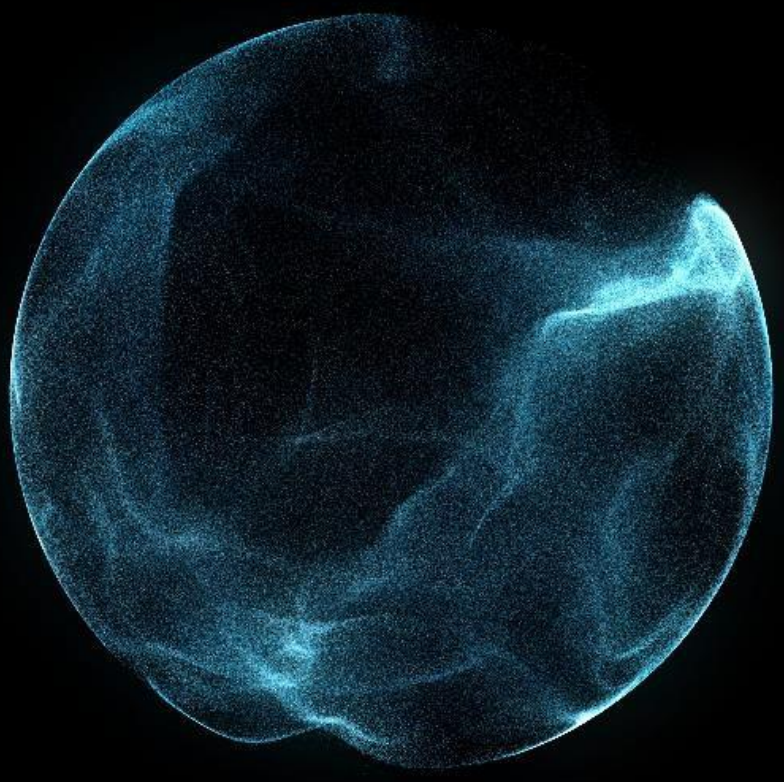
Deloitte.



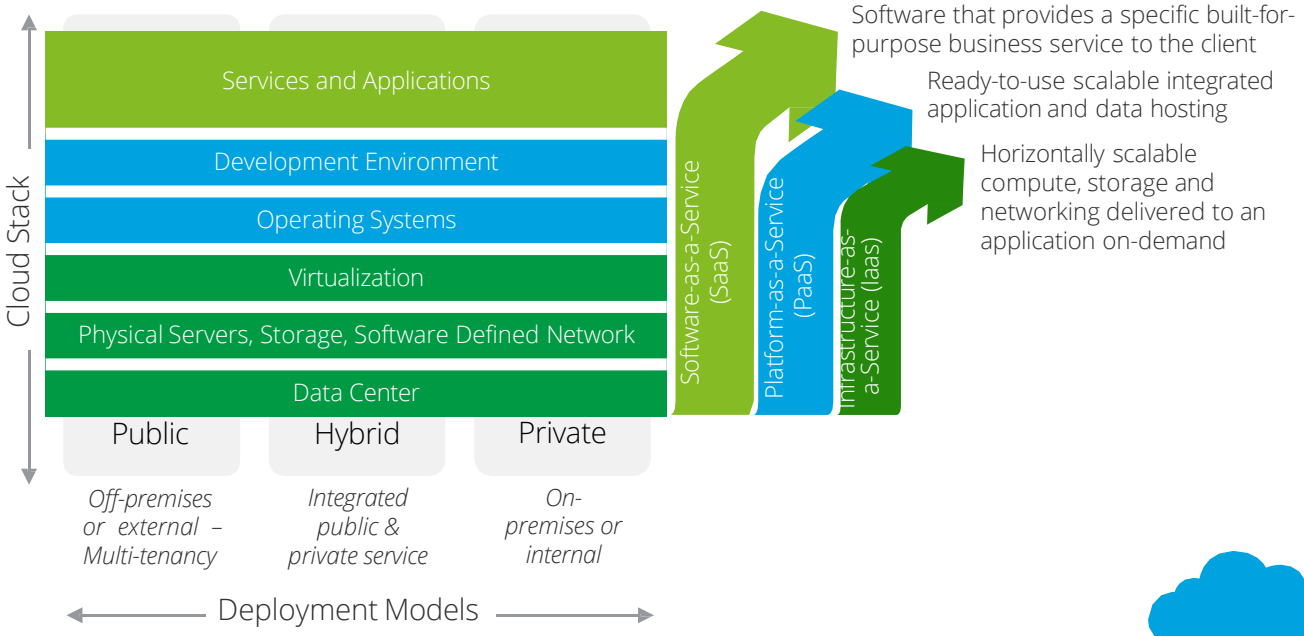
Trusted Cloud Providers

SOC 2 Reports and Cloud Security Alliance (CSA) Security, Trust, Assurance & Risk Registry (STAR) Level 2

