CCSP

CCSP EXAM CRAM

EXAM PREPARATION SERIES

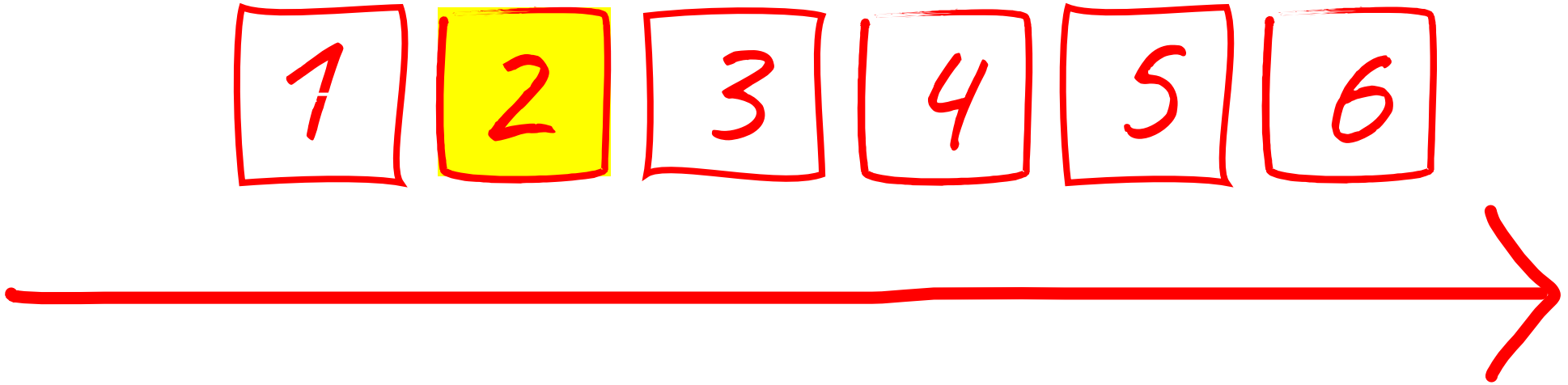
2023 EDITION

DOMAIN 2

Coverage of every topic in the official exam syllabus!

with **Pete Zerger** vCISO, CISSP, MVP

LESSONS IN THIS SERIES



One lesson for each exam domain

...and a consolidated full course video when the series is complete

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
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%

Domain 2 is the focus of this video

CCSP

EXAM STUDY GUIDE

& PRACTICE TESTS BUNDLE

BUY IT NOW AT amazon.com

Link to the latest exam bundle in the video description !

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 2

Cloud Data Security

I will cover every topic mentioned in the exam syllabus!

INSIDE CLOUD AND SECURITY

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 2 Cloud Data Security

I will also provide examples of concepts when possible

INSIDE CLOUD AND SECURITY

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 2 Cloud Data Security

as well as a bit of show-and-tell
in a real cloud environment

INSIDE CLOUD AND SECURITY

EXAM ESSENTIALS – DOMAIN 2

Role of all these in the 'cloud secure data lifecycle'

Risk & controls in each phase of the cloud data lifecycle

Which risks appear in each phase and which controls should be used to address.

Various cloud data storage architectures

Long-term, ephemeral, raw, file-based, block, and databases.

How and why encryption is implemented in the cloud

Role of cryptography, encryption, key and certificate management, and HSMs.

Practices of obscuring data

Masking, anonymization, tokenization.

Elements of data logging, storage, and analysis

Importance of logging, key data elements, SIEM technology, implementation, and challenges.

Importance of egress monitoring

Data loss prevention solutions, identification through tags, pattern matching, and labels.

EXAM ESSENTIALS – DOMAIN 2

Role of all these in the 'cloud secure data lifecycle'

Data flows & their use in a cloud environment

Details such as ports, protocols, services, and endpoints are captured in data flow diagrams.

Purpose & method of data categorization & classification

How to assign data categories and classifications, data mapping and labeling.

Roles, rights, & responsibilities of data ownership

Roles like data subject, owner, controller, processor and custodians.

Data discovery methods

Know differences between structured, unstructured, semi-structured.

Objectives & tools for info rights management (IRM)

Tools that protect data rights, provide permissions based on roles and responsibilities.

Policies for data retention, deletion, & archiving

Retention and disposal formats, affect of regulations on these, policy lifecycle.

2. CLOUD DATA SECURITY

2.1 Describe Cloud Data Concepts

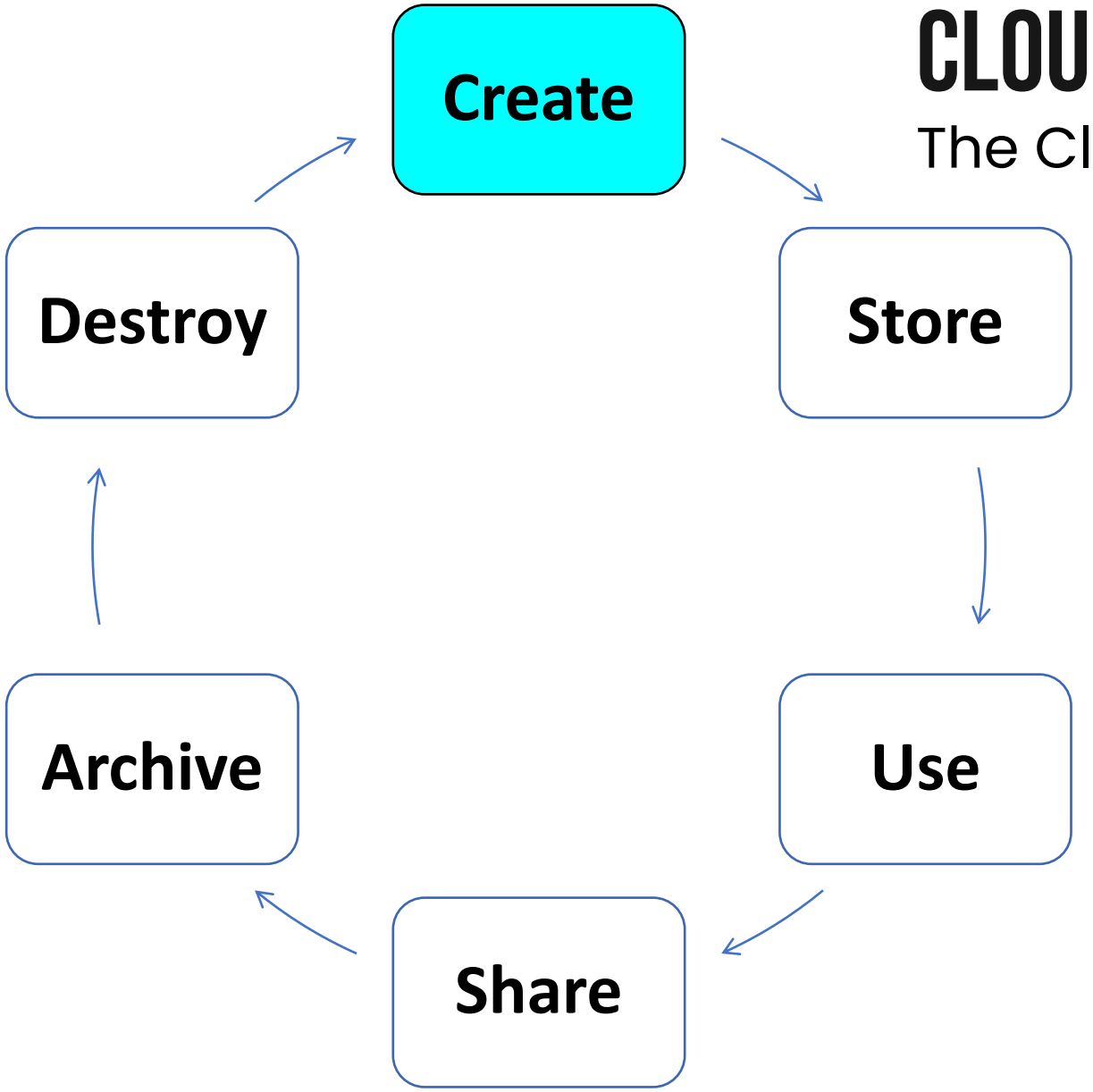
Cloud Data Lifecycle Phases

Data Dispersion

Data Flows

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model



Can be created by **users**

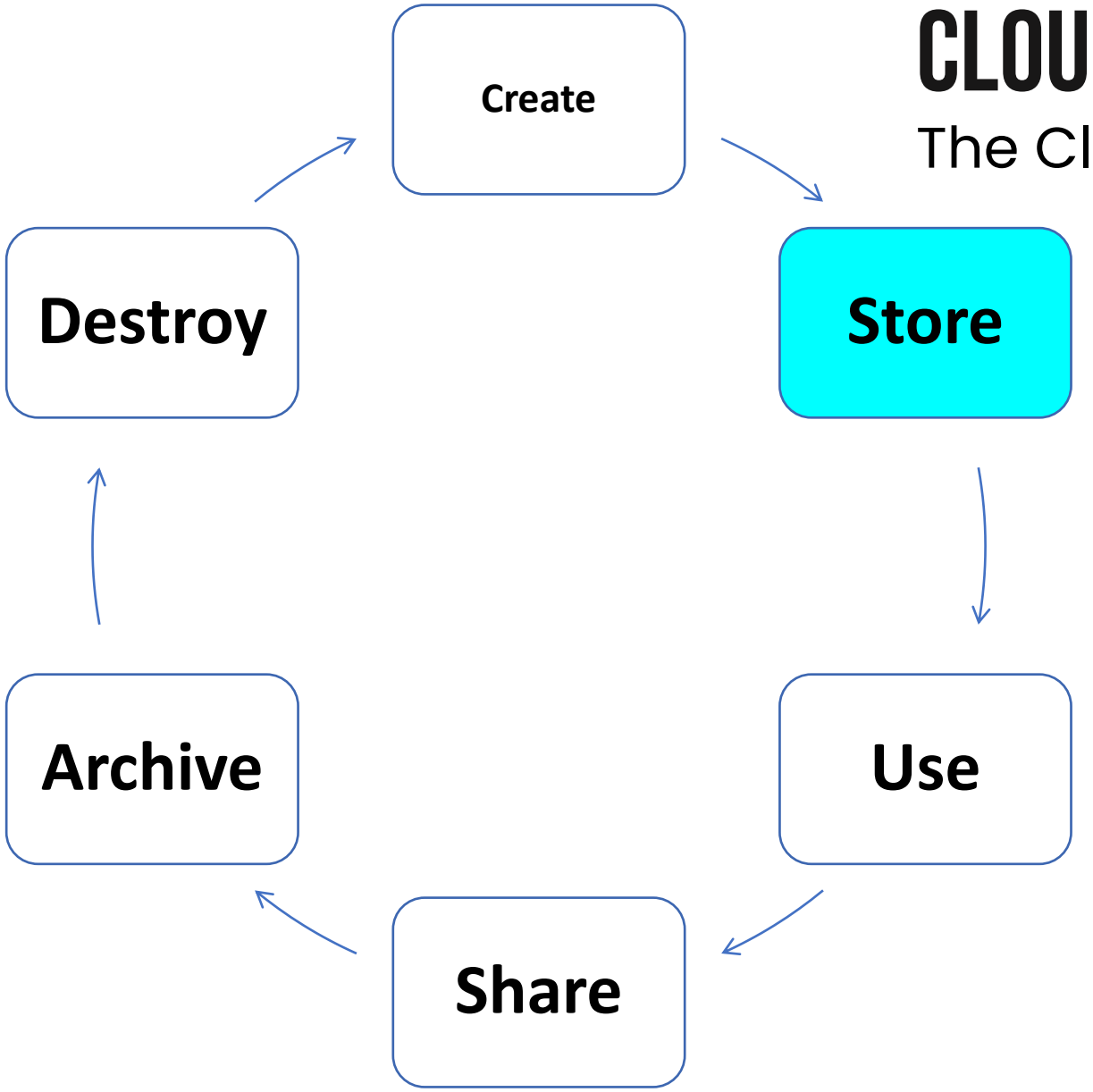
a user creates a file

Can be created by **systems**

a system logs access

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model

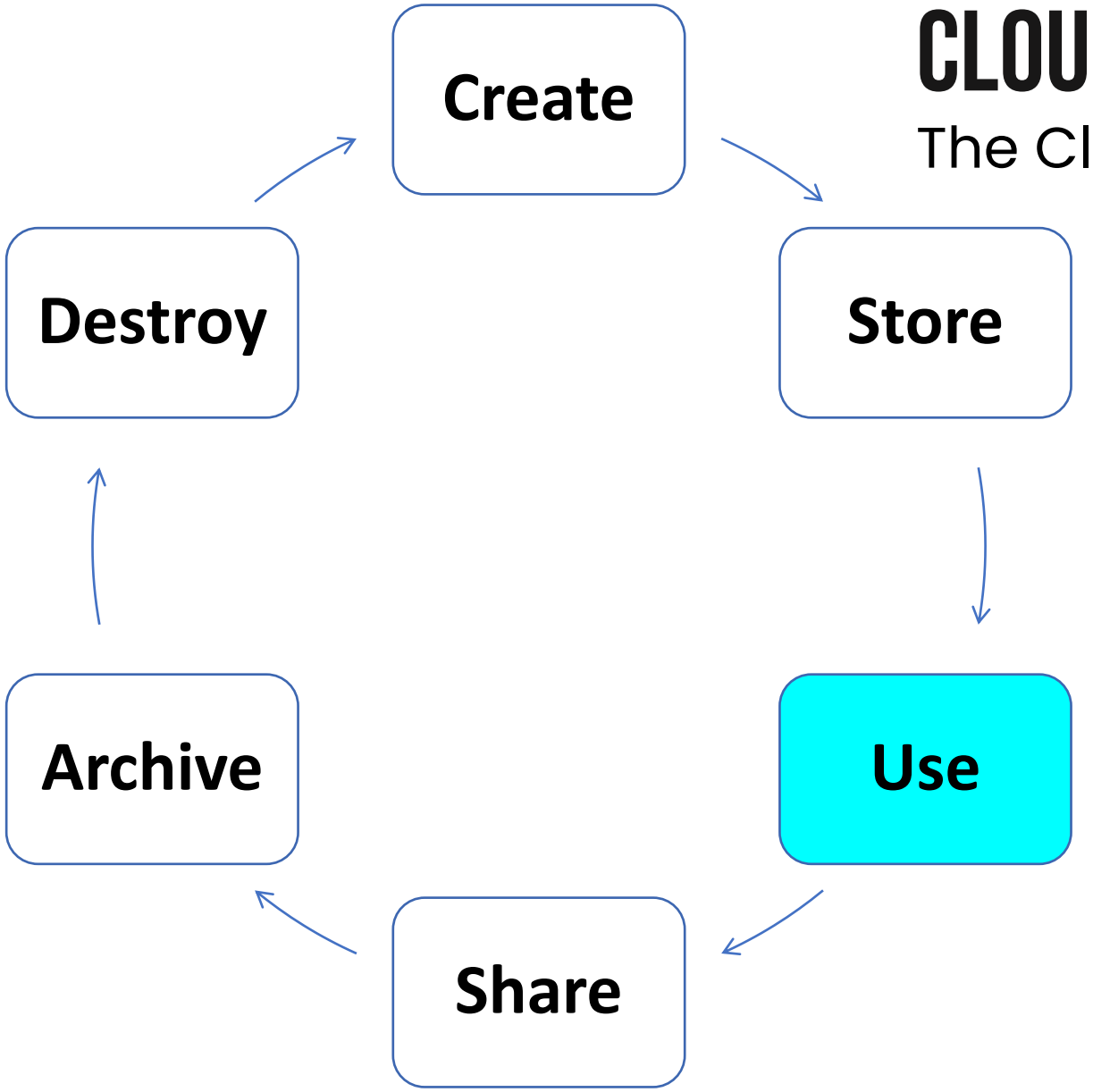


To ensure it's handled properly, it's important to ensure data is **classified** as soon as possible.

Ideally, data is encrypted at rest

CLOUD SECURE DATA LIFECYCLE

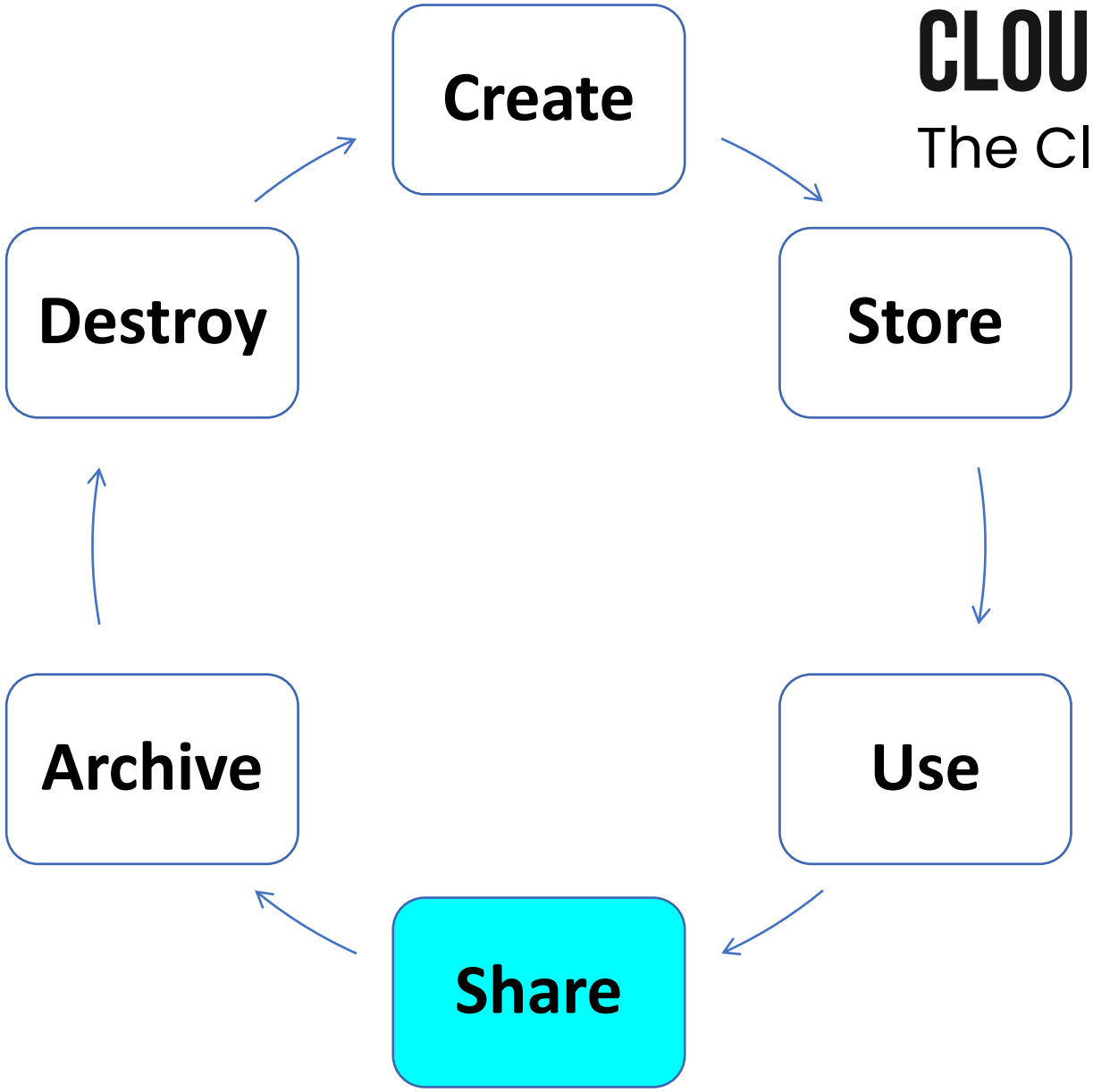
The Cloud Security Alliance model



Data should be **protected** by adequate security controls based on its classification.

