

Cloud Data Security for CCSP®

CLOUD DATA SECURITY CONCEPTS



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance	13%



Cloud Data Security

Agenda:

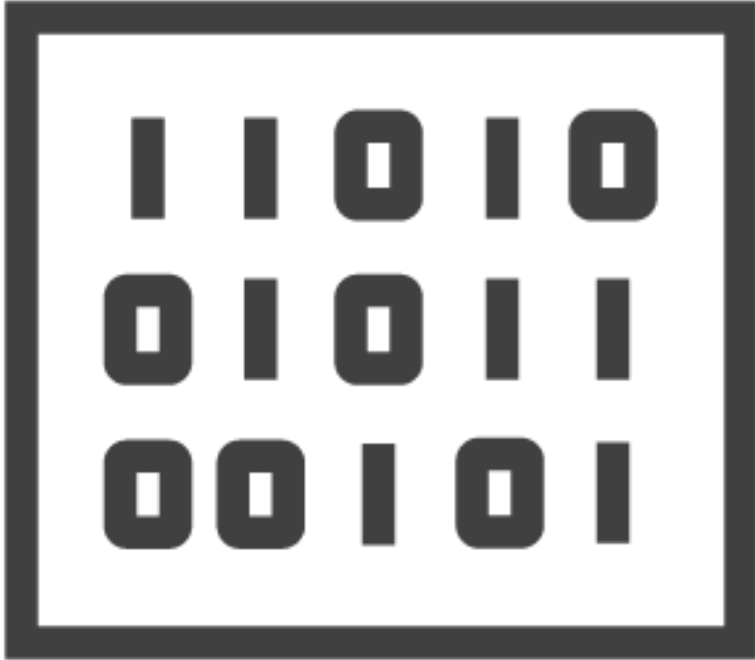
Cloud Data Security Concepts

**Cloud Data Security
Technologies**



Cloud Data Security Concepts





Data is an asset of the organization

- Essential for business operations
 - Criticality

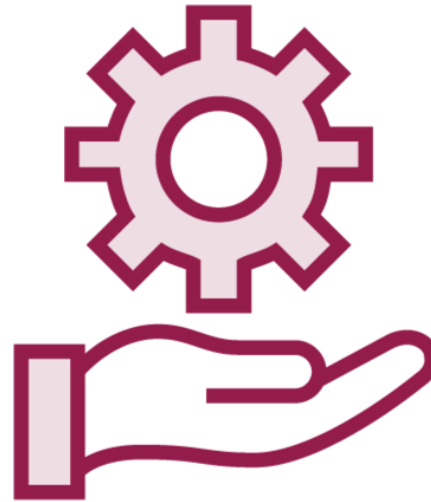


Protection of Data

1. Identification of data:



Location



Uses



Format

- Electronic, paper, verbal

2. Establish ownership



Data Ownership



Legal requirement



Senior management



May be one or more
owners



Role of the Data Owner



- Ensure data has the appropriate level of protection – consistently – throughout the organization
 - Multiple:
 - Departments
 - Systems
 - Formats
- Sometimes known in the cloud as the data controller or data processor



Liability

The data owner is liable and accountable for the protection of the data even if the data is processed by a third party – even several layers deep into the processing operation

Examples of Data Protection Laws:



GDPR

SOx

GLBA

HIPAA

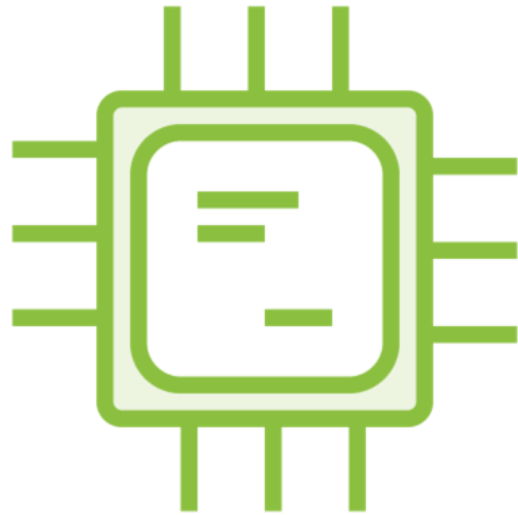
Australian, Canadian, New Zealand,
Argentinian, etc., laws



