Principles of Secure Cloud Computing

Defining the Cloud

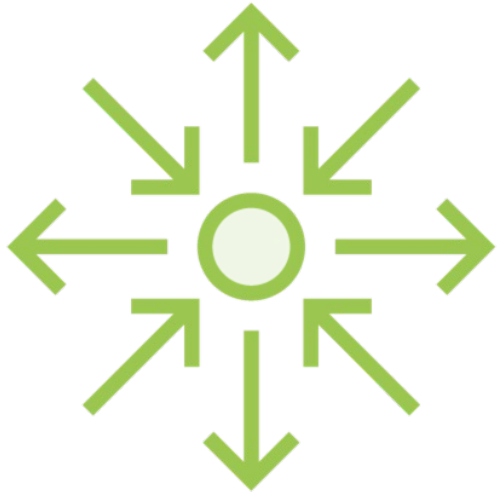
Agenda

- Cloud Concepts and Architecture
- Principles of Secure Cloud Computing
- Evaluating Cloud Providers

Information Security

Confidentiality

Integrity



Availability

Confidentiality

The protection of information from unauthorized disclosure. Protection of intellectual property, personally identifiable information (PII), and sensitive business data.

This is much more complex in the cloud because of the dependency on the cloud provider.

Integrity

Protection of information from unauthorized modification. Assurance of correct processing, storage and use of information.

The cloud introduces more layers into the systems model – creating new attack surfaces or potential points of compromise

Availability

Ensuring that systems and data are accessible when required. A measure of criticality – since the Cloud represents a dependency for the consumer, availability is a critical concern

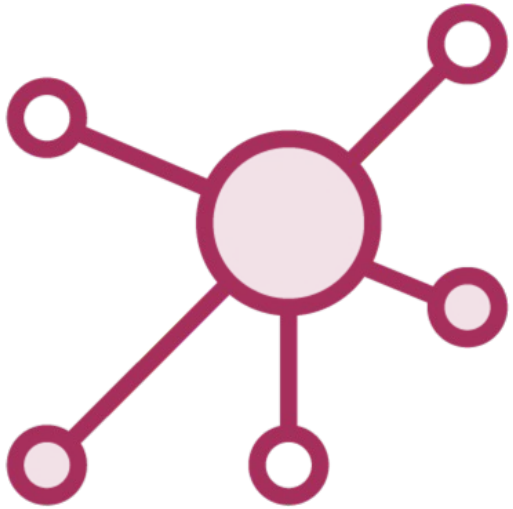
Key Points Review

For many years, CIA has been used to help define what information security is. These core concepts should be used in relation to all information and information systems.