CLOUD SECURE DATA LIFECYCLE

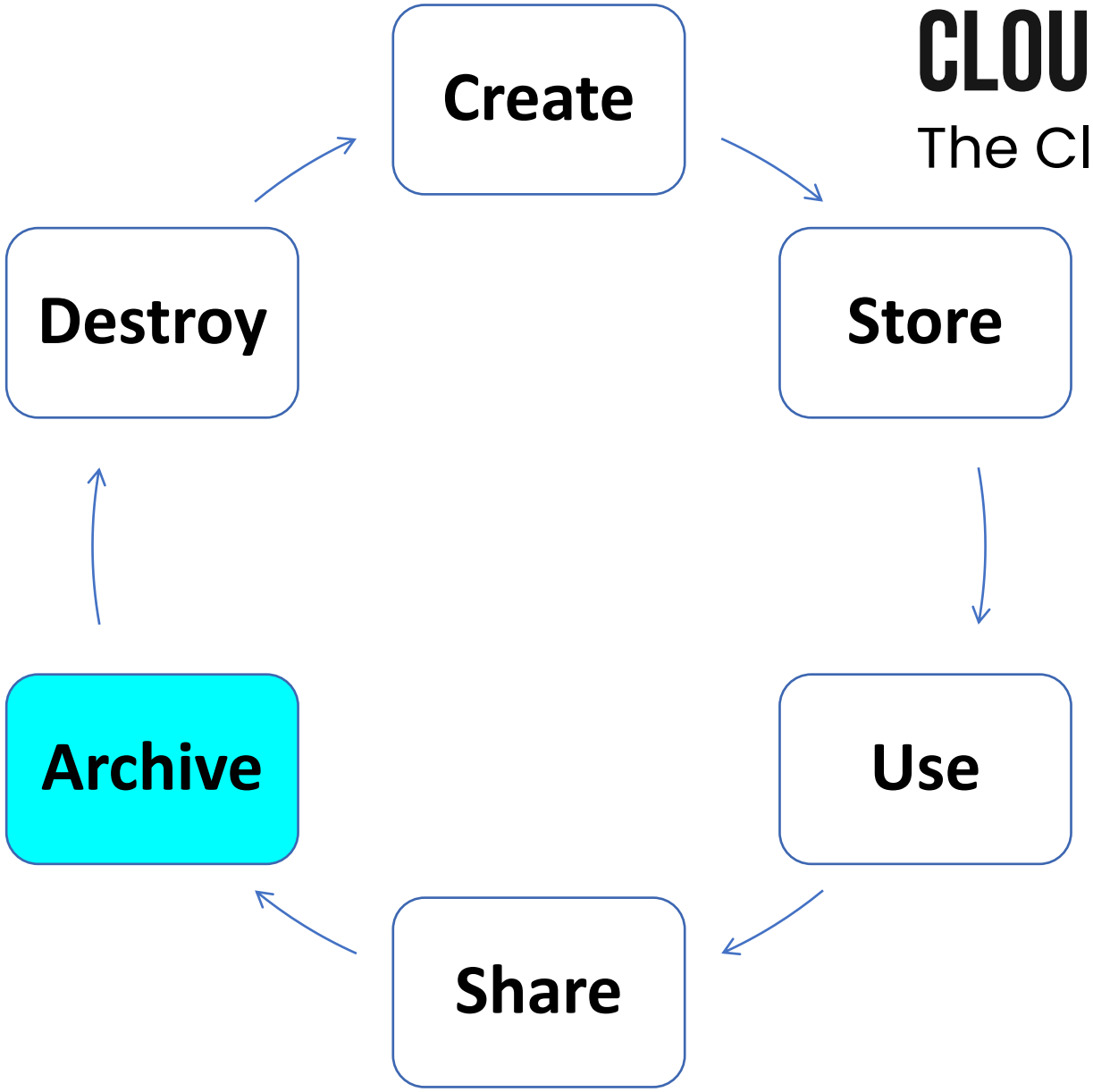
The Cloud Security Alliance model



refers to anytime data is in use or in transit over a network

CLOUD SECURE DATA LIFECYCLE

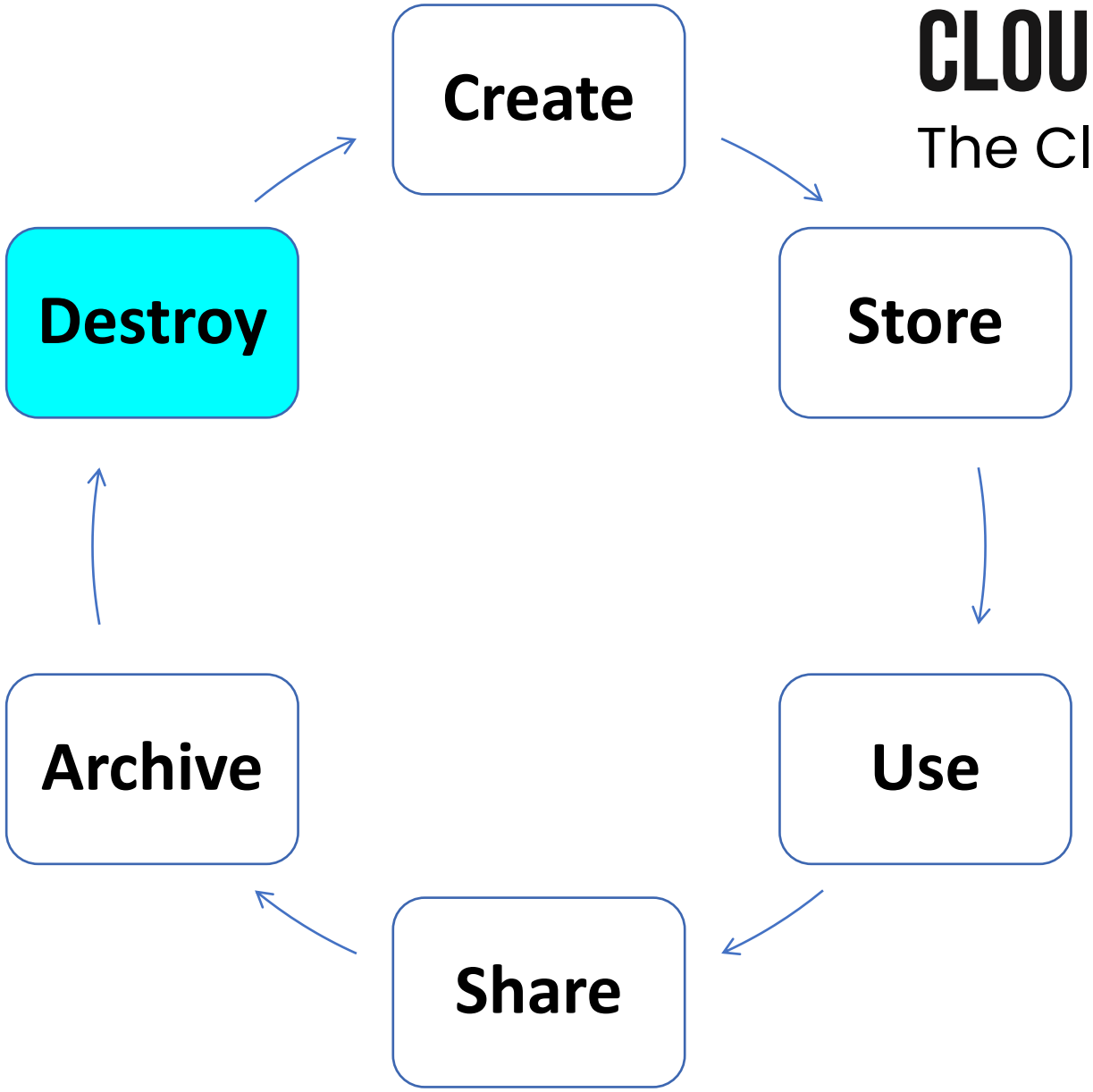
The Cloud Security Alliance model



Archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model



When data is no longer needed, it should be destroyed in such a way that it is not readable nor recoverable.

Crypto-shredding happens in this phase!

DATA DISPERSION

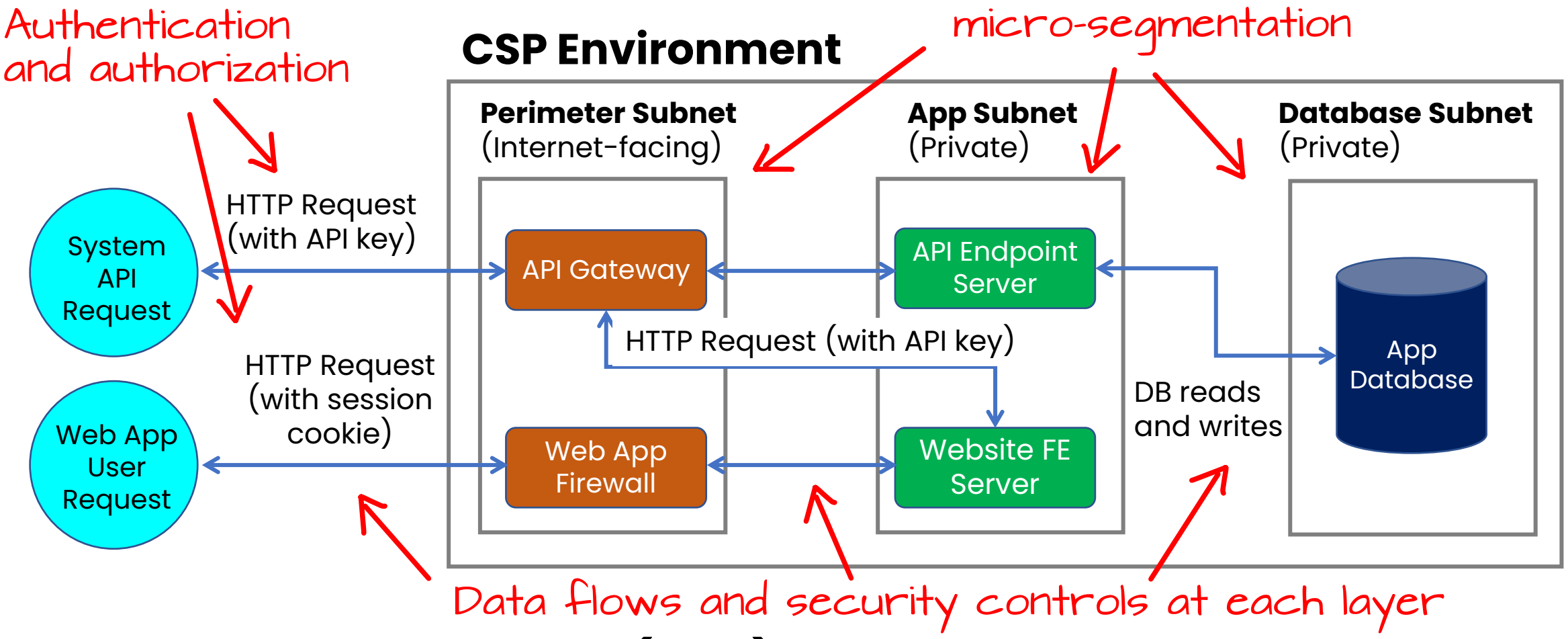
A core principle of business continuity says that important data should always be stored in more than one location

Data dispersion is easier in the cloud because the CSP owns the underlying complexity that delivers site-level resiliency.

Cloud storage for IaaS includes different levels of storage redundancy, including:

- **Local** – replicas within a single datacenter
- **Zone** – replicas to multiple datacenters within a region
- **Global** – region level resiliency (replicas to backup region)

DATA FLOWS



A **data flow diagram (DFD)** is useful to gain visibility and ensure that adequate security controls are implemented

DATA FLOWS

A **data flow diagram (DFD)** is useful to gain visibility and ensure that adequate security controls are implemented

BENEFITS

Decreased development time and faster deployment of new system features. and with reduced security risk!

Visibility into data movement, critical for regulatory compliance, where data security is often mandated in law.

Some compliance frameworks require DFDs to capture specific information, such as the geographic location of data flows or ownership of systems where data is flowing.

BOTTOM LINE: Creating the DFD can be both a risk assessment activity and a crucial compliance activity.

2. CLOUD DATA SECURITY

2.2 Design and Implement Cloud Data Storage Architectures

Storage Types
(e.g. long term, ephemeral, raw-disk)

Threats to Storage Types

STORAGE TYPES

Know the storage types and security concerns associated with storage for all cloud computing categories

Infrastructure as a service (IaaS)
Ephemeral, raw, long-term, volume, and object

Platform as a service (PaaS)
Disk, databases, binary large object (blob)

Software as a service (SaaS)
Information storage and management, content and file storage, content delivery network (CDN)

These storage types were covered in "Building Block Technologies" in Domain 1

STORAGE TYPES BY CATEGORY

key examples (not exhaustive)

Storage types associated with each cloud computing category

IaaS

- **Raw Storage.** Physical media, allows a VM access a storage LUN
- **Volume storage**. Attached as IaaS Instance (EC)
- **Object storage**. S3 storage bucket, Azure storage

PaaS

- **Structured**. Relational databases (RDBMS)
- **Unstructured**. Big data

SaaS

- **Information Storage and Mgmt**. Data entered via the web interface
- **Content/File Storage**. File-based content
- **Ephemeral Storage**. It used for any temporary data such as cache, buffers, session data, swap volume, etc.
- **Content Delivery Network (CDN)**. Geo-distributed content for (better UX)

THREATS TO STORAGE TYPES

All of these can happen in the cloud, it is largely a question of "who is responsible?"

There are universal threats to data at rest (in storage) regardless of the location, on-premises or in the cloud

Universal threats from the perspective of the **CIA Triad**:

- **Unauthorized access** threatens **C**onfidentiality
- **Improper modification** threatens **I**ntegrity
- **Loss of connectivity** threatens **A**vailability

OTHER THREATS:

- Jurisdictional issues
- Denial of service
- Data corruption/destruction
- Theft or media loss
- Malware and ransomware
- Improper disposal

THREATS TO STORAGE TYPES

Unauthorized Access

User accessing data storage without proper authorization presents security concerns

Customer must implement proper access control, CSP must provide adequate logical separation

Unauthorized Provisioning

Primarily a cost and operational concern

Ease of use can lead to unofficial use, unapproved deployment, and unexpected costs

Shadow IT a common issue

Loss of Connectivity

Loss of connectivity for any reason, whether network connectivity, access controls, authentication services, etc.

THREATS TO STORAGE TYPES

Jurisdictional Issues

GDPR, Germany

Data transfer between countries can run afoul of legal requirements.

Privacy legislation bars data transfer to countries without adequate privacy protections

Customer bears some responsibility!

Denial of Service

In the event a network connection is severed between the user and the CSP. CSPs are better prepared to defend against DDoS attacks.

Data Corruption or Destruction

Human error in data entry, malicious insiders, hardware and software failures, natural disasters rendering data or storage media unusable.

Defenses: least privilege, RBAC, offsite data backups

THREATS TO STORAGE TYPES

Theft or Media Loss

In the cloud, CSPs retain responsibility for preventing the loss of physical media through appropriate physical security controls

Malware and Ransomware

Ransomware not only encrypts data stored on local drives but also seeks common cloud storage locations like SaaS apps.

Responsibility will vary by cloud category

Improper Disposal

Ensuring that hardware that has reached the end of its life is properly disposed of in such a way that data cannot be recovered.

CSP responsible for hardware disposal

RANSOMWARE COUNTERMEASURES & PREVENTION

There are a number of countermeasures and prevention techniques:

COUNTERMEASURES

- Back up your computer
- Store backups separately
- File auto-versioning

cloud-hosted email and file storage ease this process

RANSOMWARE COUNTERMEASURES & PREVENTION

There are a number of countermeasures and prevention techniques:

PREVENTION

- Update and patch computers
- Use caution with web links
- Use caution with email attachments
- Verify email senders
- Preventative software programs
- User awareness training

AI-driven cloud services offer help with these

Most important defense!

THREATS TO STORAGE TYPES

Regulatory Compliance

Certain cloud service offerings may not meet all the organization's compliance requirements, which leads to **two security concerns**:

THREATS TO STORAGE TYPES

Regulatory Compliance

Certain cloud service offerings may not meet all the organization's compliance requirements, which leads to **two security concerns**:

First are the consequences of noncompliance like fines or suspension of business operations.

Second is the reason for the compliance requirements— **data protection**.

Requirements may include use of specific encryption standards, handling, and retention

All the regulatory standards you need for the exam are covered in the exam cram series

2. CLOUD DATA SECURITY

2.3 Design and Apply Data Security Technologies and Strategies

Encryption and Key Management

Hashing

Data Obfuscation
(e.g., masking, anonymization)

Tokenization

Data Loss Prevention (DLP)

Keys, Secrets, and Certificates Management

CONCEPT: SYMMETRIC VS ASYMMETRIC

Symmetric

faster

Relies on the use of a **single shared secret key**. Lacks support for scalability, easy key distribution, and nonrepudiation

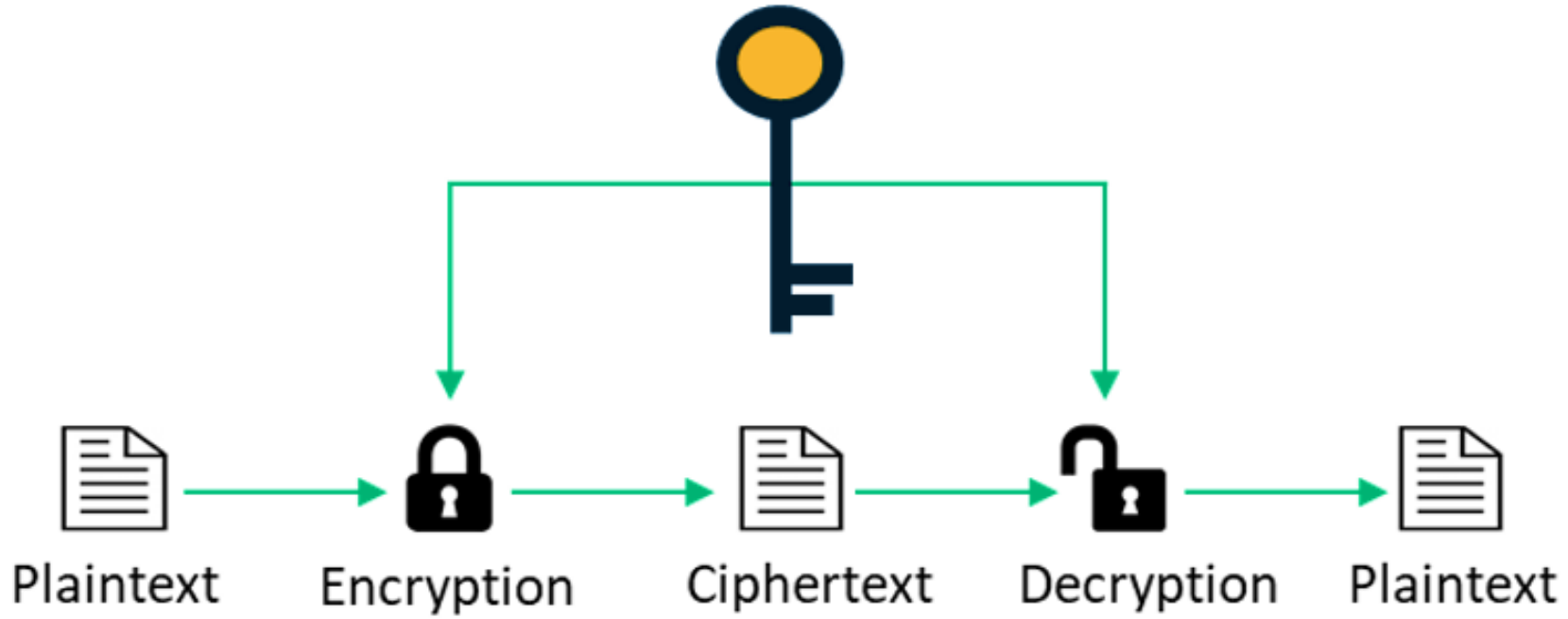
Asymmetric

scalable

Public-private key pairs for communication between parties. Supports scalability, easy key distribution, and nonrepudiation

CONCEPT: SYMMETRIC VS ASYMMETRIC

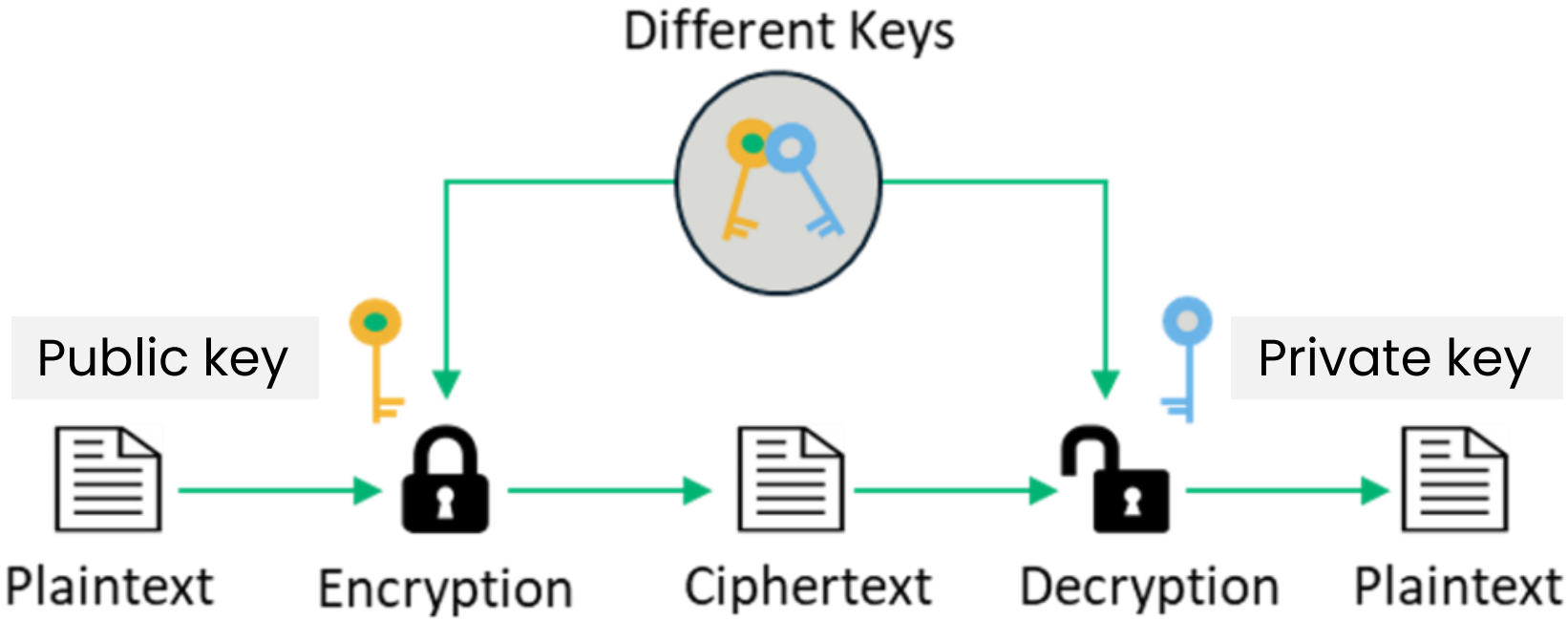
Symmetric



sender and recipient using a single shared key

CONCEPT: SYMMETRIC vs ASYMMETRIC

Asymmetric



Sender encrypts using public key (shared)
Recipient decrypts using private key (unshared)

EXAMPLE: ASYMMETRIC CRYPTOGRAPHY

Franco sends a message to Maria, requesting her public key

Maria sends her public key to Franco

Franco uses Maria's public key to encrypt the message and sends it to her

Maria uses her private key to decrypt the message

ASYMMETRIC KEY TYPES

Public keys are shared among communicating parties.