Other data roles and responsibilities



Custodian



Processor



Subject



User

Administrators



Trusted staff with elevated privileges:

- Cloud Service Provider
 - Service Operations Staff
- Internal staff
 - System administrators
 - Network administrators
 - Database administrators

Security Responsibilities

Responsibility Zones

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management	Customer	Customer	Customer	Customer	Always retained by customer
Client endpoints	Customer	Customer	Customer	Customer	
Account & access management	Customer	Customer	Customer	Customer	
Identity & directory infrastructure	CSP	CSP	Customer	Customer	Varies by Service Type
Application	CSP	CSP	Customer	Customer	
Network controls	CSP	CSP	Customer	Customer	
Operating system	CSP	CSP	Customer	Customer	
Physical hosts	CSP	CSP	CSP	Customer	Transfers to Cloud Provider
Physical network	CSP	CSP	CSP	Customer	
Physical data center	CSP	CSP	CSP	Customer	
	CSP		Customer		



Key Points Review



Data is perhaps the most important asset of many organizations:

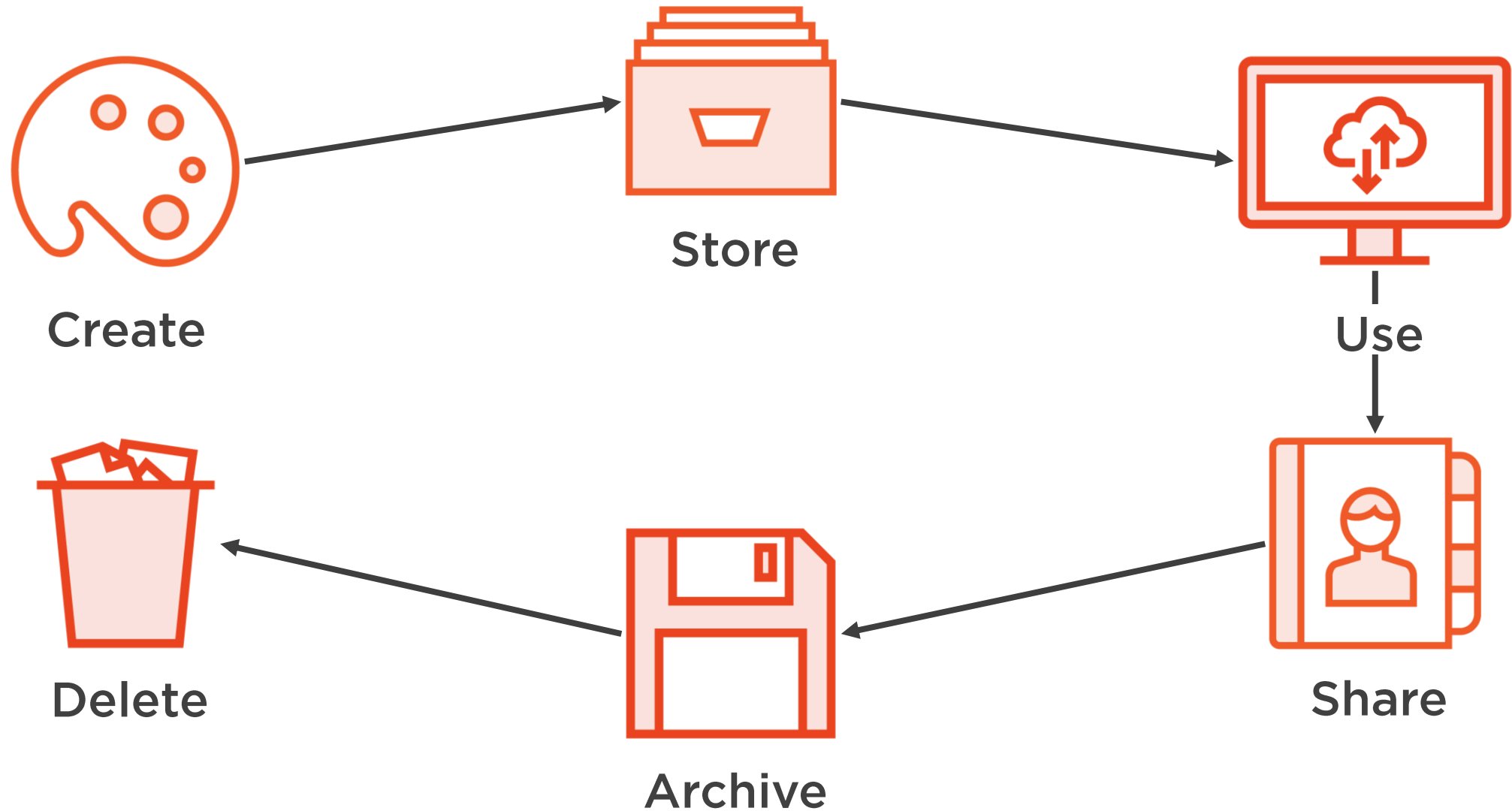
- Should you trust your most important asset to a third-party?
- What precautions should you take?



