Evaluating Cloud Providers

Defining the Cloud

Agenda:

Cloud Computing Concepts and Architecture

Security Principles of Cloud Computing

Evaluation of Cloud Providers

Managing Cloud Relationships

Service Agreements

Service Level Agreements (SLAs)

Evaluation of Cloud Providers

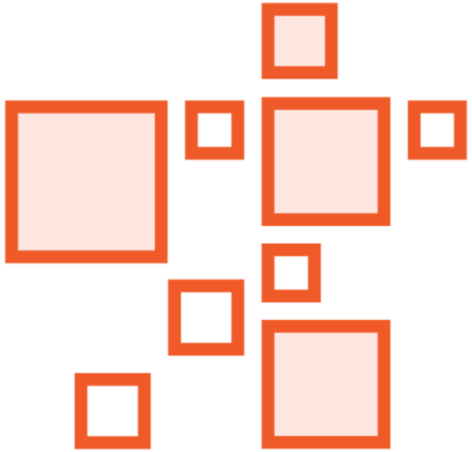
First:

- Know your business requirements
- List available choices
  - RFP

Security

Cost

Services



Considerations

Legal concerns:

Jurisdiction for contract

Location of data

Sensitivity and criticality of data

Right to Audit

May be possible in some cases

Contract

Scheduled

Skilled assessors

- Penetration testing

Cloud Evaluations

Cloud Audits

Provide independent assessment of cloud providers

- STAR
- SSAE 18
- ISAE 3402
- FISMA

CSA STAR

Security Trust Assurance and Risk

- Based on the Cloud Control Matrix and GDPR (privacy)

STAR Levels

Level One

Self-assessment

Level Two

Third-party Audit

Level Three

Continuous Auditing

Continuous Audit

Consensus Assessments Initiative Questionnaire

- Updated every 30 days for Level One

SSAE 20

Based on earlier SAS 70 and SSAE 16, 18

- Statement on Standards for Attestation Engagements (SSAE)
- American Institute of Certified Public Accountants (AICPA)
- SOC – System and Organizational Controls report

SSAE 20 SOC 1

Relevant to controls over financial reporting

SSAE 20 SOC 2

Based on WebTrust and SysTrust principles

- **Relevant to:**

Security

Privacy

Process Integrity

Confidentiality

Availability

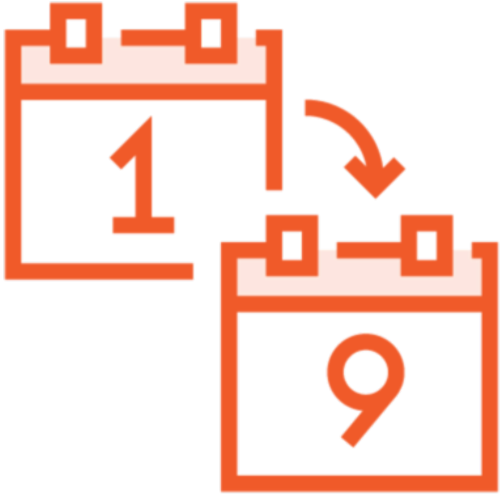
SOC 3

Summary of SOC 2 without details

- Used for marketing

Conducting an SSAE 20 Assessment

Type 1 – conducted at a point in time



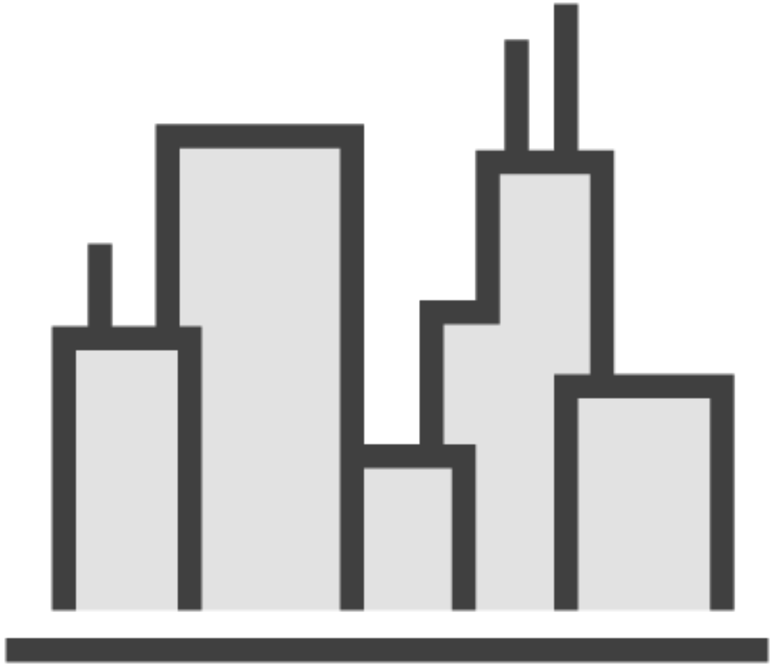
Type 2 – conducted over a period of time

(usually six months, but may be continuous)

ISO/IEC 27001:2013

- **Flagship standard of the ISO/IEC 27000 series**
  - Defines standards for an Information Security Management System (ISMS)

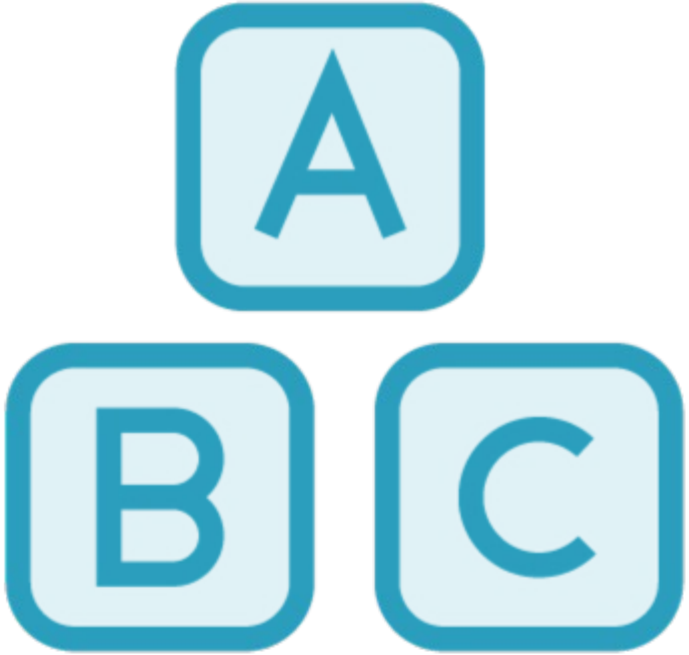
UpTime Institute



Data Center Design, Construction and on-going Operations

- Evaluation of data center infrastructure in terms of business requirements

Other Certification Standards



FISMA – Federal Information Security Management Act

PCI-DSS – Payment Card Industry – Data Security Standard

ISO/IEC 15408:2009 – Basis for evaluation of Security Properties of IT products

FIPS140-2 – Evaluation of crypto devices

Summary

This course provided an overview of Cloud-based services and highlighted some of the security concerns related to the adoption of the Cloud.

The Cloud Security Professional must ensure that security and business requirements are addressed in cloud migrations and implementations