Areas of Cloud Security

Cloud Specific Security Concerns

Multi-tenancy



Jurisdiction

Backups

Data destruction

Secure Development

Secure by design, implementation and operation

- Security throughout the SDLC
- DevOps Security

Network Security

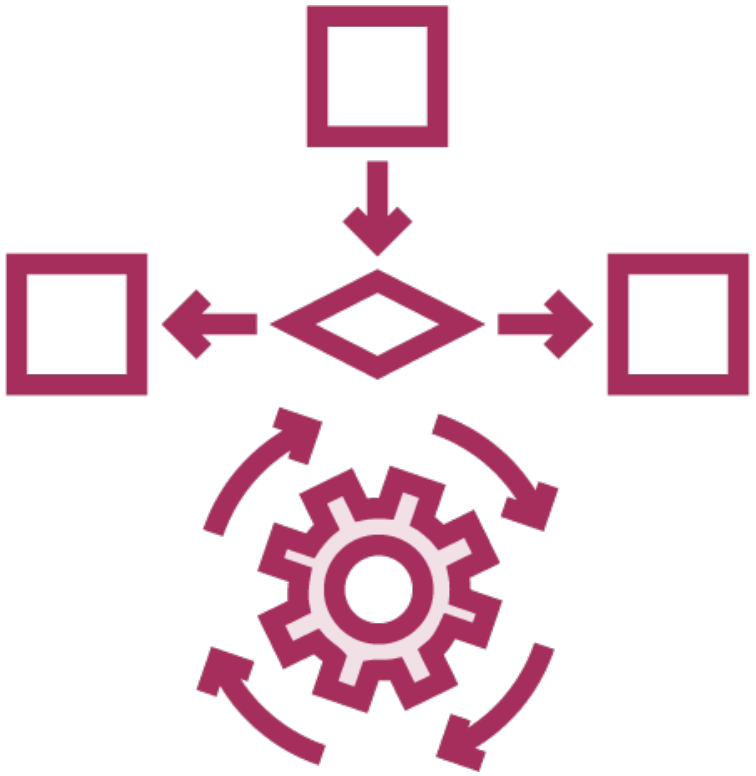
Ensure availability of network

- Redundancy

Ensure protection of confidential data in transit

Ensure protection of data from re-transmission or unauthorized alteration

Network Security



Traffic inspection

Zero-trust network

Geofencing

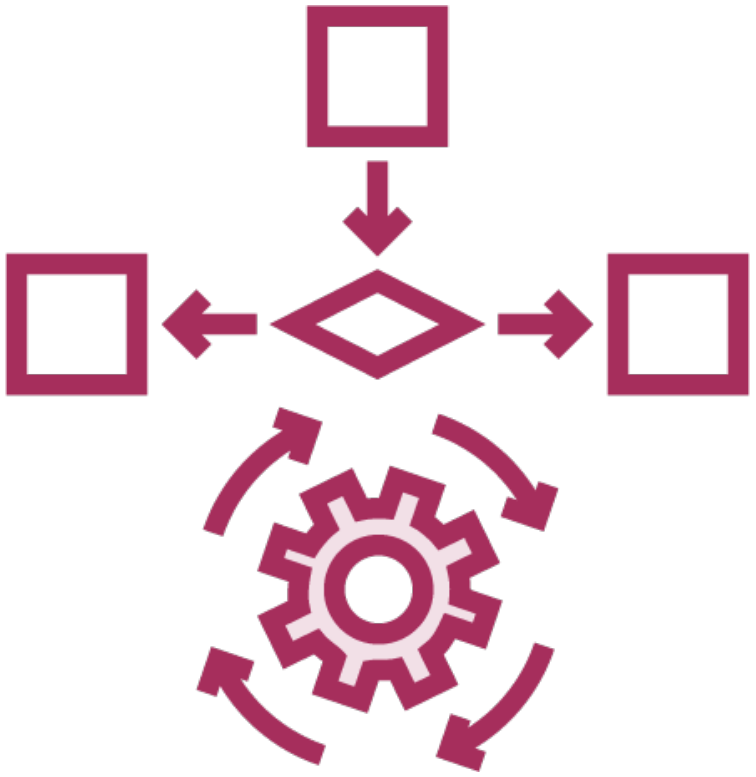
Virtualization Security

Container security

Ephemeral computing

Serverless technology

Hypervisor Security



A key component of a cloud deployment is the hypervisor – it presents a new attack surface that also must be secured

- Patching
- Configuration

Virtual Machines

Should be considered an asset and listed in the Configuration Management Database

- Correct standard configuration
- VM Sprawl
  - Wasted resources

Key Points Review

Cloud-based systems have many of the same security challenges as traditional systems, but they also introduce new challenges especially since a cloud-based system often requires coordination of different entities needing to work together.