Private keys are kept secret.

DATA

To encrypt a message: use the recipient's public key.

To decrypt a message: use your own private key.

DIGITAL SIGNATURE

To sign a message: use your own private key.

To validate a signature: use the sender's public key.

Each party has both a private key and public key!

RELATED CONCEPTS

Trust model

A model of how different certification authorities trust each other and how their clients will trust certificates from other certification authorities.

The four main types of trust models that are used with public key infrastructure (PKI) are bridge, hierarchical, hybrid, and mesh.

Key escrow

Addresses the possibility that a cryptographic key may be lost.

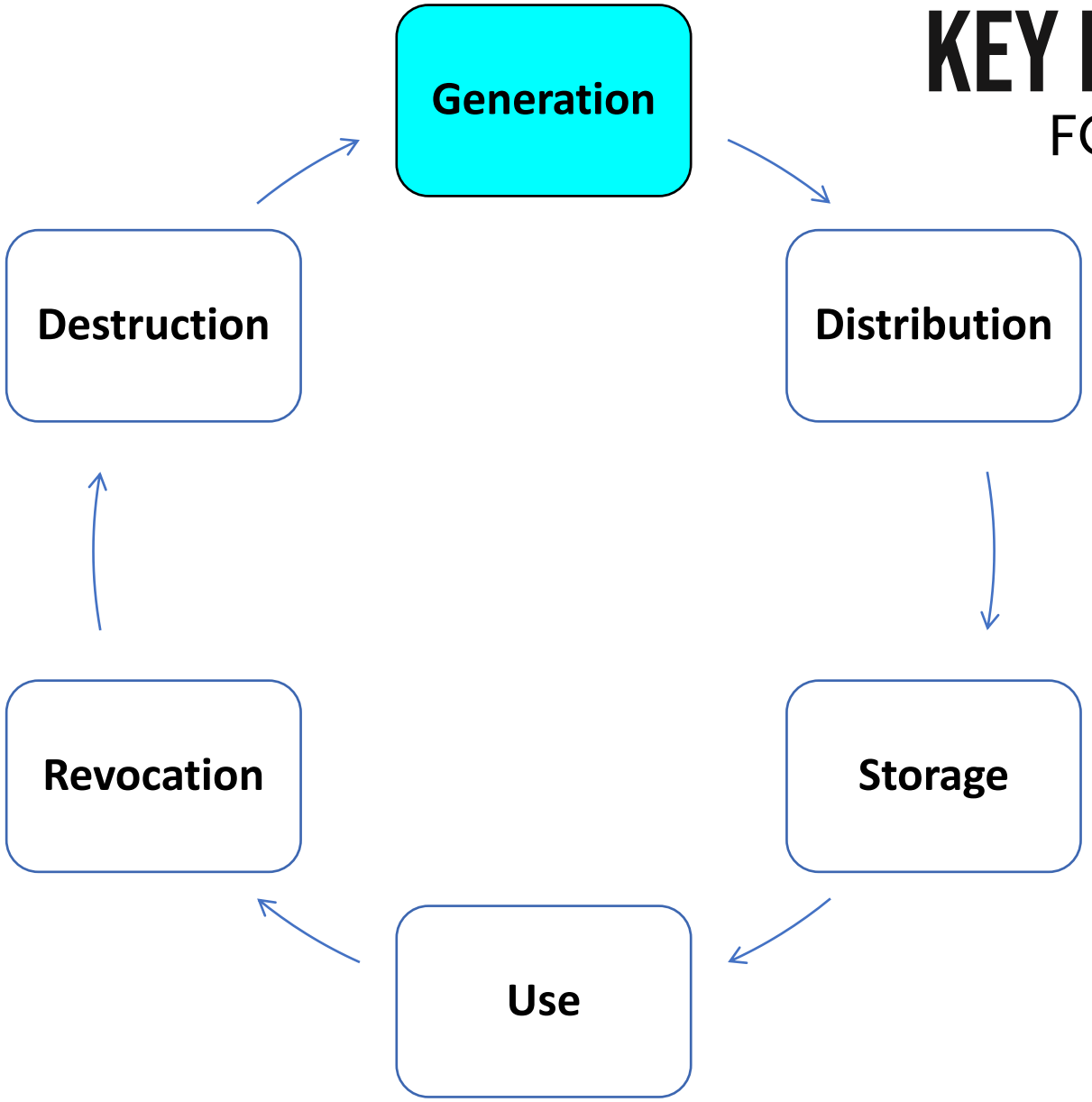
The concern is usually with symmetric keys or with the private key in asymmetric cryptography.

If that occurs, then there is no way to get the key back, and the user cannot decrypt messages.

Organizations establish key escrows to enable recovery of lost keys.

KEY MANAGEMENT STRATEGY

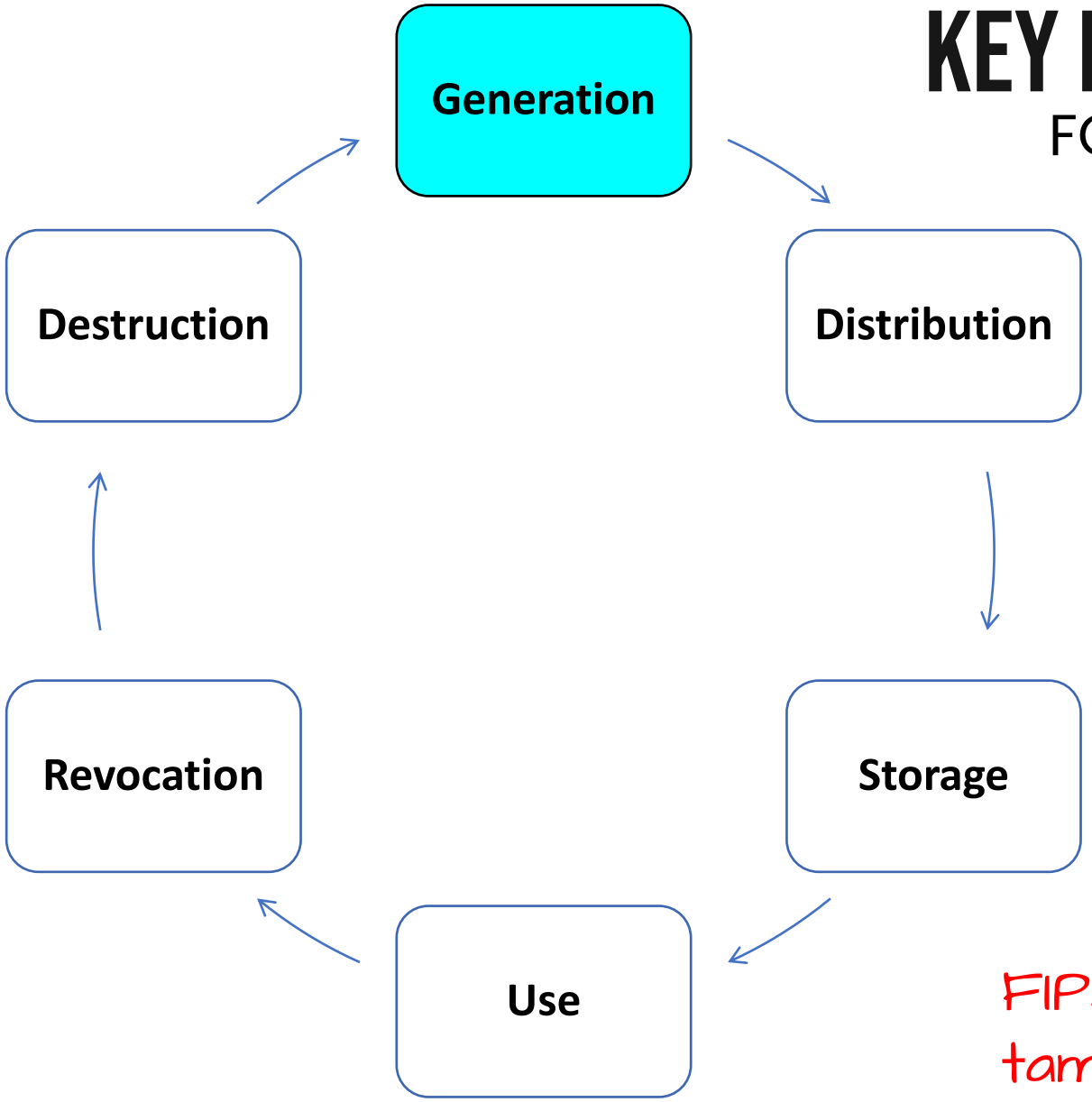
FOR ENCRYPTION KEY LIFECYCLE



Encryption keys should be generated within a trusted, secure cryptographic module

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



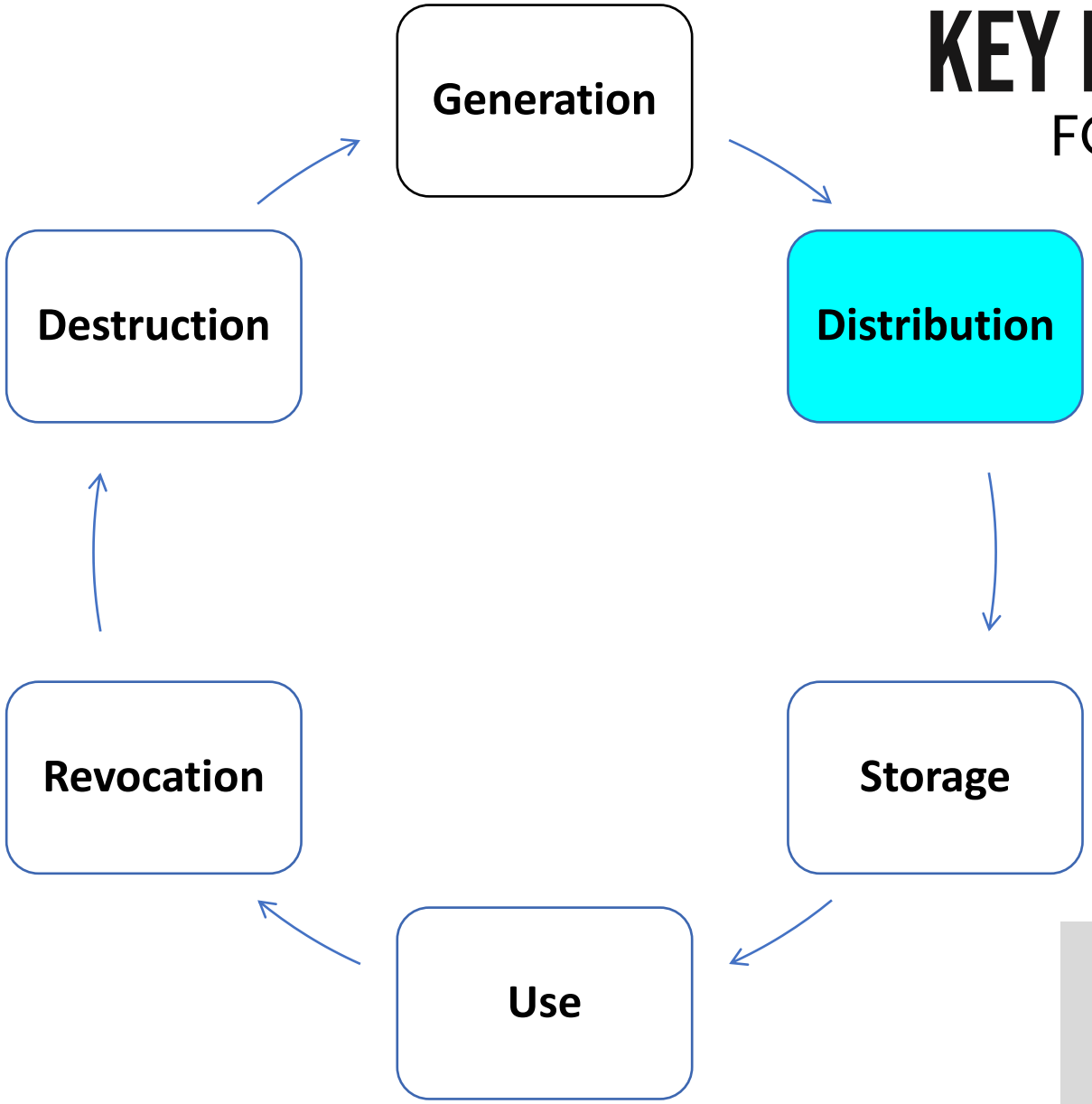
Encryption keys should be generated within a trusted, secure cryptographic module

Should use strong, random keys using cryptographically sound inputs like random numbers

FIPS 140-2 validated modules provide tamper resistance and key integrity

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



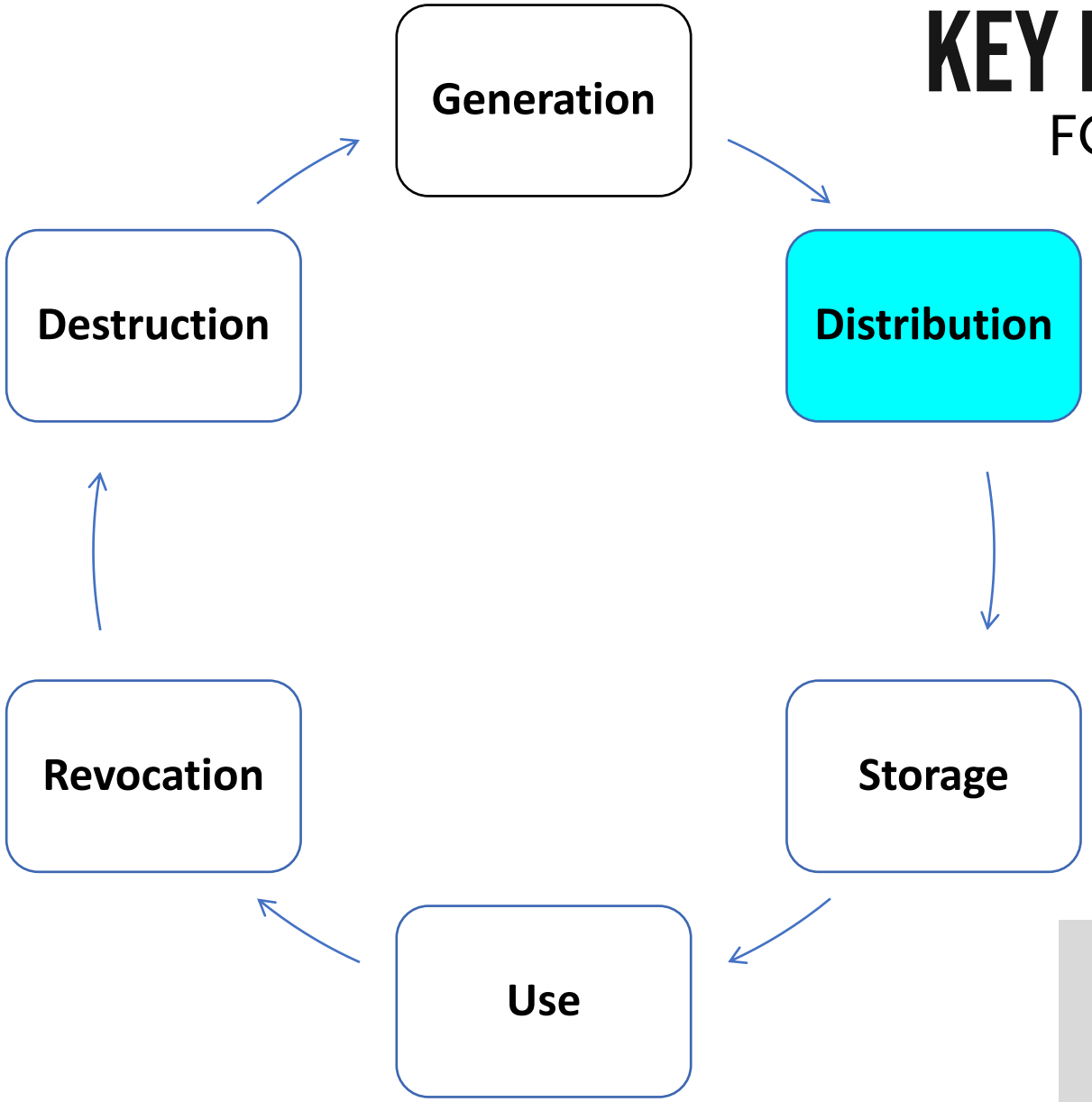
Encryption keys should be distributed securely to prevent theft/compromise during transit

BEST PRACTICE:

Encrypt keys with a separate encryption key while distributing to other parties

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



Encryption keys should be distributed securely to prevent theft/compromise during transit

