AUGUST 2024

MOORE NEWSLETTER

Navigating the Cloud Security Landscape: Why CSA STAR is Essential for Trusted Cloud Transformation

Cloud computing has become the backbone of modern business. The global spending on cloud infrastructure is set to surpass $1 trillion by 2024, as projected by the International Data Corporation. This surge is fuelled by the increasing adoption of AI models, Hybrid and Multi-Cloud, and Edge Computing, which are revolutionising industries and driving innovation worldwide. However, alongside the tremendous opportunities, global businesses are confronted by pressing challenges in the realm of cloud security, encompassing data security, data privacy, and the effective management of multi-cloud environments.

Why is the CSA STAR programme vital to cloud computing security?

The Cloud Security Alliance (CSA) is an internationally renowned organisation dedicated to promoting best practices, awareness, practical implementation, and certification for the future of cloud and cybersecurity. CSA brings together industry experts, organisations, and stakeholders with the common goal of addressing the security challenges associated with cloud computing. By fostering collaboration and advocating for standards and best practices, CSA plays a crucial role in promoting the development of a secure and trustworthy cloud environment.

CSA Security Trust Assurance and Risk (STAR) is a widely recognised cloud security provider (CSP) certification programme operated by CSA. The CSA STAR programme provides a comprehensive framework for CSPs to assess and validate their security posture. It enables providers to demonstrate compliance with industry-recognised standards and best practices. Furthermore, CSA oversees the CSA Global Consulting Programme, which facilitates connections between cloud users and a network of reliable security professionals and organisations that provide professional services aligned with CSA's best practices. Specifically, the CSA STAR programme is centered around the Cloud Controls Matrix (CCM).

Understanding CSA cloud security assessments and certifications

- **CSA STAR attestation:**

  A third-party independent assessment that combines the SOC 2 framework and the Cloud Control Matrix (CCM).

- **CSA C-STAR assessment:**

  A part of the OCF Level 2 Scheme is primarily utilised in the Greater China region. The C-STAR assessment is based on GB/T 22080-2008 and the specified set of criteria outlined in the CCM, plus related requirements of GB/T 22239-2008 and GB/Z 28828-2012.

- **CSA General Data Protection Regulation (GDPR) COC third-party audit-based certification:**

  A third-party certification assuring compliance of a CSP’s services to GDPR.

CSA STAR programme

To address critical cloud security concerns, organisations can leverage the CSA STAR programme to demonstrate their commitment to robust security practices. The programme offers two levels of certification:

- **CSA STAR Level 1 Self-assessment:**

  CSP undergo a self-assessment process using the Consensus Assessments Initiative Questionnaire (CAIQ) to document compliance with the Cloud Controls Matrix (CCM). CAIQ is a comprehensive set of questions and requirements that encompass a wide array of domains pertaining to security practices. It allows providers to divulge and communicate information about their security measures to their customers. STAR self-assessments undergo annual updates. This level is ideal for organisations operating in low-risk environments and seeking an affordable means to enhance trust and transparency.

- **CSA STAR Level 2 Third-party audit:**

  CSP undergoes a certification process by independent third-party assessors, allowing organisations to customise existing industry certifications and standards for the specific needs of the cloud. By selecting suitable security and privacy audits and certifications, organisations can demonstrate compliance with relevant regulations and standards, considering their location and specific cloud computing requirements. This level is well suited for organisations operating in medium to high-risk environments and already complying with established standards such as ISO27001, SOC 2 and GDPR.

Specifically, the CCM provides a set of security controls mapped to leading industry standards such as ISO27001, CCM V3.0.1 and CIS Controls V8. CCM covers 197 control objectives organised into 17 domains as shown below.