Securing Data in the Cloud

Cloud Design Patterns

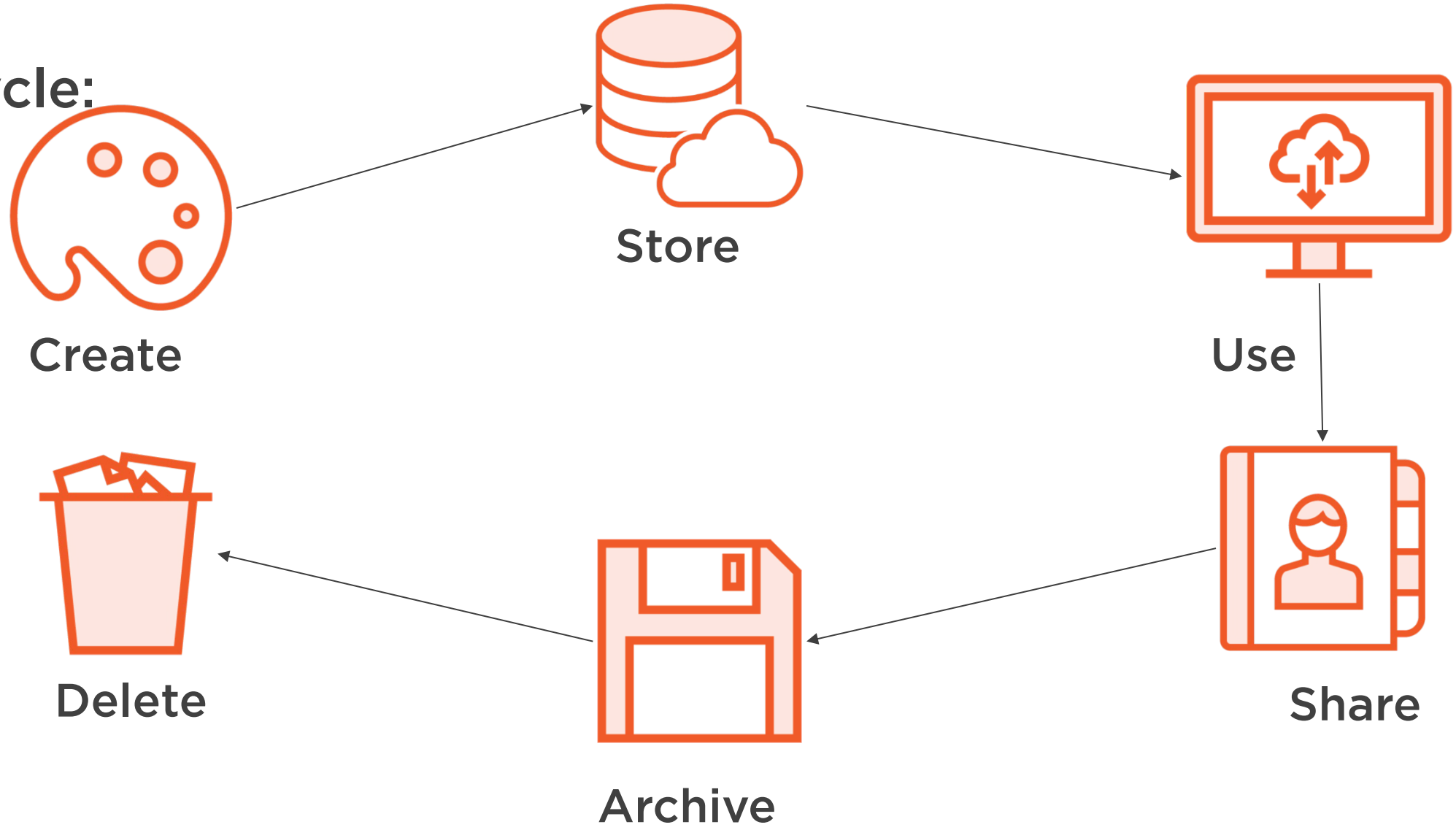
Well-Architected Framework

Cloud Security Alliance (CSA) Enterprise Architecture

SANS Security Principles

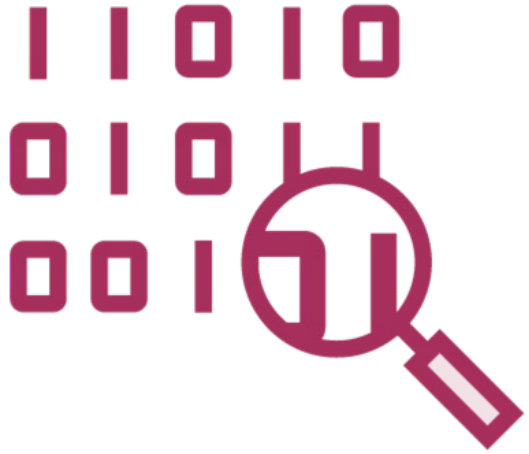
Cloud Security Concerns

Data Lifecycle:



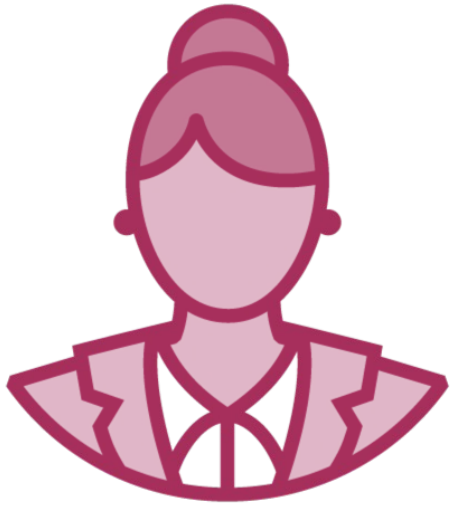
Data Protection

In order to protect data appropriately it is necessary to:



Identify data elements

- Data location



Determine data owner

Create data classification scheme

- Specify data handling requirements

Securing Data Consistently

Data should be protected all the way through the data lifecycle:

Including in all forms

- Electronic, Paper, Logs
- Stored
- Transmitted
- Displayed

Secure (defensible) destruction

Identity and Access Management

Ensure that authorized entities have the appropriate levels of access:

- Problems with access ‘creep’
- Who manages access
  - Users
  - Managers
  - Administrators

Responsibility may be shared or different with different service models

IAAA

To be examined in greater detail later in the course

Identification

Authentication

Authorization

Accounting

Access Control Concepts

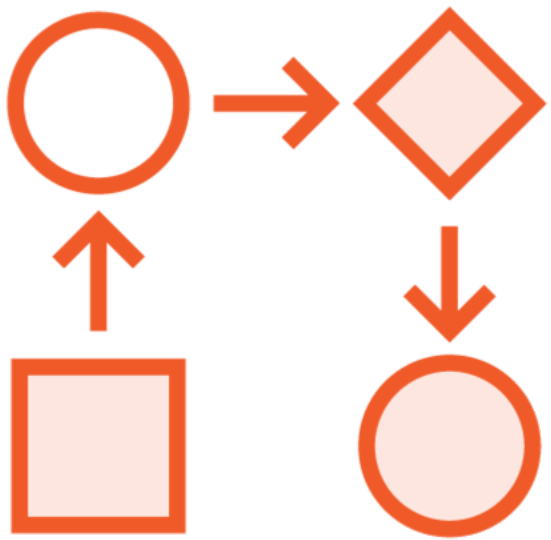
Least privilege and separation of duties

- Cloud staff

Need to know

- Stored sensitive data

Encryption



Data is encrypted to protect it from unauthorized disclosure or modification

- Requires careful key management
  - Who holds the keys
    - Escrow. HSM
    - Cryptographic erase
- Different for each Service Model

Uses of Encryption

Application

Database

Network

- Wireless

Data Destruction

Hardware disposal

- Service level agreements
- Defensible destruction

Overwriting?

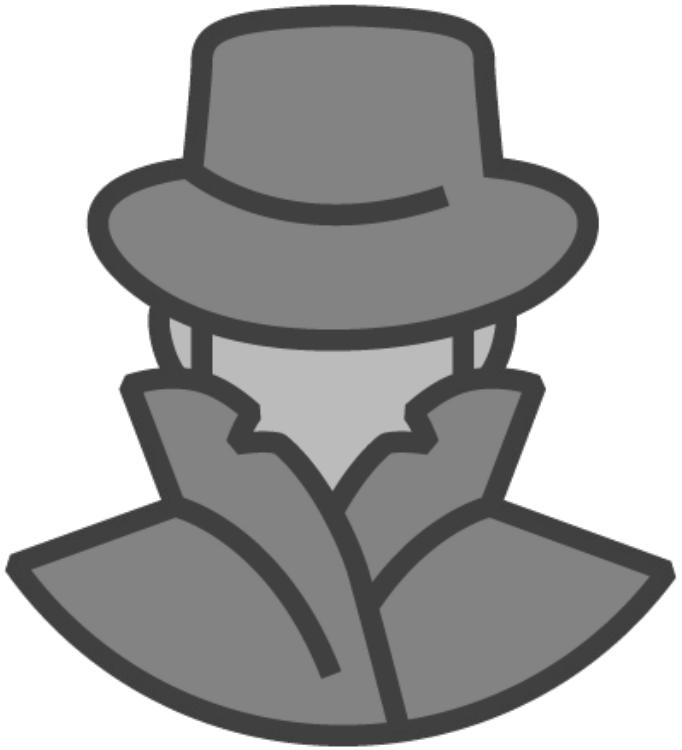
Cryptographic erase

Key Points Review

In the end, information security is just information security – but in the cloud there are some essential differences that must be acknowledged and addressed.