The Cloud Data Lifecycle



The Cloud Data Lifecycle:



Create



Initial receipt of data

- Secure receipt process - encryption



Establish ownership



Classification of data

- Labeling
- Encryption etc.

Store



Usually concurrent with create

- Follow data handling procedures associated with the data classification

Data Lifecycle: Use



Protect data in use:

- Training of users
- Data hiding
 - Encryption
 - Masking
 - Obfuscation
 - Anonymization
- DLP
- DRM/IRM

Share

Many Cloud deployments permit global access



Multi-factor
authentication



Least privilege



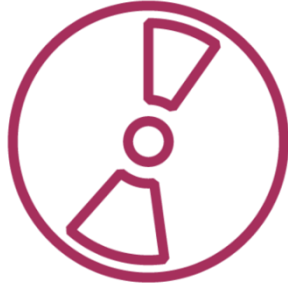
Export regulations

- Cryptography
- Jurisdiction for data storage and access



Archive

Long term storage:



Storage medium



Hardware

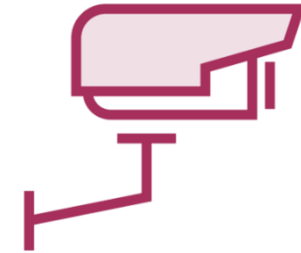


Format



Encryption

Algorithms and keys



Physical security

Natural disasters -
geographic separation

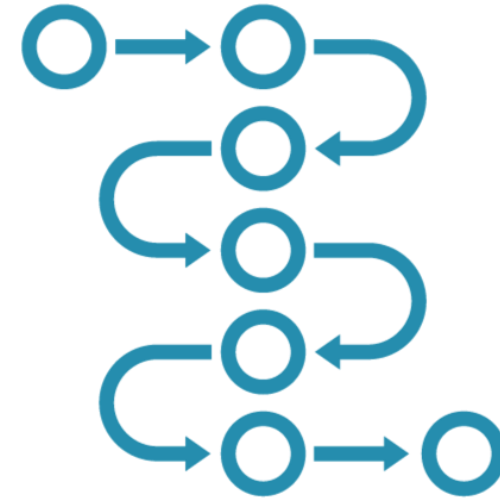


Delete / Destroy

Secure (defensible) destruction of data at end of retention period



Policy: Retention period



Policy: Process for destruction

Key Points Review



Data must be protected throughout the entire data lifecycle

- Responsibility of the data owner
- Assurance of compliance with regulations and that data will be available to support business operations



Cloud Data Classification



Data Classification

The purpose of data classification is to ensure that data is provided an appropriate level of protection.