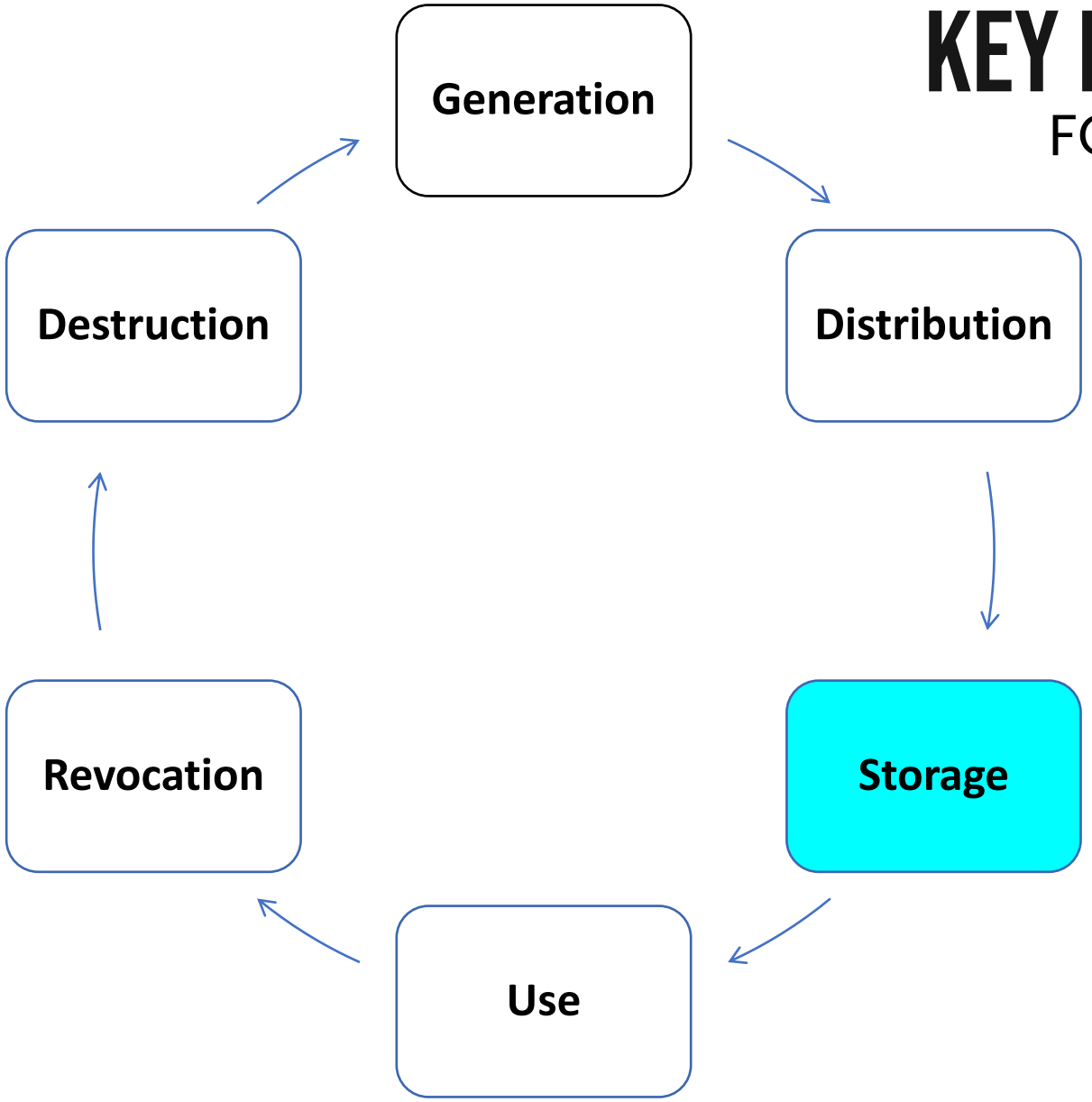
Plan for securely transferring symmetric keys and distributing keys to the key escrow agent

BEST PRACTICE:

Encrypt keys with a separate encryption key while distributing to other parties

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE

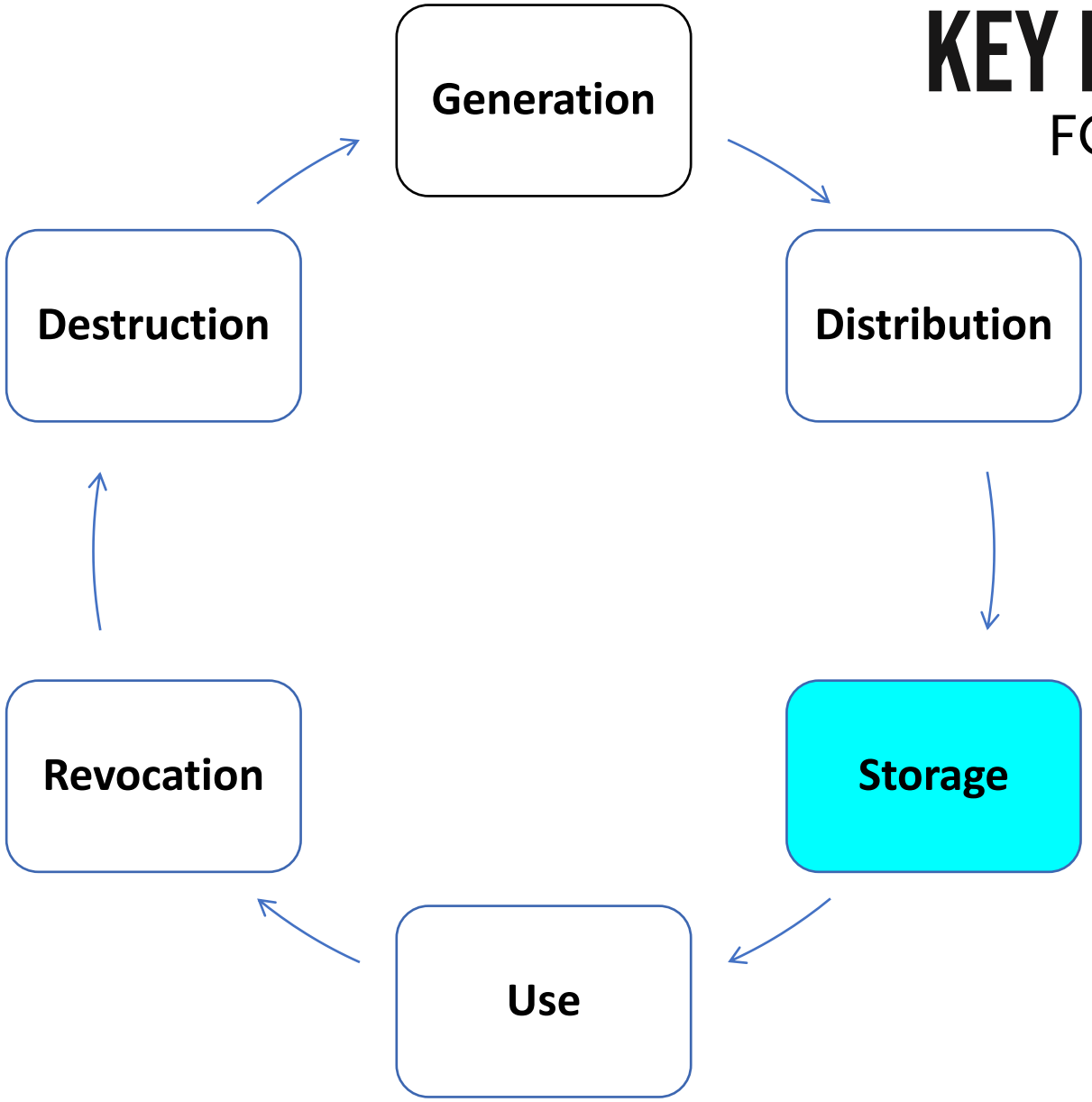


Encryption keys must be protected at rest and should never be stored in plaintext

This includes keys in volatile and persistent memory

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



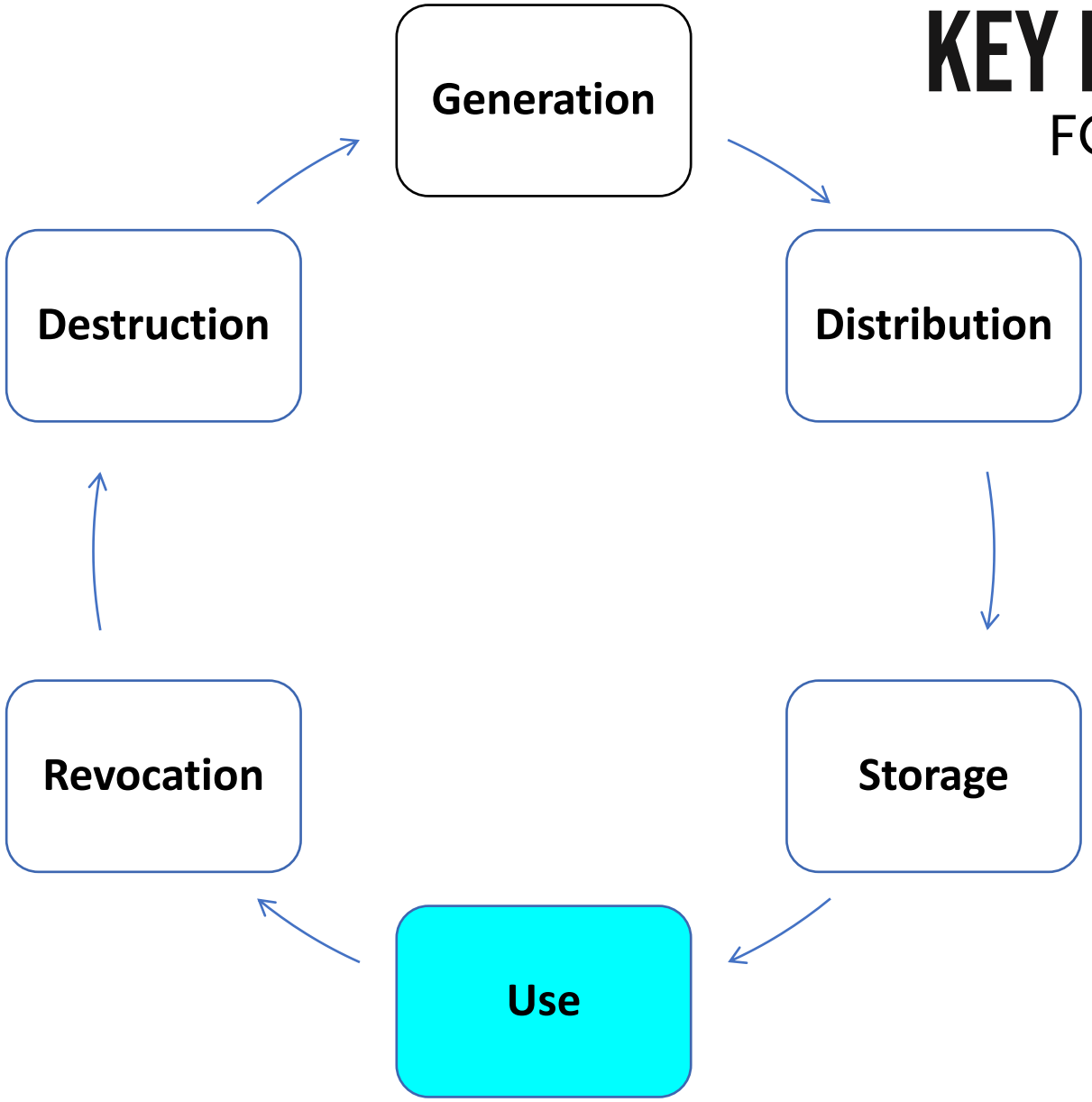
Encryption keys must be protected at rest and should never be stored in plaintext

Storing keys in a secure manner, whether encrypted in a key vault or on a physical device

Also consider handling in the process of storing copies for retrieval if a key is ever lost (known as key escrow)

KEY MANAGEMENT STRATEGY

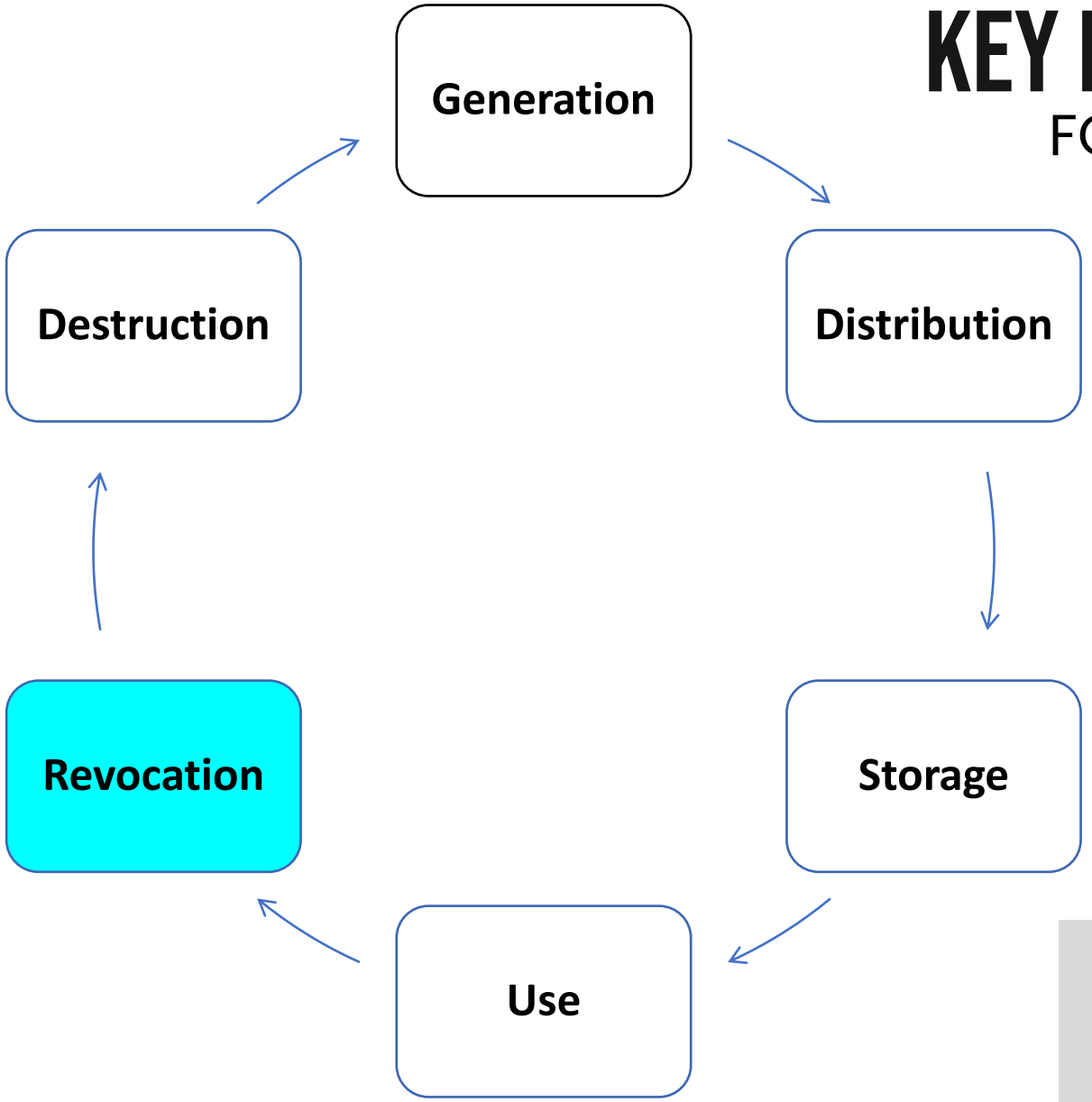
FOR ENCRYPTION KEY LIFECYCLE



Using keys securely, primarily focused on access controls and accountability

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



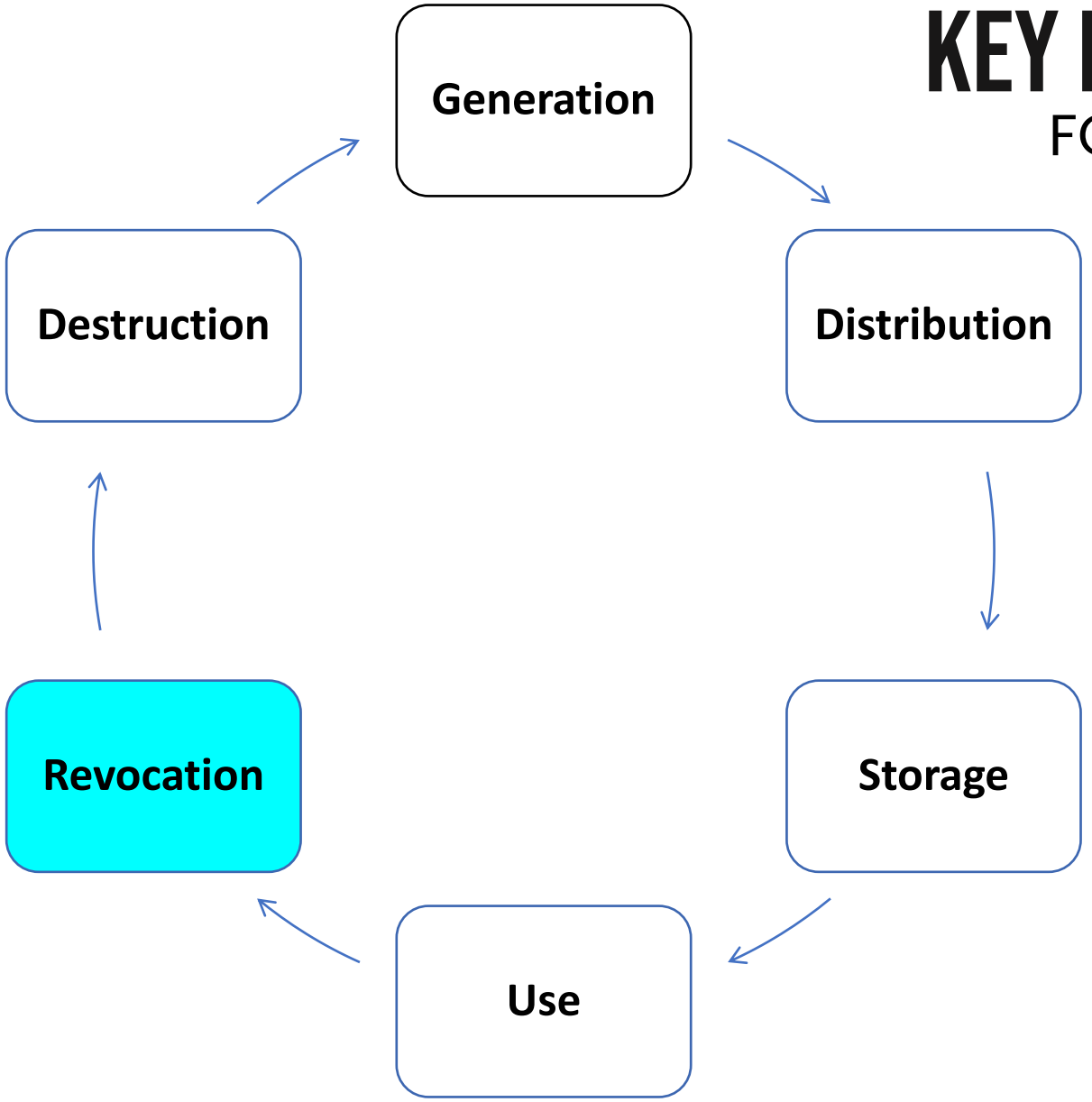
A process for revoking access at separation, policy breach, device or key compromise.

EXAMPLE:

In PKI, you would revoke the certificate on the issuing Certification Authority (CA)

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE

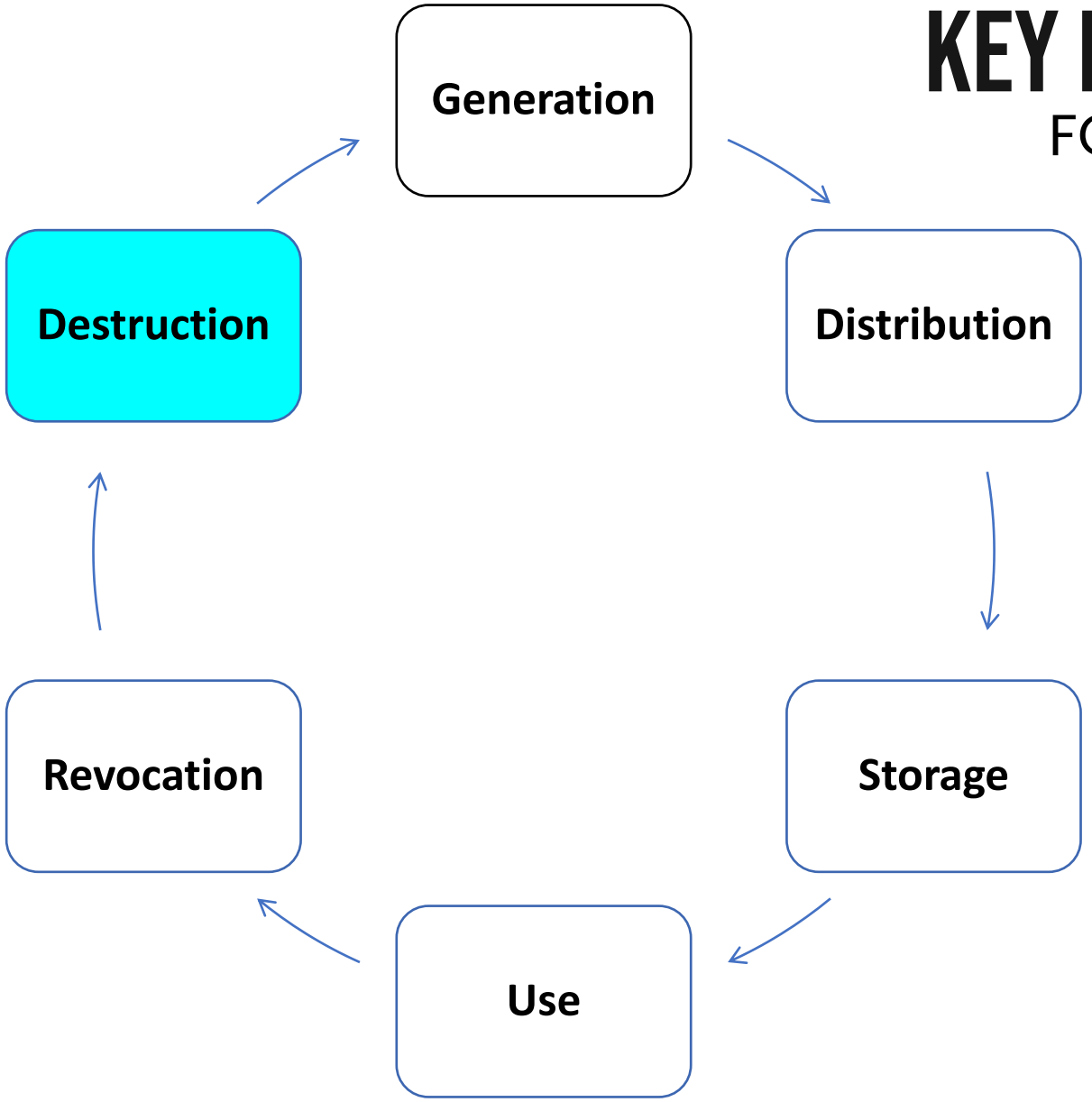


A process for revoking access at separation, policy breach, device or key compromise.