1. Audit and assurance
2. Application and interface security
3. Business continuity management and operational resilience
4. Change control and configuration management
5. Cryptography, encryption and key management
6. Data centre security
7. Data security and privacy lifecycle management
8. Governance, risk and compliance
9. Human resources
10. Identity and access management
11. Interoperability and portability
12. Infrastructure and virtualisation security
13. Logging and monitoring
14. Security incident management, e-discovery and cloud forensics
15. Supply chain management, transparency and accountability
16. Threat and vulnerability management
17. Universal endpoint management

Key benefits of CSA STAR programme

- **Adapting to new threats:** The STAR programme enables CISOs to remain at the forefront of managing evolving cyber vulnerabilities by compelling CSPs to consistently maintain security measures capable of tackling new and emerging risks.
- **Fostering innovation:** The CSA STAR programme encourages a culture of continuous security improvement among CSPs. This drives CSPs to develop innovative security solutions and approaches, enabling enterprises to stay ahead in managing cloud security risks.
- **Strengthen confidence and reliability:** The CSA STAR programme enables CSPs to showcase their commitment to security best practices. CISOs can leverage a CSP's public STAR record to gain visibility into how the provider addresses threats and vulnerabilities, as well as which security controls are shared responsibilities between the CSP and the customer.
- **Risk assessment and management:** CISOs and their teams can leverage a CSP's self-assessment, certification, and continuous monitoring data to identify potential risks and make informed decisions. STAR illuminates the disparities between the controls managed by the CSP and those implemented by the enterprise. This empowers the CISO team to pinpoint and introduce compensating controls to address outstanding risks.

CSA STAR certification

The CSA STAR certification is a third-party independent assessment of a CSP's security using the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA CCM.

During the certificate assessment process, each CCM security domain will be evaluated and scored according to maturity level, which is scored from 1 to 15 as follows:

Score	Descriptor
1-3	No formal approach
4-6	Reactive approach
7-9	Proactive approach
10-12	Improvement-based approach
13-15	Optimising approach

To calculate the overall maturity score for a CSP, the domain scores are averaged together. This average considers the lowest scores achieved within each domain. The overall maturity score will determine whether the CSP receive no award, a bronze award, a silver award, or a gold award in their CSA STAR report.

In terms of prerequisites for obtaining these certifications, there are no prerequisites for STAR Level 1 while organisations seeking STAR Level 2 need to hold STAR Level 1. Generally, CSA STAR is designed to cater to a wide range of CSPs, encompassing Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service providers, as well as managed security service providers and other cloud-related services.

Benefits of obtaining CSA STAR certification

- **Independent validation:** The programme offers unbiased third-party verification of a CSP's cloud security practice. Validation by a trusted authority enhances customer trust and confidence in CSP's ability to protect their data and systems.
- **Strengthened security posture:** By conforming to the stringent controls and recommended methodologies established in the CSA STAR programme, CSPs can bolster their comprehensive security stance. This entails deploying resilient security measures, pinpointing vulnerabilities, and mitigating potential risks.
- **Competitive advantage:** Possessing a CSA STAR certification showcase CSP their dedication to security and adherence to compliance standards, setting them apart from providers who lack independent verification.
- **Enhanced data security:** The stringent security controls and practices mandated by CSA STAR certification lead to heightened data protection, mitigating the risks of data breaches and unauthorised access.

Conclusion

The CSA STAR programme is essential for addressing the security challenges associated with cloud computing. It provides a comprehensive framework for CSPs to evaluate and validate their security practices, showcasing adherence to industry standards. By participating in the programme, CSPs can strengthen their security measures, obtain independent validation, and distinguish themselves in the highly competitive cloud services market. As the adoption of cloud technology continues to expand, the CSA STAR programme plays a pivotal role in assisting organisations in navigating the intricacies of cloud security, mitigating risks, and fostering customer trust in an interconnected environment. Organisations are strongly encouraged to embrace the CSA STAR certification to ensure robust protection over their data and systems.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

To find out more, please contact our experts below:

PATRICK ROZARIO
Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal
T +852 2738 4631
E kevinlau@moore.hk

www.moore.hk