Principles of Secure Cloud Computing

Common Cloud Threats



Attacks or failures can happen at any layer:

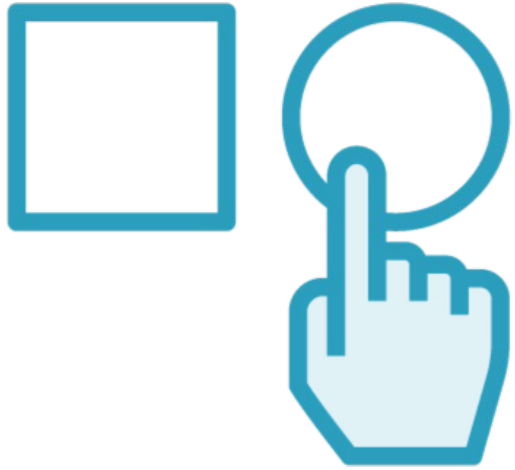
- User
- Application
- API
- Database
- Network
- Operating System
- Hypervisor
- Hardware
- Facility
- Administrators

Cost/Benefit Analysis

What is adequate security?
When is enough, enough?

Depends on:

Risk



Available options

Regulations

Business goals and mission

Security Controls in the Cloud

Contracts – service agreements

Liability

Ownership of risk

Right to audit

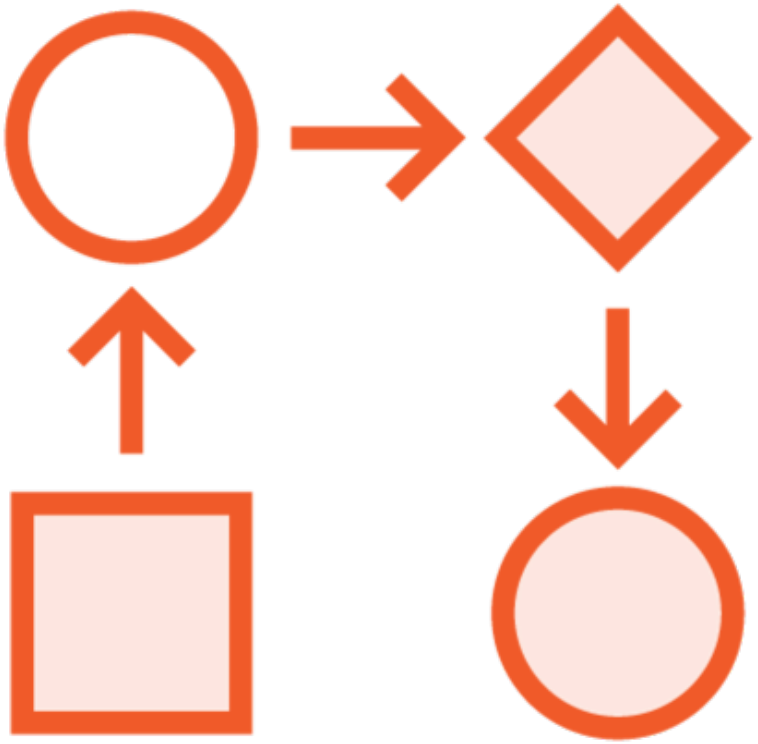
Patching and Baselining

Set security baselines that represent required settings and configuration

- Zero-trust
- Require patching of all systems including virtual machines

Business Continuity?

Business Continuity Planning



The Cloud Service Provider is often a critical dependency for the operations and mission of the Cloud Consumer

- Business Impact Analysis

Therefore, the Consumer must ensure that the CSP has a plan for business continuity in the event of a serious incident

BCP Options

The Cloud provider has:

Multiple sites

Geographically dispersed

An arrangement with another Cloud provider

BCP Options (Consumer)

Multiple Cloud Providers

- Portability
- Data transfer
- Interoperability

Key Points Review

Each organization must exercise due care and due diligence in protecting the assets of the organization

- Adequate security
  - Controls
  - Monitoring