Cloud computing highlights

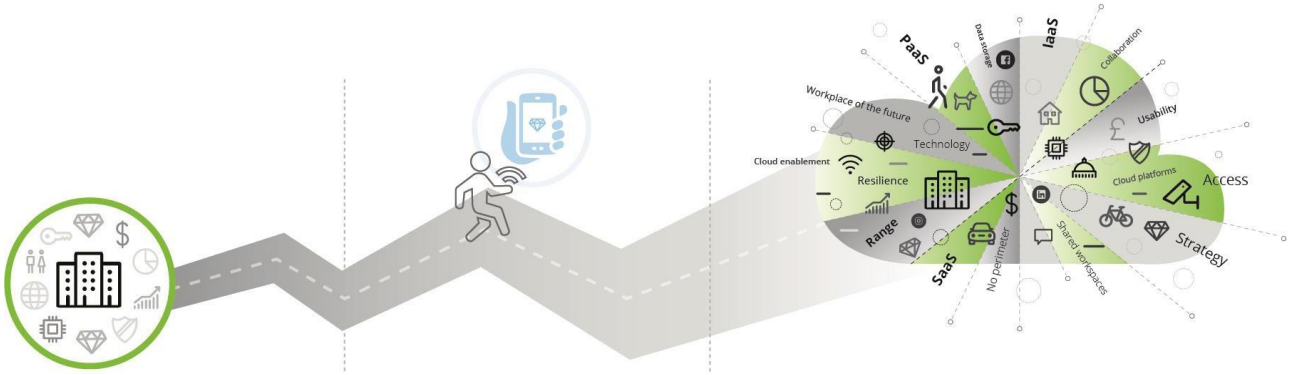
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

- The NIST (National Institute of Standards and Technology) 800-145 Definition of Cloud Computing, Peter Mell and Timothy Grance, September 2011



The journey to the cloud – from perimeter, to mobile and more

For many businesses, cloud computing represents the new normal. As companies expand their presence in the cloud, additional risk considerations beyond protecting the perimeter continue to emerge.



If the perimeter was intact, the crown jewels remained safe	Users and crown jewels… became mobile	Organizations are leveraging cloud technologies for additional capabilities
• Perimeter-based security • Crown jewels were protected by the organization's strong perimeter	• Increasingly porous perimeters • Security embraced remote and mobile users • Focus shifted to compliance • Private networks still dominated	• More complex threat landscape • User-based security • Security by design • Security as a business enabler • Increased support for bring your own device (BYOD)

Cloud service models—Controls at different layers

The primary responsibility for controls may reside with the cloud customer ("user entity") or cloud service provider. Below is a typical chart of responsibilities by technology stack, which may vary.

Technology Stack	On-premise	IaaS	PaaS	SaaS
Application	User entity	User entity	User entity	User entity
Middleware/Software stack	User entity	User entity	User entity + Cloud provider	Cloud provider
Servers and operating systems	User entity	User entity + Cloud provider	Cloud provider	Cloud provider
Management console*	User entity	User entity + Cloud provider	Cloud provider	Cloud provider
Hypervisor/Data storage/File storage	User entity	Cloud provider	Cloud provider	Cloud provider
Physical	User entity	Cloud provider	Cloud provider	Cloud provider

* Refers to the hypervisor management console managing the underlying virtualized infrastructure for on-premise. IaaS scenarios would also include a management console for the cloud customers while the underlying hypervisor console is managed by the cloud service provider (CSP).

SOC 2 reports

Cloud service providers typically make a System and Organization (SOC) 2 report available to their customers to build trust and provide assurance over the controls that intersect with the related trust services categories. They are often a cornerstone of conducting business and can provide a competitive advantage.

