

CSA STAR CHECKLIST

WHAT IS CSA STAR?

CSA STAR stands for the Cloud Security Alliance Security, Transparency, Assurance and Risk Program.

- Founded in 2011.
- Encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM).
- Publishing to the CSA STAR Registry allows organizations to show current and potential customers their security and compliance posture, including the regulations, standards, and frameworks they adhere to.



CSA STAR LEVELS OF ASSESSMENT CHECKLIST

CSA STAR Level 1: Self-Assessment

Organizations can submit one or both the security and privacy self-assessments.

Organizations should pursue Level 1 if they are:

- ☐ Operating in a low-risk environment.
- ☐ Wanting to offer increased transparency around the security controls they have in place.
- ☐ Looking for a cost-effective way to improve trust and transparency.

CSA STAR Level 2: Third Party Audit

Allows organizations to build off other industry certifications and standards to make them specific for the cloud.

Organizations should pursue Level 2 if they are:

- ☐ Operating in a medium-to-high risk environment.
- ☐ Already holding or adhering to the following: ISO27001, SOC 2.
- ☐ Looking for a cost-effective way to increase assurance for cloud security and privacy.

STAR CERTIFICATION FRAMEWORK

The STAR Certification Framework types of audits:

		AUDIT FREQUENCY	SECURITY	PRIVACY	
TYPE OF AUDIT		STAR Level 3	Continuous Auditing		TRANSPARENCY & ASSURANCE ↑
		STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment		
		STAR Level 2	3rd Party Certification	GDPR CoC Certification	
		STAR Level 1 Continuous	Continuous Self-Assessment		
		STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment	

CSA STAR DOMAINS

Application & Interface Security	Audit and Assurance	Business Continuity Mgmt & Op Resilience	Change Control & Configuration Management	Cryptography, Encryption, and Key Management	Datacenter Security
Data Security & Privacy	Governance, Risk Management, and Compliance	Human Resources Security	Identity & Access Management	Interoperability & Portability	Infrastructure & Virtualization Security
Logging and Monitoring	Security Incident Management, E-Discovery, & Cloud Forensics	Supply Chain Management, Transparency, & Accountability	Threat & Vulnerability Management	Universal EndPoint Management	

ABOUT CONTROLCASE

ControlCase is a CMMC RPO and a global provider of certification, cyber security, and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost-effective, and comprehensive in both on-premise and cloud environments. ControlCase offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT, and FedRAMP.