Classification (also known as categorization) is managed by the data owner



Basis for Classification



- Business requirements
 - Projects
 - Business functions
- Laws and regulations

Data Protection

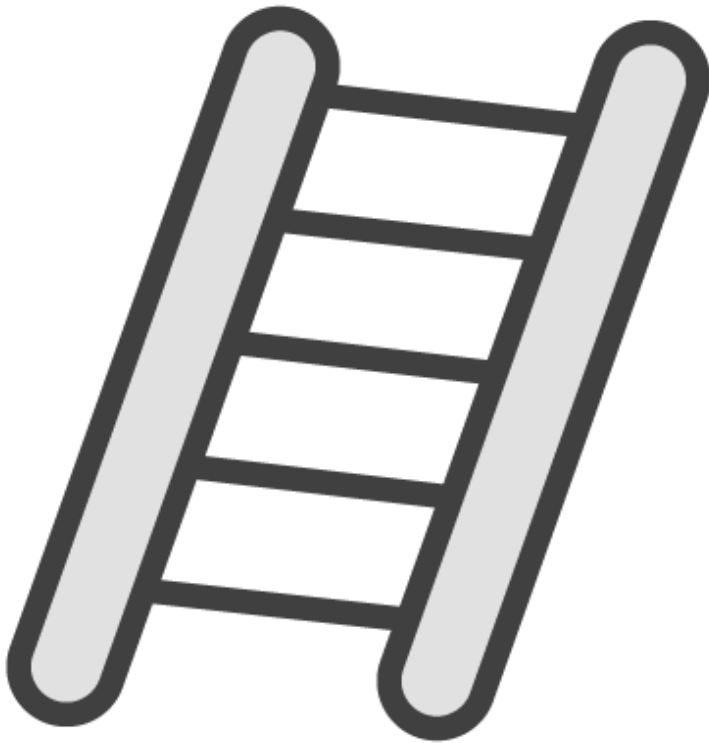


- Sensitivity
 - Confidentiality
 - Integrity



- Criticality
 - Availability

Levels of Data Classification:



- Distinct levels
 - Each with separate handling requirements
 - Documented parameters to decide classification levels

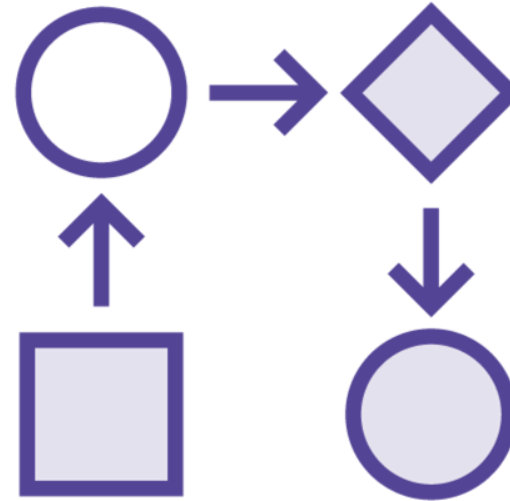
Process for Data Classification



Data
identification

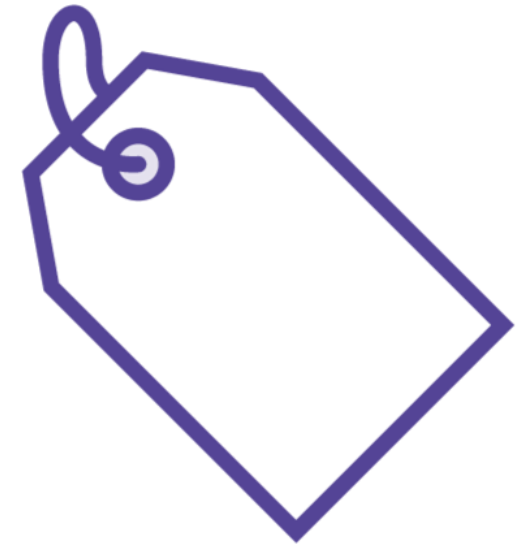


Determination
of data owner



Data
mapping

- Data flow diagrams
- Flowcharts



Labelling

Labelling



- Indication of classification
 - Mandates handling
- Consistent
 - Across the organization
- Benefits and disadvantages