SOC 2

- Examination of controls related to specific trust categories (security, availability, processing integrity, confidentiality, or privacy), service commitments, system requirements, and potentially compliance (SOC 2+)
- Standard trust services criteria (TSC) in which controls are identified and mapped to
- Scope is IT controls for specified products or services
- Issued in accordance with the AICPA's SSAE 18 standard and AICPA 2017 Trust Services Criteria

Trust Services Categories

Category	No. of TSC
Availability, addressing continuity of operations.	3
Processing Integrity, including complete, accurate, and timely processing.	5
Confidentiality of information designated as confidential. Such information varies from organization to organization.	2
Privacy in keeping with AICPA's trust criteria and the organization's privacy policy or other regulations around the collection, use, retention, disclosure, and disposal of personal information (PI).	18
Security against unauthorized access or appropriation, either logical or physical *Note: Security is a required category mapped to common criteria; the remaining categories are optional*	33

Who is the Cloud Security Alliance (CSA)?

Over time, cloud service providers may incorporate additional cloud specific frameworks, such as CSA, in their SOC 2 reports

- The CSA is the world's leading organization dedicated to defining and raising awareness of leading practices to help ensure a secure cloud computing environment.
- CSA's objective is to:
  - Promote "best practices for providing security assurance within Cloud Computing"
  - Inform consumers and providers on security issues
  - Plays a role in addressing and implementing viable solutions for security challenges
  - Increase size and relevance as interest in implementing cloud solutions proliferate
- CSA operates the most popular cloud security provider certification program, the CSA Security, Trust, Assurance & Risk (STAR) Registry, a two-tiered provider assurance program of self-assessment and 3rd party audit
  - Being part of CSA STAR registry gives cloud service provider organizations to provide assurance on the level of maturity of their security and compliance controls and frameworks
  - For cloud service customer organizations, STAR registry provides transparency to understand how cloud security and privacy risks are handled by their providers

Source for images: Cloud Security Alliance (https://cloudsecurityalliance.org/)
Source for content: (https://cloudsecurityalliance.org/about/), (https://cloudsecurityalliance.org/star/)

Security, Trust, Assurance and Risk (STAR) Registry

The industry's most powerful program for security assurance in the cloud

The STAR Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud servicers

STAR contains the key principles of transparency, auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM)	Transparency
Publishing to the registry allows organizations to advertise their security and compliance frameworks to current and potential customers.	Global Recognition
The registry reduces complexity brought on by traditional customer paperwork and questionnaires.	Promotes Efficiency
Organizations listed in the registry as CSA Trusted Cloud providers have fulfilled various training and volunteer requirements that demonstrate a commitment to innovation and professional development to customers	Education and Training

Source for content: (https://cloudsecurityalliance.org/star/)

Levels of STAR

There are two levels of assurance for companies that submit to the STAR registry

Level 1: Self-Assessment

At this level, organizations can submit one or both security and General Data Protection Regulation (GDPR) self-assessments and use the CCM to assess and document their cloud security controls

Who should pursue this level?

- Low-risk environment organizations
- Organizations looking for an efficient and cost-effective way to improve trust and reliability
- Organizations wanting to offer increased transparency around the security controls they have in place

Level 2: Third-Party Audit

At this level, organizations can build off other industry certifications and standards to make them specific for the cloud providing greater flexibility for companies to grow and innovate.

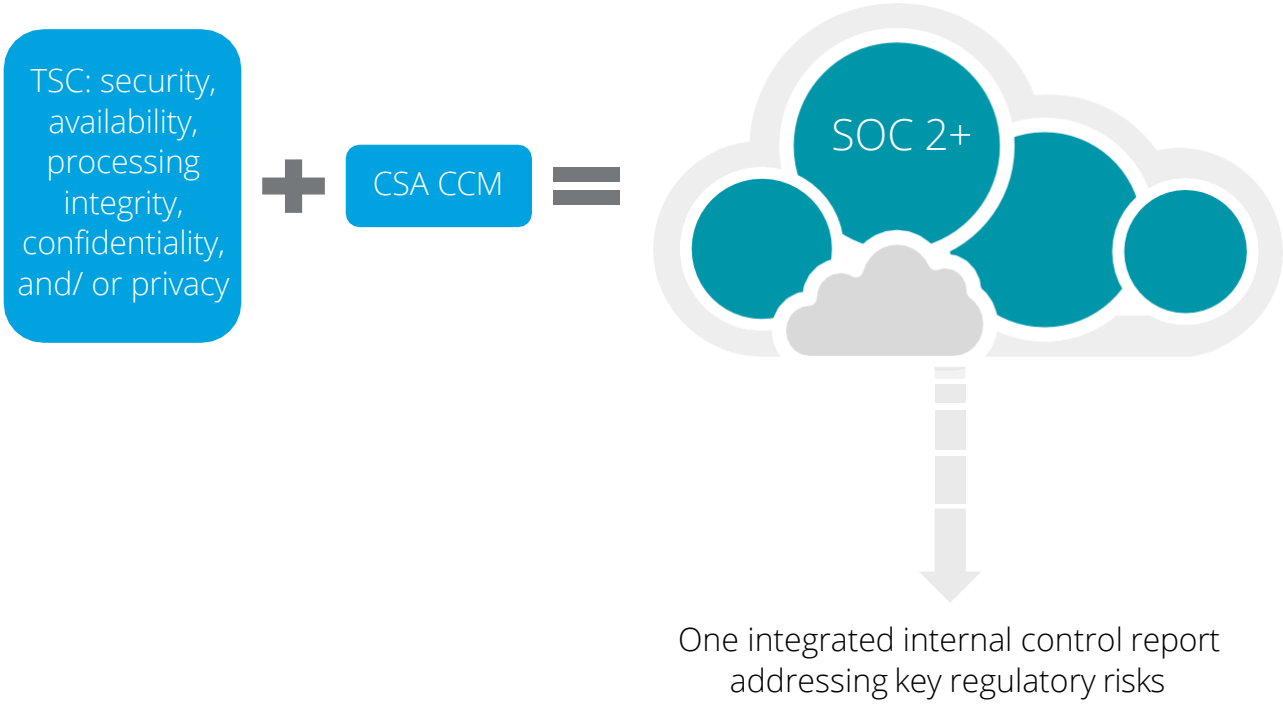
Who should pursue this level?