A process for archiving keys no longer needed for routine use, in case needed for existing data.

KEY MANAGEMENT STRATEGY

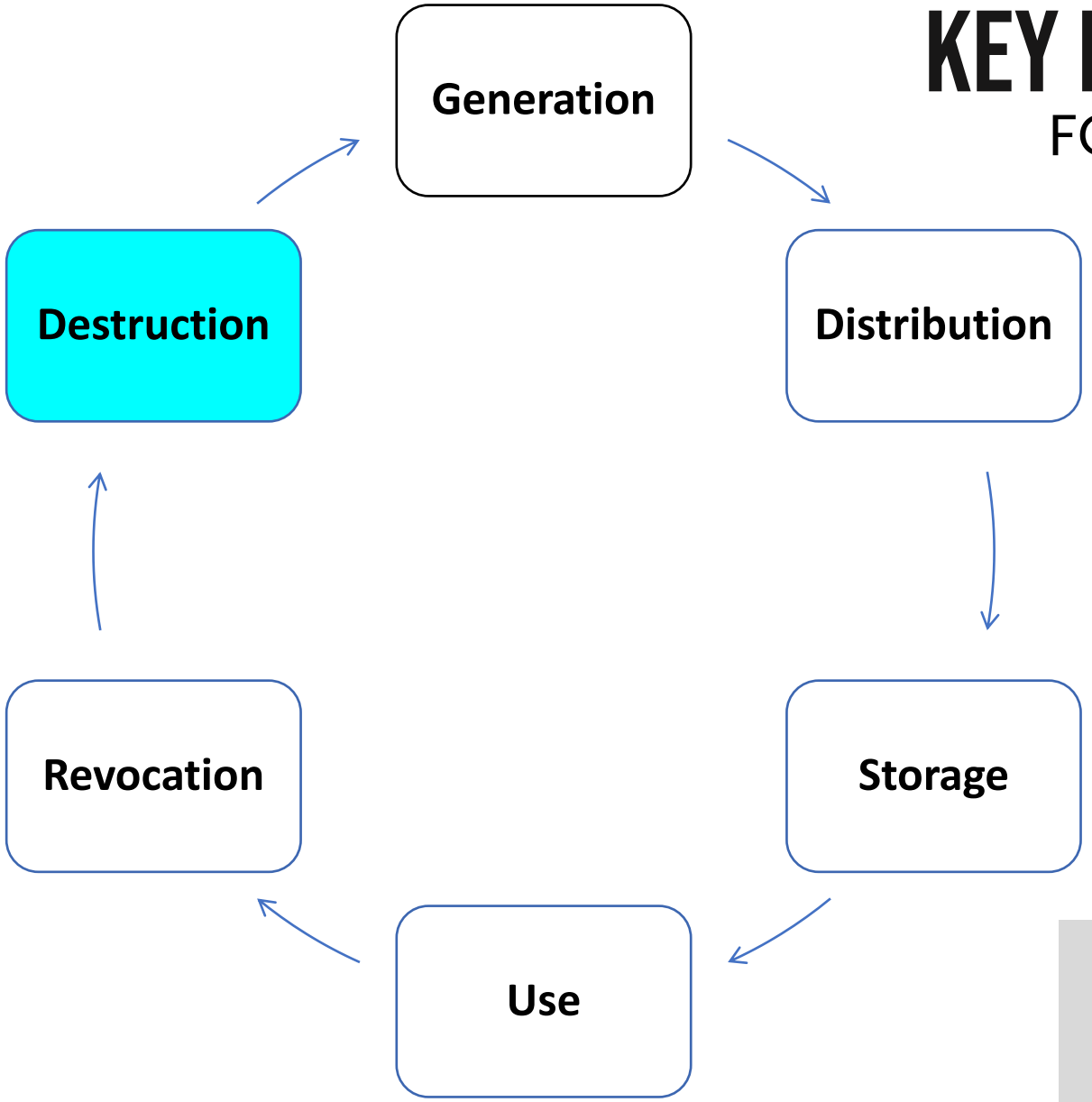
FOR ENCRYPTION KEY LIFECYCLE



Key destruction is the removal of an encryption key from its operational location.

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



Key destruction is the removal of an encryption key from its operational location.

Key deletion goes further and removes any info that could be used to reconstruct that key.

EXAMPLE: (MS Intune, AirWatch)

MDM systems remove certificates from a device during device wipe or retirement.

KEY MANAGEMENT IN THE CLOUD

You need to understand where encryption can be deployed to protect the organization's data and systems

Know the layers and services where you can enable encryption, and your options for key storage and management.

Key storage

CSP-managed or self-managed

Many CSPs offer FIPS compliant virtualized HSMs to securely generate, store, and control access to cryptographic keys.

Self-managed keys typically not the default and may have a cost

Organizations that use multiple cloud providers or need to retain physical control over key management may need to implement a bring-your-own-key (BYOK) strategy.

Regulatory compliance sometimes necessitates BYOK or self-managed

Generally to let the CSP manage keys unless you have requirements that mandate your organization manages keys

OTHER CLOUD ENCRYPTION SCENARIOS

Know the common cloud-based encryption scenarios for storage, services, and applications

Storage-level encryption

Provides encryption of data as it is written to storage, utilizing keys that are controlled by the CSP.

Volume-level encryption

Provides encryption of data written to volumes connected to specific VM instances, utilizing keys controlled by the customer.

Examples: Bitlocker (Windows), DM-Crypt (Linux)

Object-level encryption

Encryption of objects as they are written to storage, in which case the CSP likely controls the keys and could potentially access the data.

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Storage-level encryption in the cloud

EXAMPLE FOR CONTEXT - Available with all CSPs, details vary by CSP.

INSIDE CLOUD AND SECURITY

OTHER CLOUD ENCRYPTION SCENARIOS

Know the common cloud-based encryption scenarios for storage, services, and applications

File-level encryption

Implemented in client apps, such as word processing apps like Microsoft Word or collaboration apps like SharePoint

Will vary by app and CSP platform

Application-level encryption

Implemented in an application typically using object storage

Data entered by user typically encrypted before storage

Database-level encryption

Transparent data encryption (database files, logs, backups), column-level or row-level encryption, or data masking

Will vary by RDBMS platform (MSSQL, MySQL, PostgreSQL)

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements

Anonymization. The process of removing all relevant data so that it is impossible to identify original subject or person.

If done effectively, then GDPR is no longer relevant for the anonymized data.

Good only if you don't need the data!

Anonymization is sometimes called **de-identification**

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements

Anonymization. The process of removing all relevant data so that it is impossible to identify original subject or person.

If done effectively, then GDPR is no longer relevant for the anonymized data.

Pseudonymization. de-identification procedure using pseudonyms (aliases) to represent other data.

Can result in less stringent requirements than would otherwise apply under the GDPR.

Use if you need data and want to reduce exposure

HASHING VS ENCRYPTION

How is hashing different from encryption?

Encryption

Encryption is a two-way function; what is encrypted can be decrypted with the proper key.

Hashing

no way to reverse if properly designed

A one-way function that scrambles plain text to produce a unique message digest.

Conversion of a string of characters into a shorter fixed-length value

Common uses

Verification of digital signatures

Generation of pseudo-random numbers

Integrity services

file hash comparison

HASH FUNCTION REQUIREMENTS

Good hash functions have five requirements:

1. They must allow input of any length.
2. Provide fixed-length output.
3. Make it relatively easy to compute the hash function for any input.
4. Provide one-way functionality.
5. Must be collision free.

Data masking

when only partial data is left in a data field.

for example, a credit card may be shown as

**** **** **** 1234

Commonly implemented within the database tier, but also possible in code of frontend applications

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Database-level
encryption in the cloud

EXAMPLE FOR CONTEXT:
Features will vary by RDBMS & CSP

INSIDE CLOUD
AND SECURITY

DATA PROTECTION & OBFUSCATION

Tokenization

Stateless, stronger than encryption, keys not local

where meaningful data is replaced with a token that is generated randomly, and the original data is held in a vault.

Pseudonymization

Reversal requires access to another data source

de-identification procedure in which personally identifiable information (PII) fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

Tokenization goes further than pseudonymization, replacing your pseudonym with an unrecognizable token

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

a system designed to identify, inventory, and control the use of data that an organization deems sensitive.

spans several categories of controls including detective, preventative, and corrective.

Policies can be typically applied to email, SharePoint, cloud storage, removeable devices, and databases

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

is a way to protect sensitive information and prevent its inadvertent disclosure.

can identify, monitor, and automatically protect sensitive information in documents

monitors for and alerts on for potential breaches, policy violations like oversharing

Protection travels with the document, file, or other data, preventing local override of DLP protections

KEYS, SECRETS, AND CERTIFICATE MANAGEMENT

Keys

are most often used for encryption operations and can be used to uniquely identify a user or system.

Keys should be stored in a tool that implements encryption and requires a strong passphrase or MFA to access.

In the cloud, a key vault (covered in Domain 1)

Secrets

often a secondary authentication mechanism used to verify that a communication has not been hijacked or intercepted.

Certificates

are used to verify the identity of a communication party and also be used for asymmetric encryption by providing a trusted public key.

often used to encrypt a shared session key or other symmetric key for secure transmission.

KEY MANAGEMENT IN THE CLOUD (CSPs - Azure, AWS, GCP)

Key Management Services (KMS)

E.G., Azure Key Vault, AWS KMS, GCP Cloud KMS Vault

CSPs offer a cloud service for centralized secure storage and access for application secrets called a **vault**.

A secret is anything that you want to control access to, such as **API keys**, **passwords**, **certificates**, **tokens**, or **cryptographic keys.**

Service will typically offer programmatic access via API to support DevOps and continuous integration/continuous deployment (CI/CD)

Access control at vault instance-level and to secrets stored within.

Secrets and keys can generally be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Key Vault for secrets management

EXAMPLE FOR CONTEXT: Key vault features will vary by CSP

INSIDE CLOUD AND SECURITY

Digital Signatures

Digital signatures are similar in concept to handwritten signatures on printed documents that identify individuals, but they provide more security benefits.

is an encrypted hash of a message, encrypted with the sender's private key.

in a signed email scenario, it provides three key benefits:

Authentication. This positively identifies the sender of the email.

Ownership of a digital signature secret key is bound to a specific user

Non-repudiation. The sender cannot later deny sending the message.

This is sometimes required with online transactions

Integrity. provides assurances that the message has not been modified or corrupted.

Recipients know that the message was not altered in transit

These basics should be more than enough for the CCSP exam

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Key management

management of cryptographic keys in a cryptosystem.

Operational considerations include dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys.

Design considerations include cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Certificate authority (CA)

Certification Authorities create digital certificates and own the policies.

PKI hierarchy can include a single CA that serves as root and issuing, but this is not recommended.

In a single-layer PKI hierarchy, if the server is breached no certificate, including the root, can be trusted!

TYPES OF CERTIFICATES

User

Used to represent a user's digital identity.

In most cases, a user certificate is mapped back to a user account.

Root

A trust anchor in a PKI environment is the root certificate from which the whole chain of trust is derived. this is the root CA.

Domain validation

A Domain-Validated (DV) certificate is an X.509 certificate that proves the ownership of a domain name.

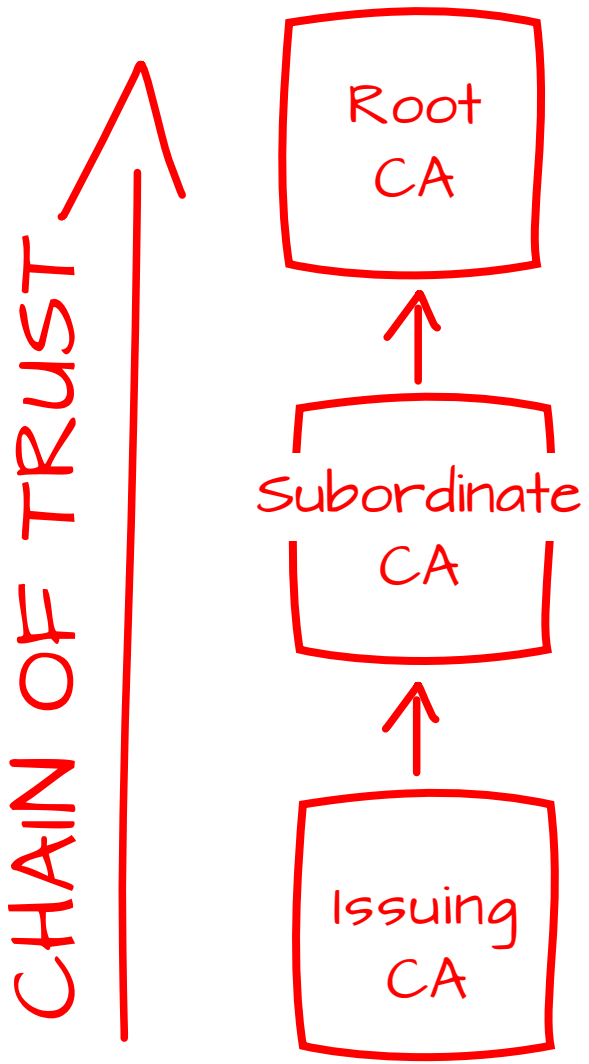
Extended validation

Extended validation certificates provide a higher level of trust in identifying the entity that is using the certificate.

Commonly used in the financial services sector.

TYPES OF CERTIFICATES

These functions can be consolidated to fewer servers, creating a 1 or 2-level hierarchy



Usually maintained in an offline state

Issues certs to new subordinate CAs

Also called a Policy CA or Intermediate CA

Issues certs to new issuing CAs

Certificates for clients, servers, devices, websites, etc. issued from here

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Subordinate CA

A few important details

Regularly issue certificates, making it difficult for them to stay offline as often as root CAs.

Do have the ability to revoke certificates, making it easier to recover from any security breach that does happen

If the issuing CA is breached, its certificate can be revoked and a new one issued.

A single compromised CA does not result in compromise of the root.

Certificate revocation list (CRL)

Contains information about any certificates that have been revoked by a subordinate CA due to compromises to the certificate or PKI hierarchy.

CAs are required to publish CRLs, but it's up to certificate consumers if they check these lists and how they respond if a certificate has been revoked.

CERTIFICATE REVOCATION

Revoking (invalidating) a certificate before expiration

Certificate is effectively cancelled, and certificate serial number added to the **certificate revocation list (CRL)**.

BUT, parties checking the certificate to verify identity or authenticity must check with issuing authority on validity

Two potential options for tracking revocation: ask for the CRL or if available, OCSP endpoint/service.

Endpoint to query for CRL or OCSP is on the certificate

If the other client/server does not check the CRL or OCSP for certificate validity, they may accept an invalid certificate as valid!

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Online Certificate Status Protocol (OCSP)

Offers a faster way to check a certificate's status compared to downloading a CRL.

With OCSP, the consumer of a certificate can submit a request to the OCSP endpoint to obtain the status of a specific certificate.

Certificate signing request (CSR)

Records identifying information for a person or device that owns a private key as well as information on the corresponding public key.

It is the message that's sent to the CA in order to get a digital certificate created.

CN (common name)

the Fully Qualified Domain Name (FQDN) of the entity (e.g. web server)

2.4 Implement Data Discovery

Structured Data

Unstructured Data

Semi-structured Data

Data Location

DATA TYPES

Structured Excel, MSSQL, MySQL, PostgreSQL

Data contained in rows and columns, such as an Excel spreadsheet or relational database.

Often includes a description of its format known as a **data model** or **schema**, which is an abstract view of the data's format in a system.

Data structured as elements, rows, or tuples is given context through the schema.

Discovery methods include:

Metadata, or data that describes data, is a critical part of discovery in structured data.

Semantics, or the meaning of data, is described in the schema or data model and explains relationships expressed in data.

DATA TYPES

Unstructured

Images, video files, social media posts

Data that cannot be contained in a row-column database and does not have an associated data model.

Discovery occurs through **content analysis**, which attempts parse all data in a storage location and identify sensitive information.

Content analysis (discovery) methods include:

Pattern matching, which compares data to known formats like credit card numbers. DLP tools often have pre-defined 'sensitive data types'

Lexical analysis attempts to find data meaning and context to discover sensitive info that may not conform to a specific pattern.

Hashing attempts to identify known data by calculating a hash of files and comparing it to a known set of sensitive file hashes.

Only good for data that does not change frequently!

DATA TYPES

Semi-Structured

JSON, XML, HTML, email messages, NoSQL

A combination of structured and unstructured data.

Typically, content is unstructured, but may contain metadata to help organize the data.

Fluid, but organizable by properties or metadata

This mix of data types will require a combination of discovery methods and tooling capable of discovery in these comingled data types

DATA LOCATION & DISCOVERABILITY

The location of data will impact both its discoverability and the choice of tools used to perform discovery.

Impact on tools and discoverability

Tools must be able to access data to perform the scanning and analysis needed in the discovery process.

May require different tools for cloud and on premises discovery

Not all cloud solutions may offer a local agent for on-premises.

Network-based DLP may not analyze all traffic between on-premises endpoints and cloud.

Including in-transit via e-mail

An optimal DLP approach will discover data in **on-premises** and **in cloud** repositories, as well as **in transit**!

The location of data will impact both its discoverability and the choice of tools used to perform discovery.

Impact on tools and discoverability

Tools must be able to scan unstructured data within structured datasources, such as relational databases.

EXAMPLE: Problem description inside a helpdesk ticket stored in a SQL database

Both unstructured and structured in same repository will increase tool cost and complexity and may present classification challenges.

If a single data classification label has to be placed on a large data source the most sensitive classification found will apply!

DATA DISCOVERY

Ensures data is appropriately classified for protection

Metadata-Based Discovery

A list of traits and characteristics about specific data elements or sets.

Often automatically created at the same time as the data.

Label-Based Discovery

Based on examining labels created by the data owners during the **Create** phase. or in bulk with a scanning tool

Can be used with databases (structured data) but is more commonly used with file data.