Protecting Data

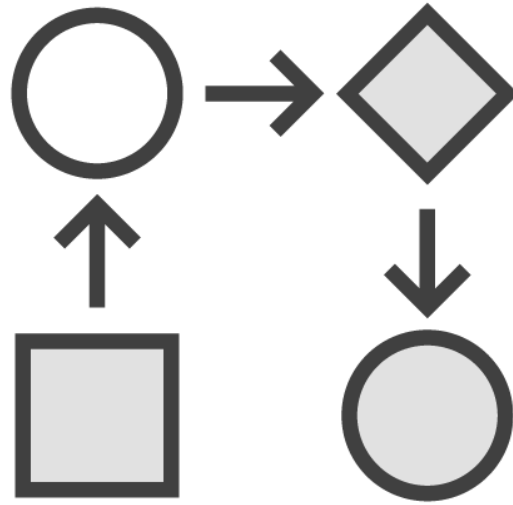


Policy

Data protection starts with policy:



Ownership

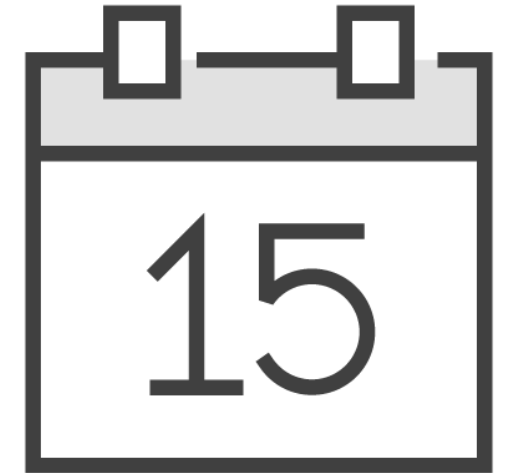


Handling
requirements



Compliance
with:

- Laws
- Regulations
- Procedures



Retention period

- Business requirements
- Legal requirements



Data Mapping



- Location and uses of data
- Data flows
- Normalization of data
 - Standard format

Data

Structured data

Defined structure

Database schema

Index based on defined fields

Data warehouse

Unstructured Data

Undefined data

Email

Analytics based on content
(individual words)

“Big Data”



Semi-Structured Data



- No rigid schema
- Does not fit a normal relational database model
 - XML
 - csv files
 - Emails

Intellectual Property

Patents

Copyrights

Trademarks

Trade secrets



Key Points Review



Data is protected from compromise according to its value

This requires:

- Ownership
- Classification
- Protection of Intellectual Property

Data Disposition



Data Mining



Searching and analysis of data to support business

- Marketing
- Research



Real-time analysis



**Business intelligence
(agile)**

Retrieving Archived Data



Procedures

- Working with CSP for data access
 - Slow access
- Backups and archival schedule

Data Retention



- Business needs
- Legal requirements
 - Legal hold

Destruction of Data



Difficult to ensure destruction by the CSP

- Hardware destruction
 - Only truly secure way to ensure data deletion
 - Data remanence
- Overwriting
- Degaussing

Bit Splitting

Protects data from compromise by encrypting the data and then splitting the encrypted data into pieces that are stored at different locations. Unauthorized access to data at only one location would not allow the unauthorized person to understand the data



Erasure Coding

The data is split into fragments and built out with redundant characters. This allows the reconstruction of the data if some bits are erased (lost). It is often described as n of m , where ' n ' fragments out of ' m ' are needed to reconstruct the data. In a 10/16 model ten pieces out of 16 would be needed to reconstruct the data.

Also known as forward error correction (FEC)

Reed Solomon was an early example of this.



Cryptographic Erasure / Cryptoshredding

The process of encrypting the data to be protected.



Encrypting the key
used to encrypt
the data



Destruction of the
key used to
encrypt the key



Should ensure
data is
irretrievable



Key Points Review



It is not possible to ensure that a CSP's hardware is properly destroyed at end of life.

Contracts and SLAs does not guarantee secure deletion – the consumer should ensure secure data deletion

