in time” assessment); and
- Type 2, report on management’s description of a cloud service provider’s system and the suitability of the design and operating effectiveness of controls (“over a period of time” assessment)

The Type 1 audit is used as a steppingstone to the more rigorous Type 2 audit. A CSA STAR Attestation Type 1 status demonstrates to your customers the commitment to cloud security through a thorough assessment of the policies and procedures in place to protect the Confidentiality, Integrity, and Availability of their data. A STAR Attestation obtained based on a SOC 2 Type 1 report is only valid for 6 months from the as-of date, i.e., an organization that received their STAR Attestation based on a SOC 2 Type 1 report is required to submit a SOC 2 Type 2 report to maintain uninterrupted STAR Attestation status. The validity period of a STAR Attestation is extended by grace period of 3 months on top of the basic validity period for report generation and delivery (“maximum validity period”).
Value Proposition

CSA STAR is being recognized as the international harmonized solution leading the way of trust for cloud providers, users and their stakeholders by providing an integrated cost-effective solution that decreases complexity and increases assurance and transparency while enabling organizations to secure their information, protect themselves from cyber-threats, reduce risk and strengthening their information governance and privacy platform.

Organizations that invest in STAR Attestation provide easier justification for users during the provider selection process. Providers with STAR Attestation emerge as industry leaders during the RFP process, as it provides an increased level of trust that is so critical in today’s culture. STAR Attestation will facilitate reducing complexity and costs in the following ways:

• Eliminate or reduce audits
  • STAR Attestation is based on SOC2 plus the CCM. The CCM is the only meta-framework of cloud-specific security controls, mapped to over 40 leading standards, best practices and regulations. CCM is currently considered a de-facto standard for cloud security assurance and compliance, to a great extent, reducing the need for clients and prospects to audit or require lengthy questionnaires.
  • If a CSP uses a third party’s infrastructure (AWS/Azure/IBM/GCP/data center) to offer cloud services, and these third parties have obtained STAR attestation, it will provide sufficient assurance to stakeholders as well as making a case to eliminate or greatly reduce the need to audit or send out security questionnaires.

• Reduce time evaluating supply-chain
  • STAR Attestation provides a continuous, consistent method for monitoring and evaluating cloud providers
  • Provides complete visibility and transparency through the STAR Registry that can be used to benchmark the total supply chain by obtaining an objective picture of what’s really happening through clean, standardized data.

• Increase awards of RFP’s
  • Since STAR Attestation is based on SOC2 + the CCM, and CCM has an extended set of questions called the CAIQ. Organizations often use the CAIQ to get additional protection by building a request for proposal (RFP) with the information from CAIQ. Organizations can then verify the validity of a vendor’s answers during the RFP interview. This along with the STAR attestation report is a powerful tool in the RFP process.
  • The CCM control specifications constitute suitable criteria as defined by the Attestation Standard (“CCM criteria”) and include criteria equivalent to the criteria for the security principle in the TSC plus certain additional criteria related to security.
• In a SOC 2® report, the CPA expresses an opinion on whether the controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria.

• STAR will facilitate reducing complexity in terms of time, cost, trust and transparency.
Conclusion

CSA STAR Attestation brings big benefits to all companies of all sizes. Confidence, reputation, and new business can come with CSA STAR Attestation as more customers ask for proof of these measures. Plus, it can help you as a cloud service provider to:

- Provide top management with visibility, so that they can evaluate the effectiveness of their security system in relation to expectations of the cloud security industry and SOC2.
- Implement an audit that is designed to reflect how your organization’s objectives are aimed at optimizing the cloud services.
- Demonstrate progress and performance levels via an independently validated award from an external AICPA Firm.
- Benchmark your performance against your peers.

Additionally, for customers of cloud service providers, CSA STAR Attestation will provide a greater understanding of the level of controls that are in place.

For more information visit https://cloudsecurityalliance.org/star/levels/
Or contact us at info@cloudsecurityalliance.org