2. CLOUD DATA SECURITY

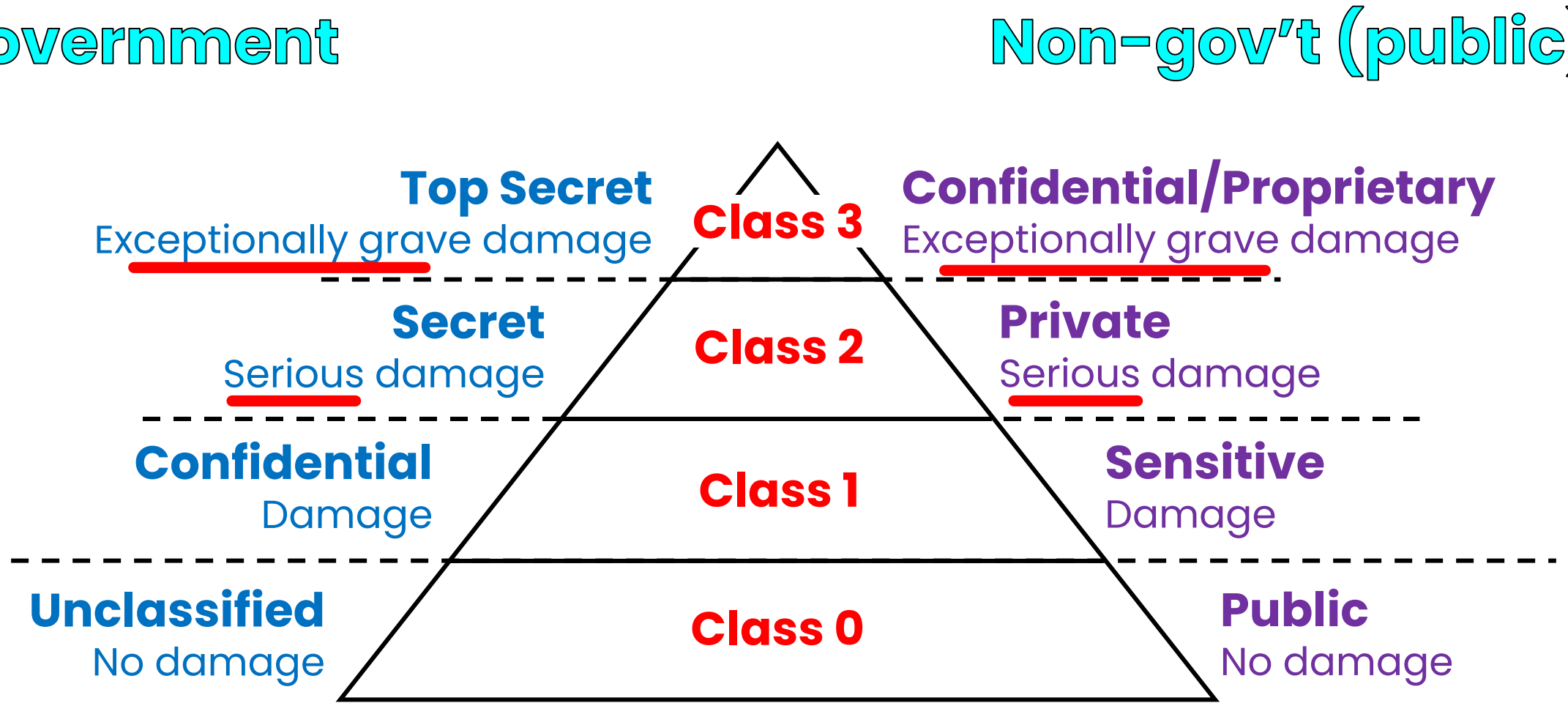
2.5 Implement Data Classification

Data Classification Policies

Data Mapping

Data Labeling

DOMAIN 2: DATA CLASSIFICATION



Non-government scenarios often called 'commercial' or 'public'

COMMON SENSITIVE DATA TYPES

Personally Identifiable Information (PII). any information that can identify an individual (name, SSN, birthdate/place, biometric records, etc)

Protected Health Information (PHI). health-related information that can be related to a specific person.

Regulated by HIPAA / HITRUST

Cardholder Data. allowable storage of information related to credit and debit cards and transactions.

Defined and regulated by PCI DSS

DATA POLICIES

Data classification

Labeling/tagging of data based on type, like personally identifiable info (PII), protected health info(PHI), etc.

Data retention

Ensures that legal and compliance issues are addressed.

Regulatory compliance

For legal and compliance reasons, you may need to keep certain data for different periods of time.

A driver of classification and retention

EXAMPLES:

Some financial data needs to be retained for 7 years

Some medical data may need to be retained up to 20-30 years.

DATA CLASSIFICATION

Data should be classified as soon after creation as possible!

A process for categorization of data and defining the appropriate controls. Categories include:

- Data type (format, structure)
- Jurisdiction and other legal constraints
- Ownership, Context
- Contractual or business constraints
- Trust levels and source of origin
- Value, sensitivity, and criticality
- Retention and preservation

DATA MAPPING AND LABELING

Mapping

Informs organization of the locations where data is present within applications and storage.

Brings understanding that enables implementation of security controls and classification polices.

Usually precedes classification and labeling

Labeling

Labeling requirements that apply consistent markings to sensitive data should accompany classification.

Often applied through classification policies, providing a target for data protection.

Often applied in bulk using classification tools

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

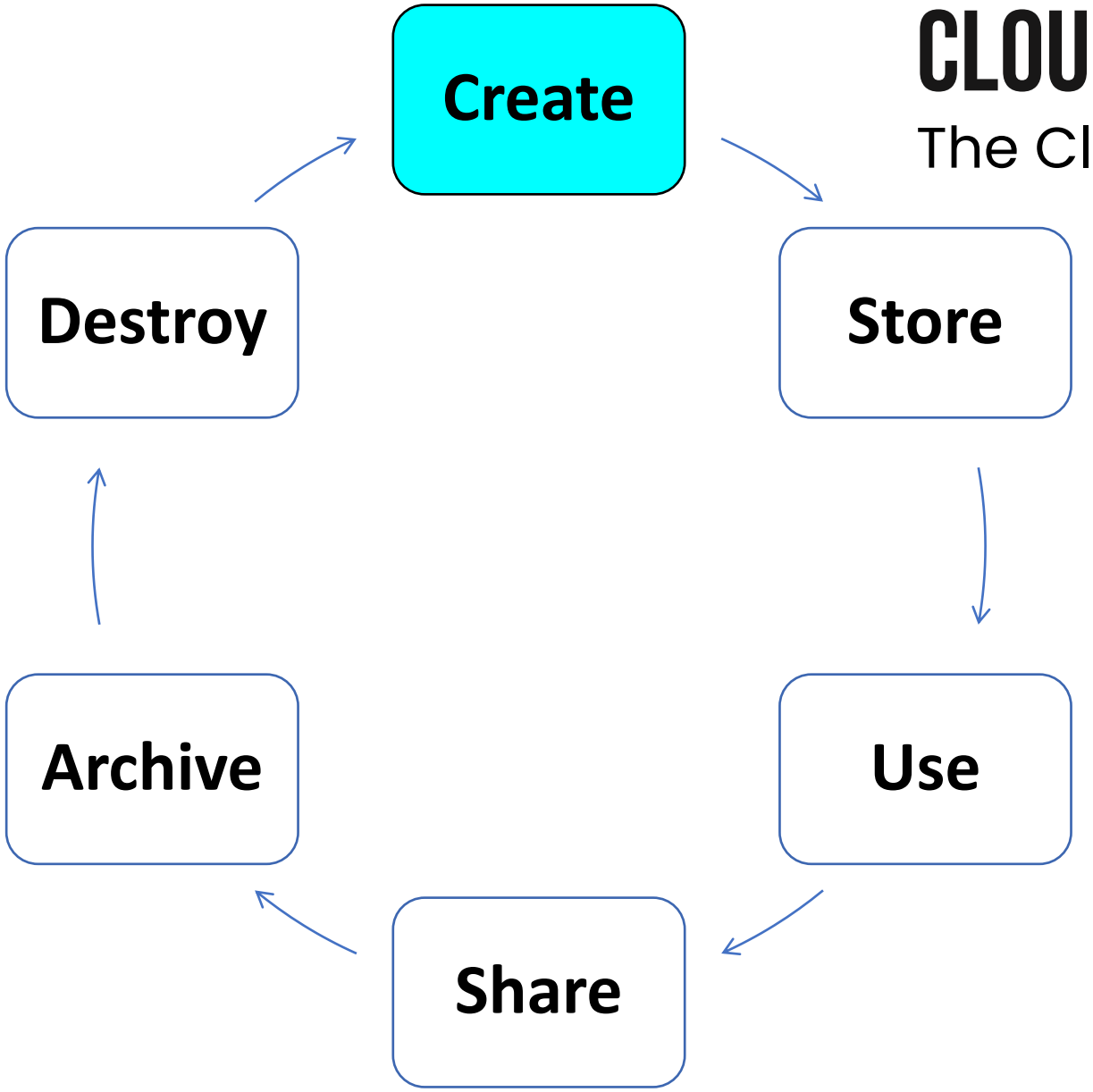
Data Discovery, Mapping, Labeling & Classification

EXAMPLE FOR CONTEXT:
Features will vary by CSP

INSIDE CLOUD AND SECURITY

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model



Can be created by **users**

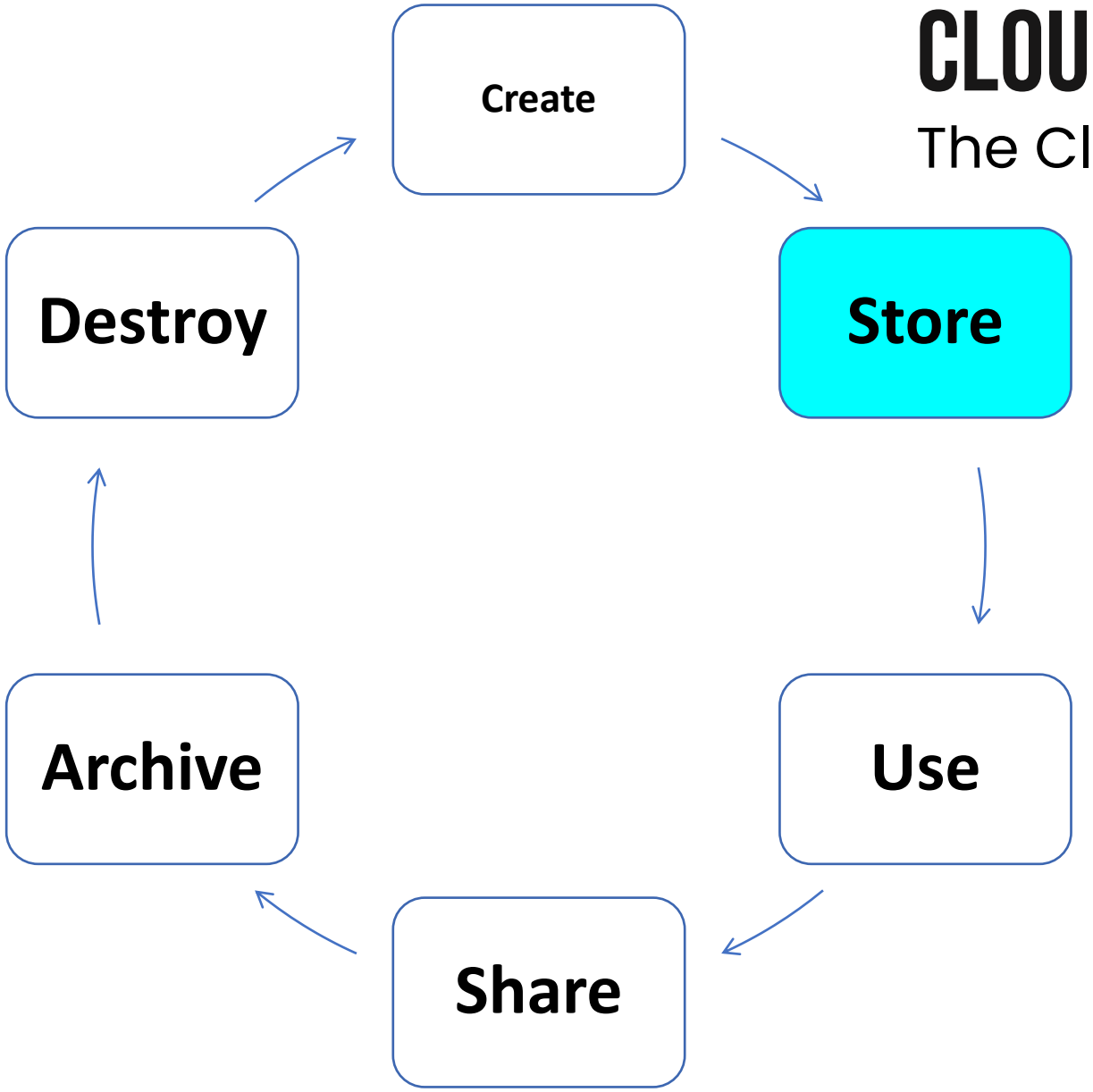
a user creates a file

Can be created by **systems**

a system logs access

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model

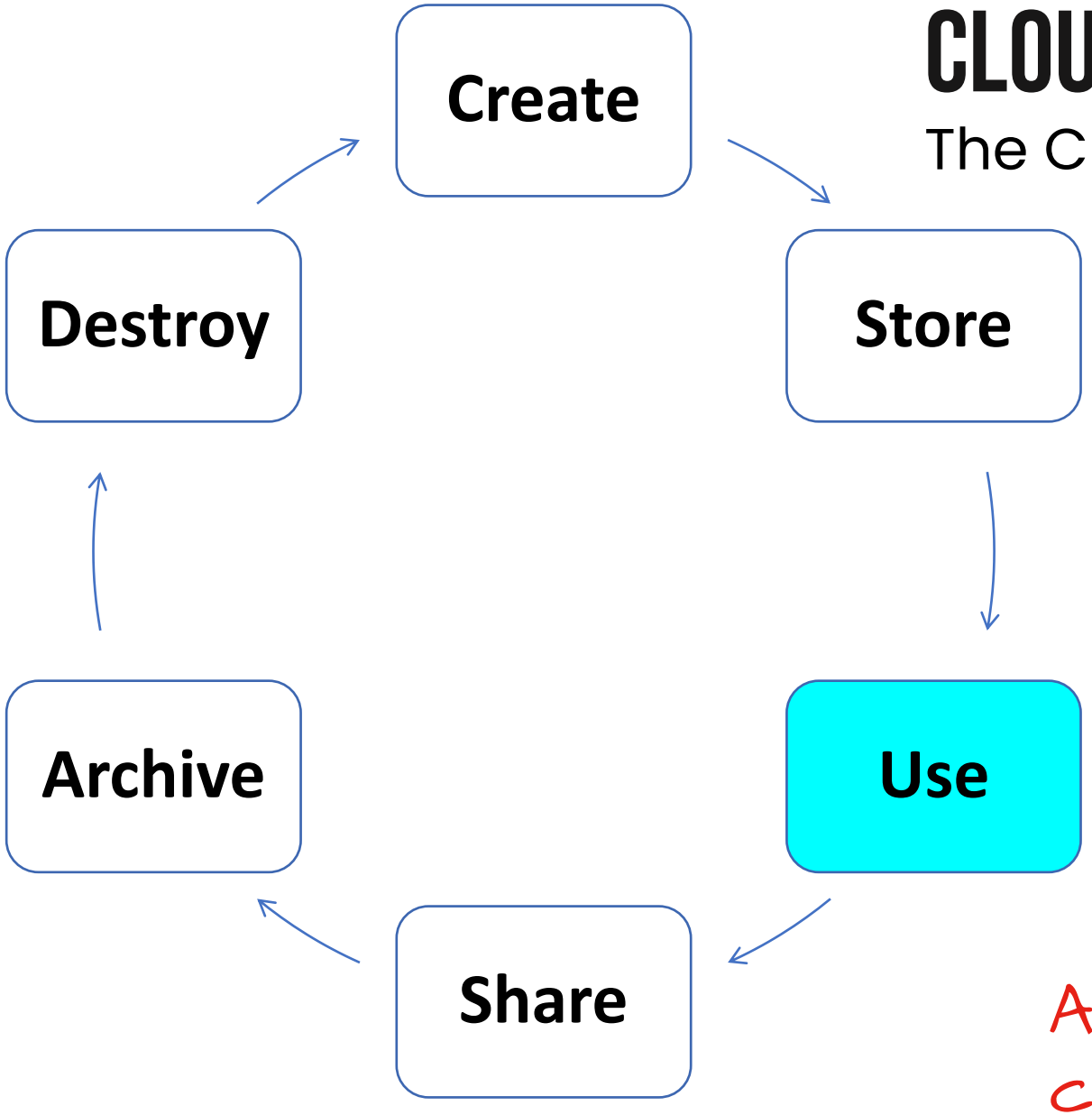


To ensure it's handled properly, it's important to ensure data is **classified** as soon as possible.

Ideally, data is encrypted at rest

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model

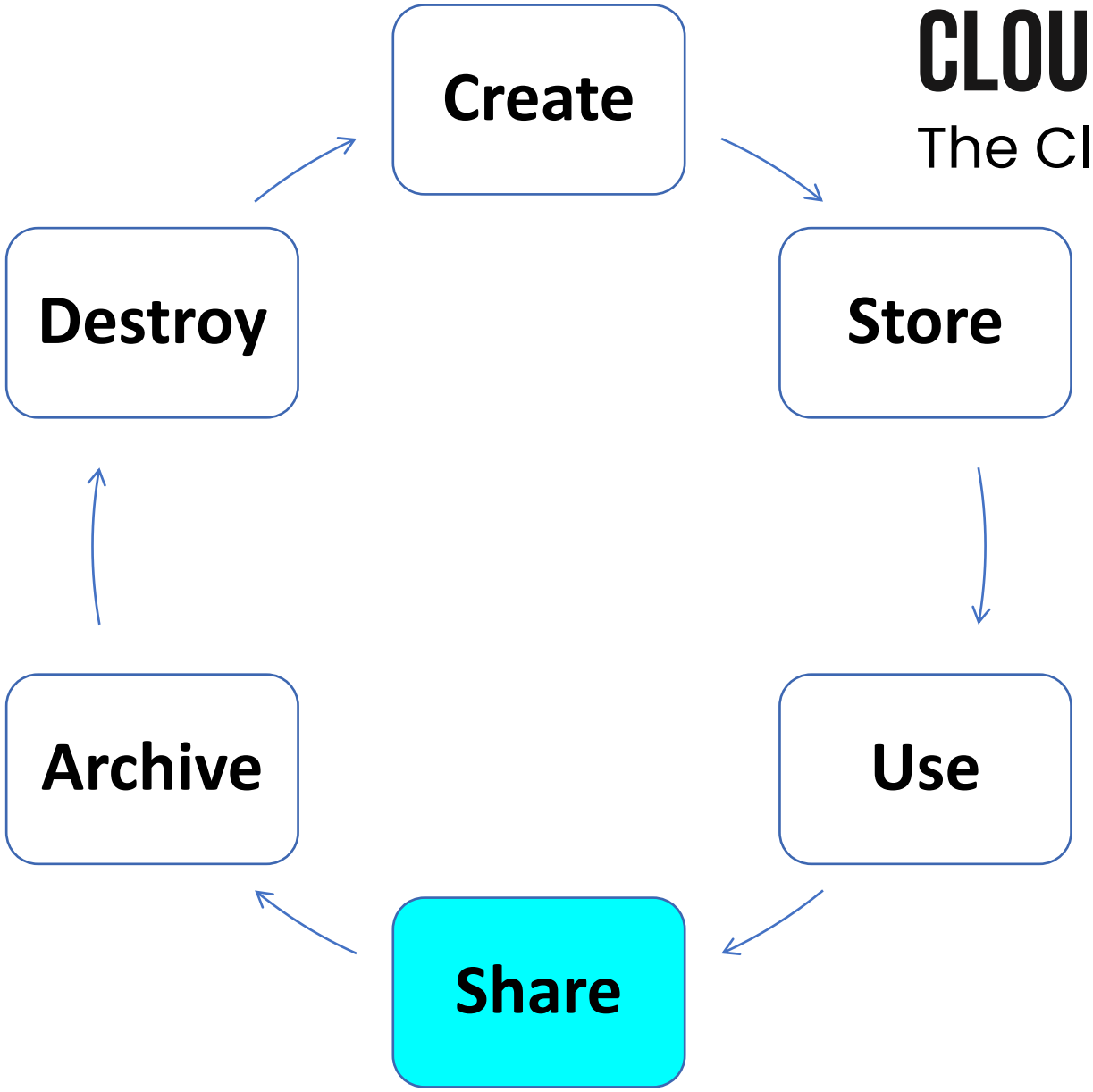


Data should be **protected** by adequate security controls based on its classification.

As data is used and modified, classifications may change!