- Medium to high-risk environment organizations
- Organizations looking for a cost-effective way to increase assurance for cloud security and privacy
- Organizations already holding or adhering to existing industry certifications

Source for content: (https://cloudsecurityalliance.org/star/)

SOC 2 + CCM = STAR Attestation (Level 2)

The AICPA collaborated with the CSA to develop a third-party assessment program for cloud providers called the Security, Trust, Assurance and Risk (STAR) Registry Attestation. This framework combines SOC 2 attestation with the CSA's CCM.



Benefits:

- SOC2+ is a way to demonstrate the more precise cloud-specific requirements of the CCM are also fulfilled in conjunction with the Trust Services Criteria.
- For cloud service providers, security, controls, and compliance and the transparency are rapidly becoming baseline expectations of users - especially enterprise customers.
- Being on a global registry, CCM provides potential customers with transparency and creates a competitive advantage.

Cloud Controls Matrix

- The CSA CCM V4 provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the CSA guidance in 17 domains.
- The CSA CCM framework is broken down by control groups, controls specification and consensus assessment questions to assist in determining cloud related controls.
- The CSA CCM can be obtained directly from the CloudSecurityAlliance.org website.

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

The CSA CCM is specifically designed to provide security principles to help guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Your service auditor makes a difference

Why Deloitte?

SOC Leader

Deloitte is a leading provider of SOC services, issuing 800+ SOC reports in the United States annually. Representative clients range from emerging companies embarking on their first SOC report to Fortune 100 companies with many SOC reports. Deloitte is also at forefront of issuing SOC 2+ reports and has experience working with cloud frameworks including CSA CCM.

Brand Reputation

Deloitte has stood the test of time for more than 100 years. Our reputation is a testament to our commitment to quality and our core values of integrity, objectivity, and technical excellence. Deloitte provides highly effective solutions and brand recognition that promotes trust and confidence.

AICPA Collaboration

Deloitte has served as an advisor to the AICPA for the past 25+ years. Deloitte participates in AICPA working groups responsible for developing authoritative guidance for emerging areas of assurance. Deloitte recently presented at the 2022 AICPA & CIMA SOC & Third-Party Risk Management Conference.

Our Practice

We have an extensive team of professionals who specialize in internal controls, cloud, third party assurance, cyber security, and information systems. With over 3,000 Risk & Financial Advisory professionals in the US alone, we have the breadth and depth of qualified resources.

Audit Quality Leader

Deloitte is a market leader in audit quality, which is backed by a rigorous quality focus and results in leading class assurance. We have demonstrated superior inspection results, with the lowest number of deficiencies in the PCAOB's Part 1 when compared to the other firms.[1]

1. https://pcaobus.org/oversight/inspections/firm-inspection-reports

Let's Talk

Sara Lademan

Partner,
Third Party Assurance Leader
Deloitte & Touche LLP
slademan@deloitte.com

Dimitri Ramon

Specialist Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
dramon@deloitte.com

Shar Qureshi

Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
shqureshi@deloitte.com

Tushar Jain

Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
tujain@deloitte.com

Deloitte.