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model



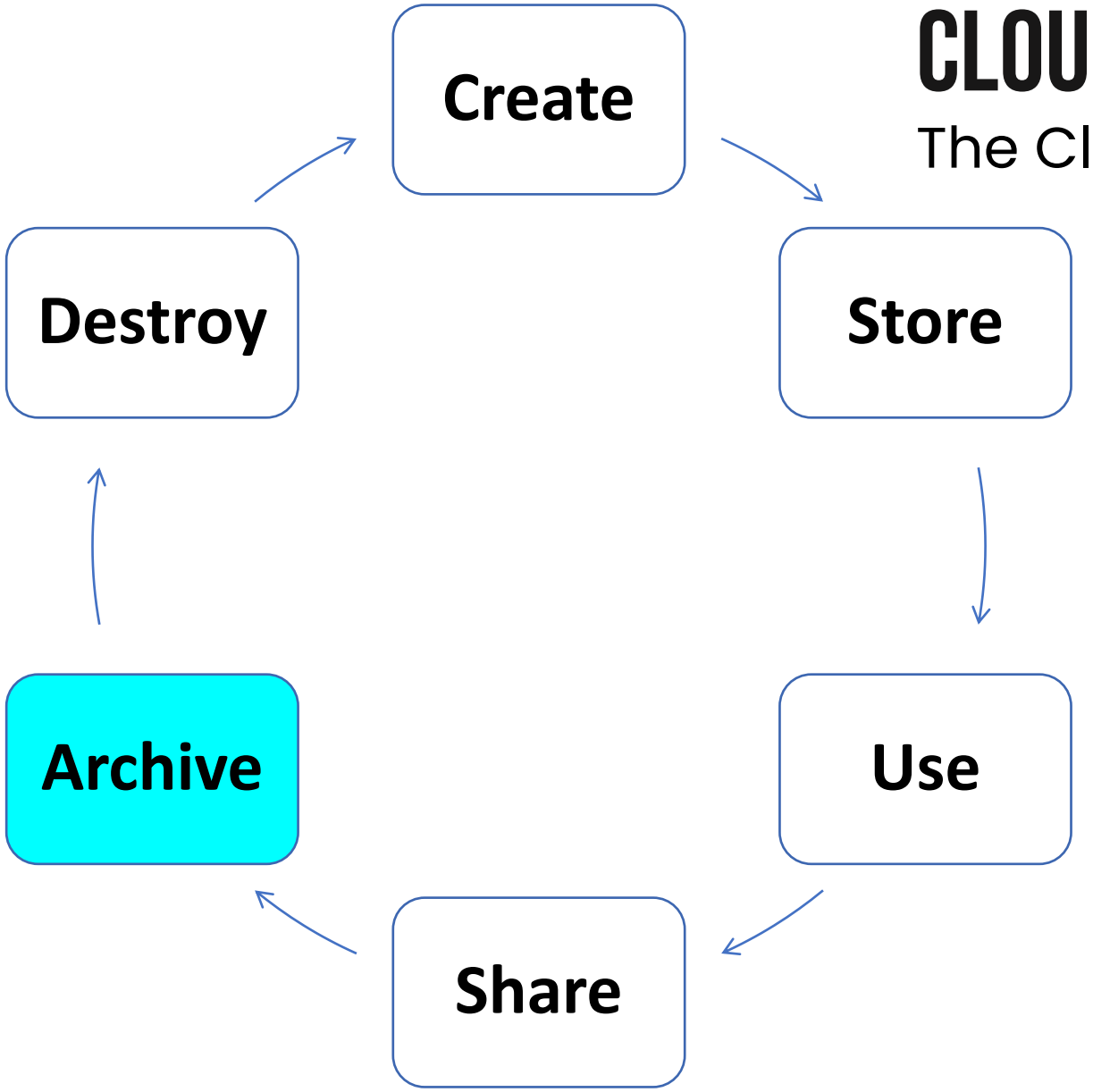
refers to anytime data is in use or in transit over a network

Classification dictates need for protection

Data protection policies may block external sharing

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model

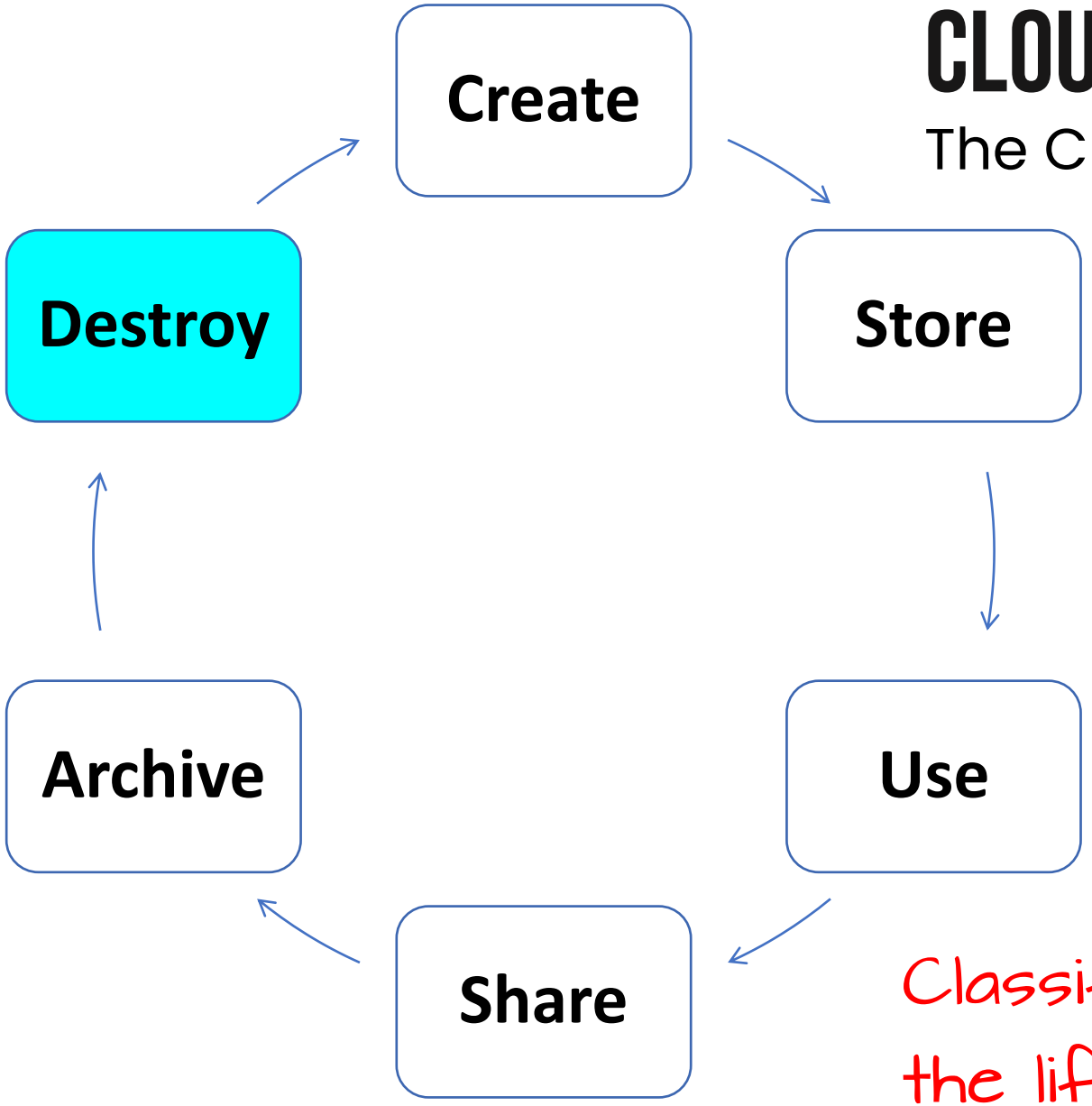


archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

Classification can drive data retention policies.

CLOUD SECURE DATA LIFECYCLE

The Cloud Security Alliance model



When data is no longer needed, it should be destroyed in such a way that it is not readable nor recoverable.

Classification drives the rest of the lifecycle, including destruction

2. CLOUD DATA SECURITY

2.6 Design and Implement Information Rights Management (IRM)

Objectives
(e.g., data rights, provisioning, access models)

Appropriate Tools
(e.g., issuing and revocation of certificates)

INFORMATION RIGHTS MANAGEMENT

IRM

Information Rights Management

IRM programs enforce data rights, provisioning access, and implementing access control models

Often implemented to control access to data designed to be shared but not freely distributed.

Can be used to block specific actions, like print, copy/paste, download, and sharing

Provide file expiration so that documents can no longer be viewed after a specified time

Always includes a cloud service, but may include a local agent

Many popular SaaS file sharing platforms implement these concepts as sharing options, which allow the document owner to specify which users can view, edit, download, share

Objectives of Info Rights Management

Persistence: access control/ability to enforce restrictions must follow the data.

Protection must follow the document or data wherever it travels

Dynamic policy control: IRM solution must provide a way to update the restrictions even after a document has been shared.

Expiration: IRM tools can enforce time-limited access to data as a form of access control.

Ability to expire/revoke access, require user check-in

Continuous audit trail: IRM solution must ensure that protected documents generate an audit trail when users interact with protected documents.

Required for accountability, non-repudiation

Interoperability: IRM solutions must offer support for users across these different system types.

Support for different OS, device types, and apps is important

Appropriate Tools

Local changes must never supersede controls implemented by the cloud service!

IRM tools comprise a variety of components necessary to provide policy enforcement and other attributes of the enforcement capability.

Centralized service for identity proofing and certificate issuance, store of revoked certificates, and for unauthorized identify information access.

Enables enforcement from anywhere

Secrets storage: IRM solutions require local storage for encryption keys, tokens, or digital certificates used to validate users and access authorizations.

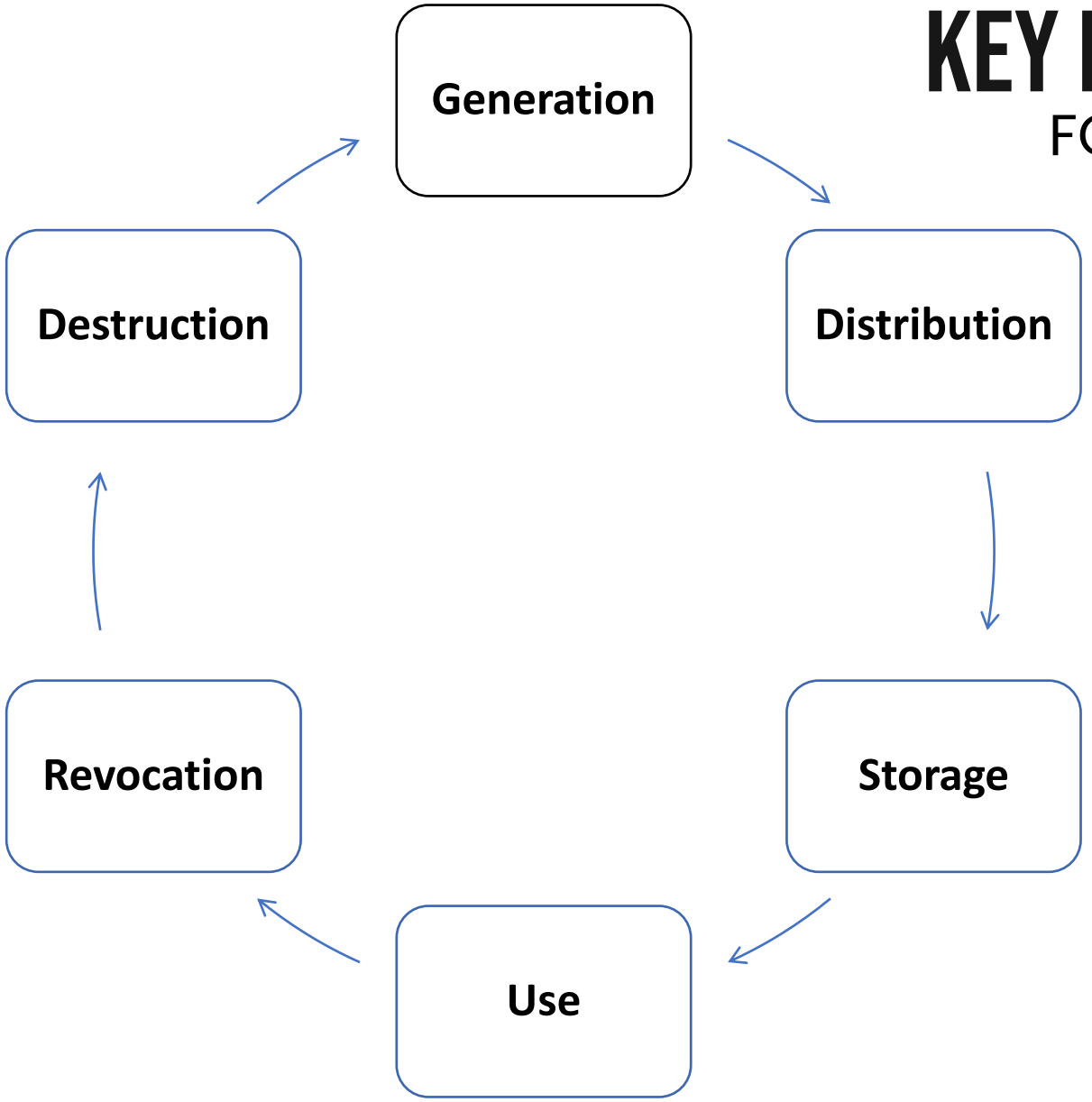
Local storage requires protection primarily for data integrity to prevent tampering with the material used to enforce IRM

Must prevent local modification of access controls and credentials.

Otherwise, a user might modify the permissions granted to extend their access beyond what the data owner originally specified

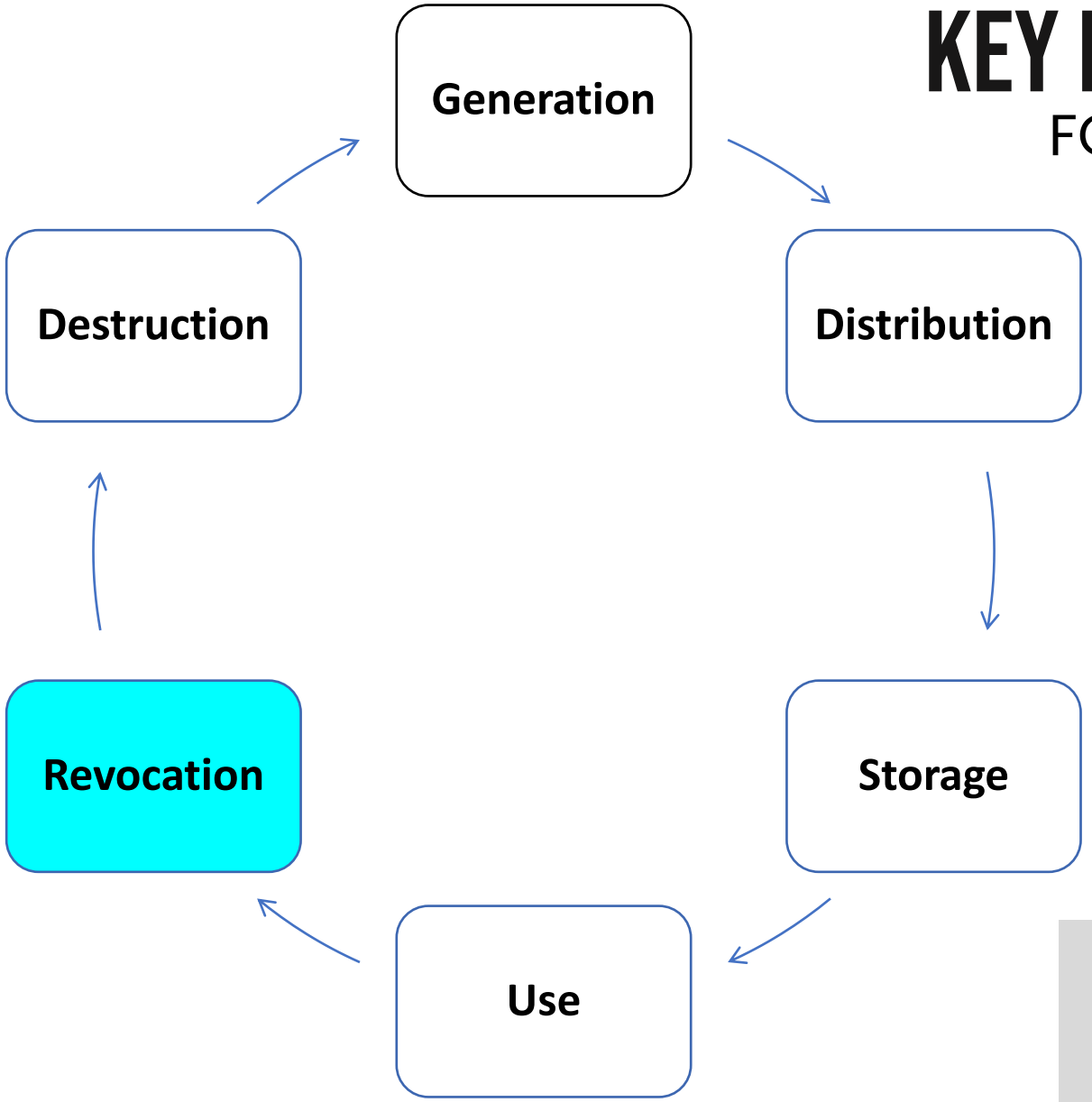
KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



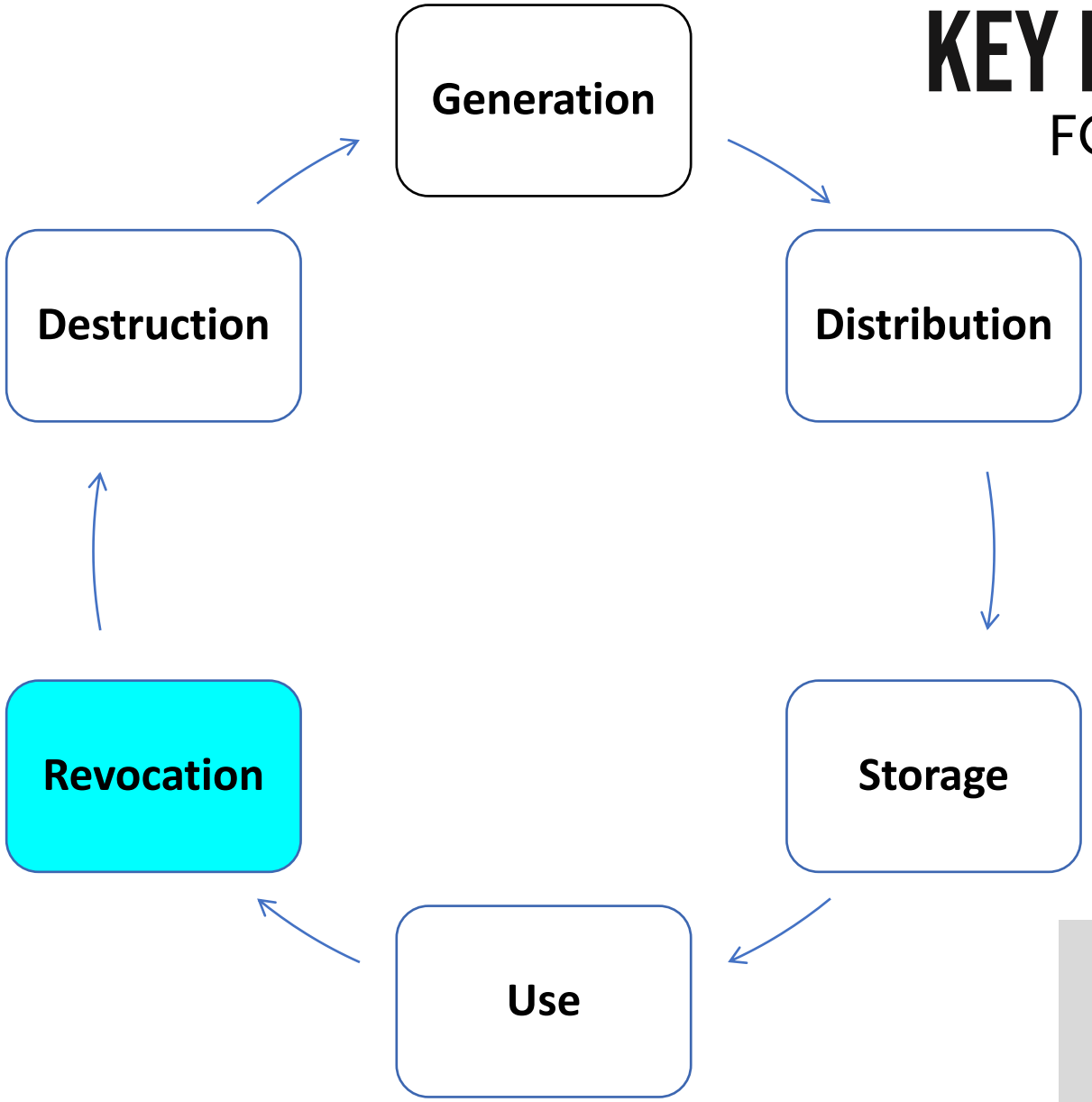
A process for revoking access at separation, policy breach, device or key compromise.

EXAMPLE:

In PKI, you would revoke the certificate on the issuing Certificate Authority (CA)

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



A process for revoking access at separation, policy breach, device or key compromise.

EXAMPLE:

The revocation would be recorded on the certificate revocation list (CRL).

Intellectual Property Protections

Trademarks. covers words, slogans, and logos used to identify a company and its products or services. Lasts 10 years, can be renewed

Patents. Patents protect the intellectual property rights of inventors.

Provides inventor exclusive use of their invention for a period of time, generally 20 years. Filing requires public disclosure

Trade Secrets. intellectual property of inventor that is absolutely critical to their business and must not be disclosed.

Valid as long as secrecy is maintained and not discovered by others

Copyright. is automatically granted to the creator of a work upon creation (but can be registered), prevents others from reusing.

Protection lasts 70 years beyond creators' death, then work moves into the public domain.

2. CLOUD DATA SECURITY

2.7 Plan and Implement Data Retention, Deletion and Archiving Policies

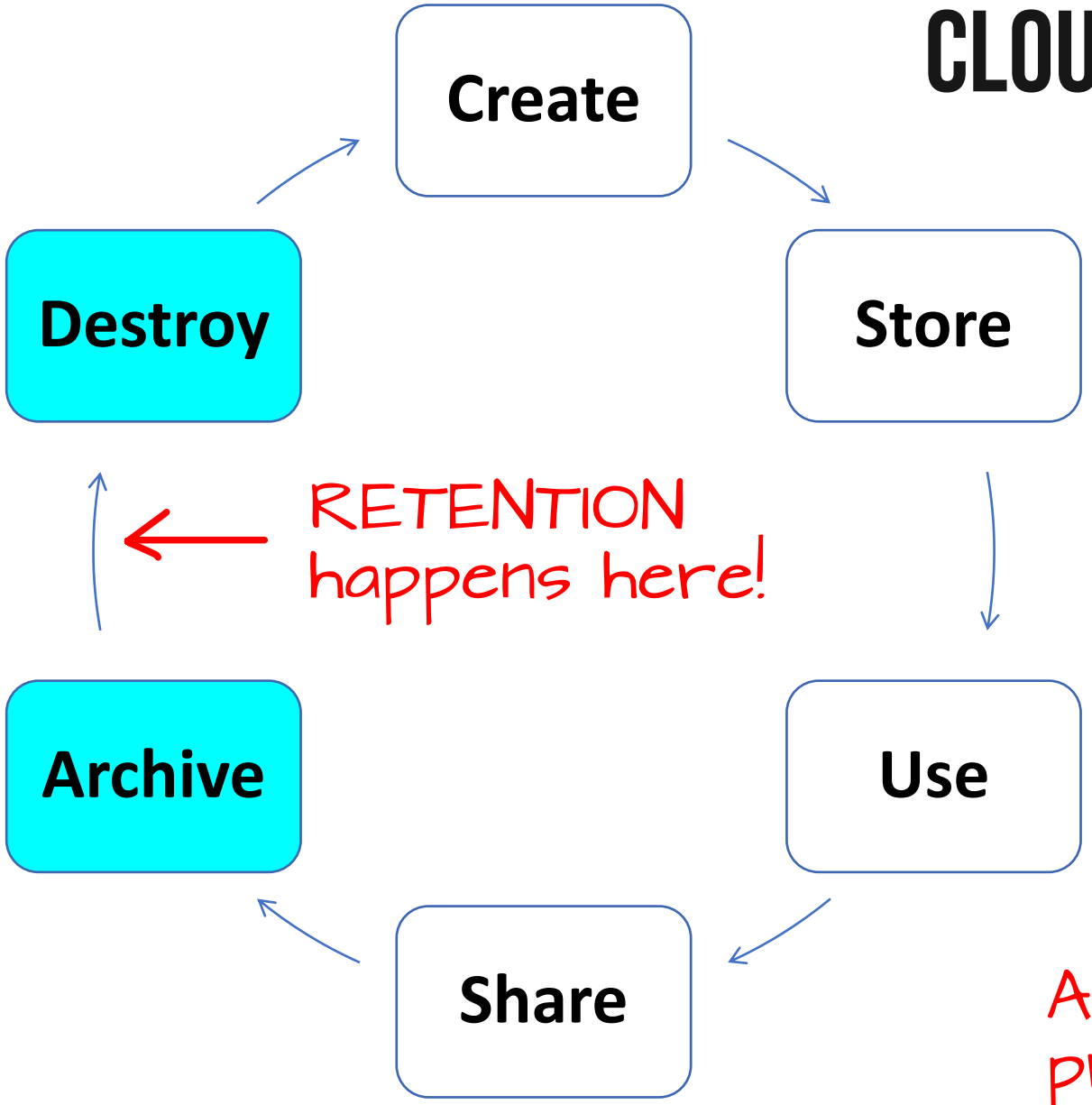
Data Retention Policies

Data Deletion Procedures and Mechanisms

Data Archiving Procedures and Mechanisms

Legal Hold

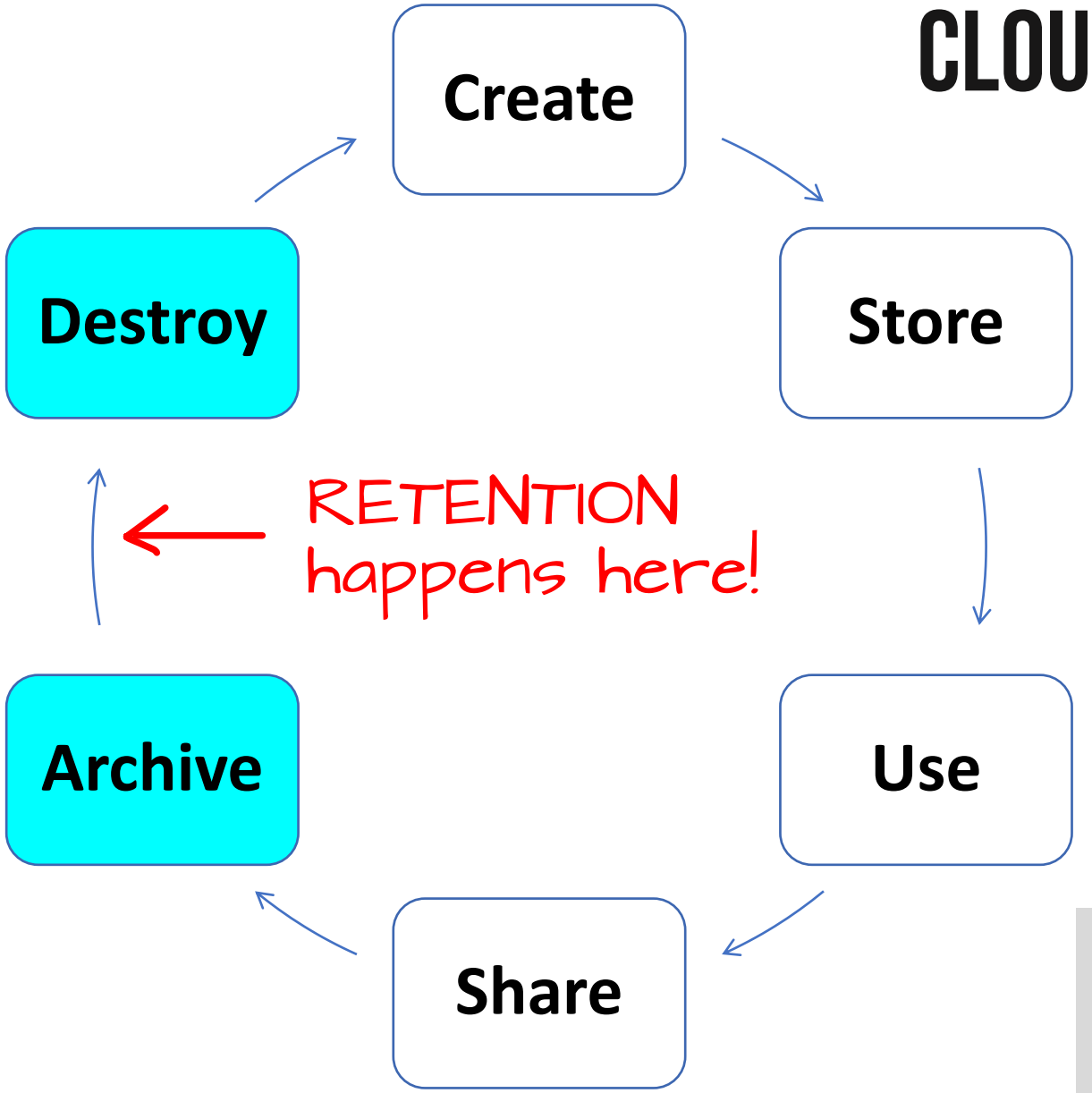
CLOUD SECURE DATA LIFECYCLE



Retention is driven by security policies and regulatory requirements

Audits or lawsuit may require production of some data

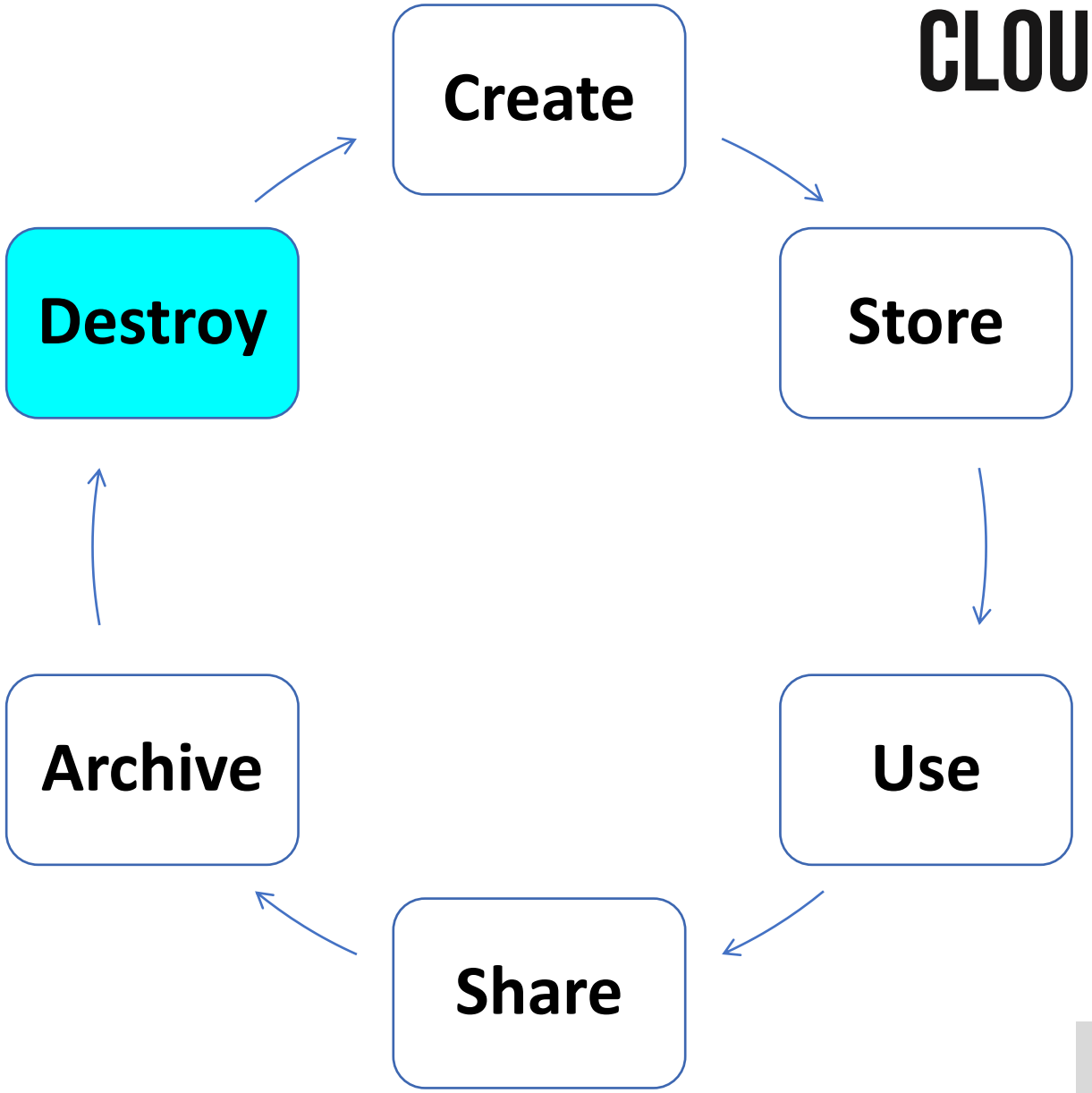
CLOUD SECURE DATA LIFECYCLE



Retention is driven by security policies and regulatory requirements

EXAMPLE: Sarbanes Oxley requires tax returns are kept for 7 years, and payroll and bank statements are forever!

CLOUD SECURE DATA LIFECYCLE

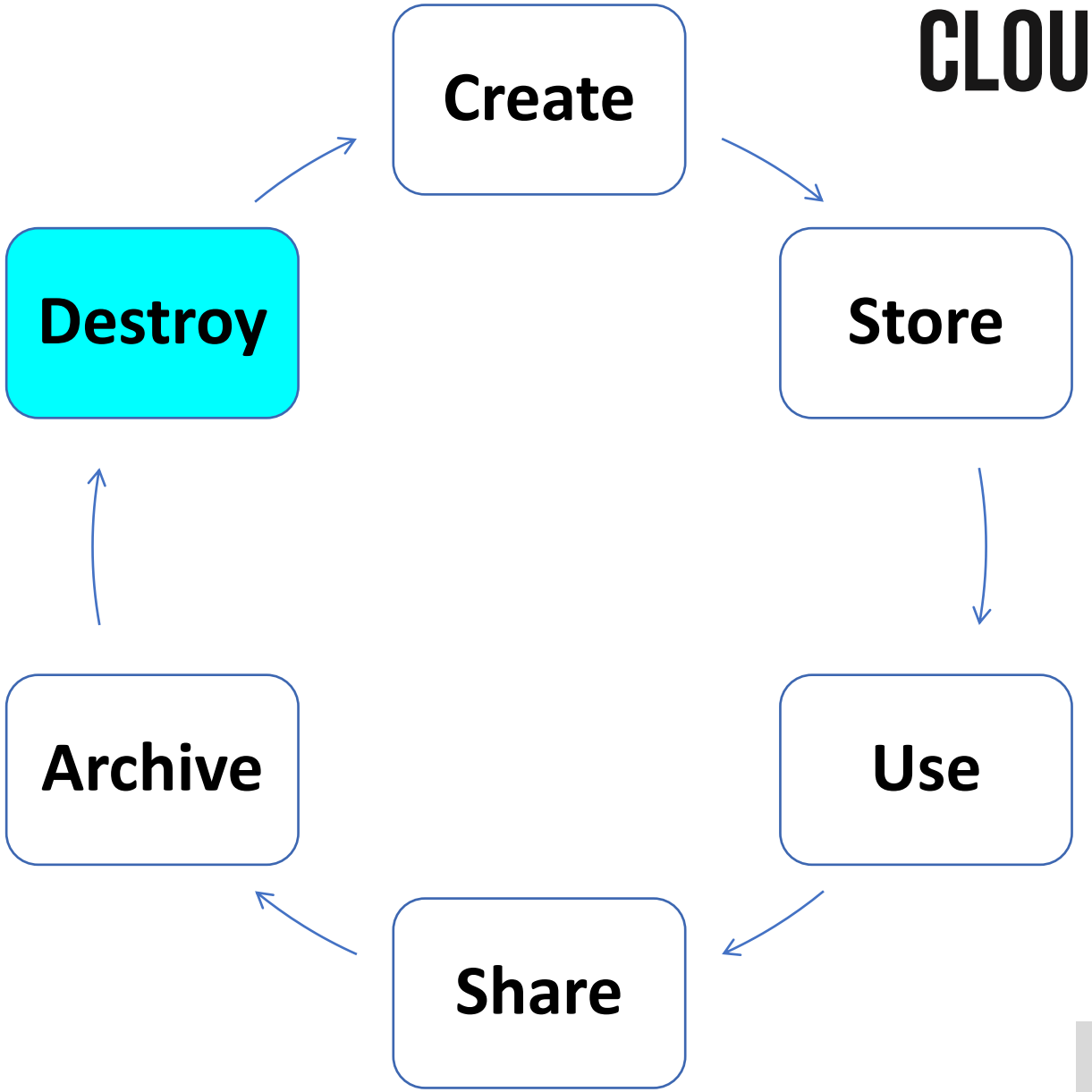


When data is no longer needed, it should be destroyed in such a way that it is not readable.

Keeping data longer then needed increases risk.

Companies know they cannot produce data they do not have for a legal case!

CLOUD SECURE DATA LIFECYCLE



When data is no longer needed, it should be destroyed in such a way that it is not readable.

Crypto-shredding (secure destruction) happens here!

Companies know they cannot produce data they do not have for a legal case!

More secure data destruction

Crypto-shredding "cryptographic erasure"

1. Data is encrypted with a strong encryption engine.
2. The keys used to encrypt the data are then encrypted using a different encryption engine.
3. Then, keys from the second round of encryption are destroyed.

PRO: Data cannot be recovered from any remnants.

CON: High CPU and performance overhead

If the exam poses questions on "secure data destruction", this is almost certainly the answer!

Data Archiving

Refers to placing data in long-term storage for a variety of purposes

The optimal approach in the cloud differs in several respects from the on-premises equivalent

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

Data Encryption

Encryption policy should consider which media is used, and data search and restoration needs, and regulatory obligations.

What threats should be mitigated by the encryption?

How will encryption keys be managed? Long-term archiving with encryption can present key management challenges.

Access controls and encryption are important to protect data integrity (by preventing unauthorized access)

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

Data Monitoring

Data stored in the cloud tends to be replicated as part of storage resiliency or BC/DR.

To maintain data governance, it is required that all data access and movements be tracked and logged.

Monitoring to ensure all security controls are being applied properly throughout the data lifecycle.

Accountability, traceability, auditability should be maintained

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

eDiscovery and Retrieval

Archive data may be subject to retrieval according to certain parameters such as dates, subjects, and authors.

The archiving platform should provide the ability to perform eDiscovery on the data to determine which data should be retrieved.

Ensures staff can manage the eDiscovery support burden

Data that is subject to more frequent search should be kept in a service that enables eDiscovery with a manageable level of effort.

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

Backup and DR Options

All requirements for data backup and restore should be specified and clearly documented

Business continuity and disaster recovery (BCDR) plans are updated and aligned with whatever procedures are implemented

Both resiliency to disaster (ensuring archive data availability) and knowledge/control of data replication are important

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

Data Format and Media Type

This is an important consideration because it may be kept for an extended period.

Format needs to be secure, accessible, and affordable.

Media type should support the other data archiving requirements, but physical media concerns fall to the CSP

AWS S3 and Azure Storage both offer cool tier (infrequent access) storage for low-cost archiving and immutability to ensure integrity

DATA ARCHIVING PROCEDURES AND MECHANISMS

Key elements of data archiving in the cloud

- Data Encryption
- Data Monitoring
- eDiscovery and Retrieval
- Backup and DR Options
- Data Format
- Media Type

Data Format and Media Type

This is an important consideration because it may be kept for an extended period.

Format needs to be secure, accessible, and affordable.

Media type should support the other data archiving requirements, but physical media concerns fall to the CSP

Often, cloud storage is billed by the GB, so cost is a factor!
However, it needs to be balanced with access needs

LEGAL HOLD

Legal Hold

aka "litigation hold"

Protecting any documents that can be used in evidence in legal proceedings from being altered or destroyed

Data protection suites in cloud platforms often have a feature to ensure immutability

Cloud storage (Azure Storage, AWS S3) offer an immutable storage feature

In data protection software, generally implements **permanent retention** until a human authorizes release

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Data Retention

EXAMPLE FOR CONTEXT:
Features will vary by CSP

INSIDE CLOUD AND SECURITY

2. CLOUD DATA SECURITY

2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

Definition of Event Sources and Requirement of Event Attributes
(e.g., identity, Internet Protocol (IP) address, geolocation)

Logging, Storage and Analysis of Data Events

Chain of Custody and Non-Repudiation

MAINTAINING ACCOUNTABILITY

Accountability

is maintained for individual subjects using auditing.

logs record user activities and users can be held accountable for their logged actions.

directly promotes good user behavior and compliance with the organization's security policy.

SECURITY AUDITS AND REVIEWS

Security audits and reviews

help ensure that management programs are effective and being followed.

commonly associated with account management practices to prevent violations with least privilege or need-to-know principles.

can also be performed to oversee many programs and processes

- patch management
- vulnerability management
- change management
- configuration management

EVENT SOURCES & EVENT ATTRIBUTES

Auditability, **Traceability**, and **Accountability** of Data Events

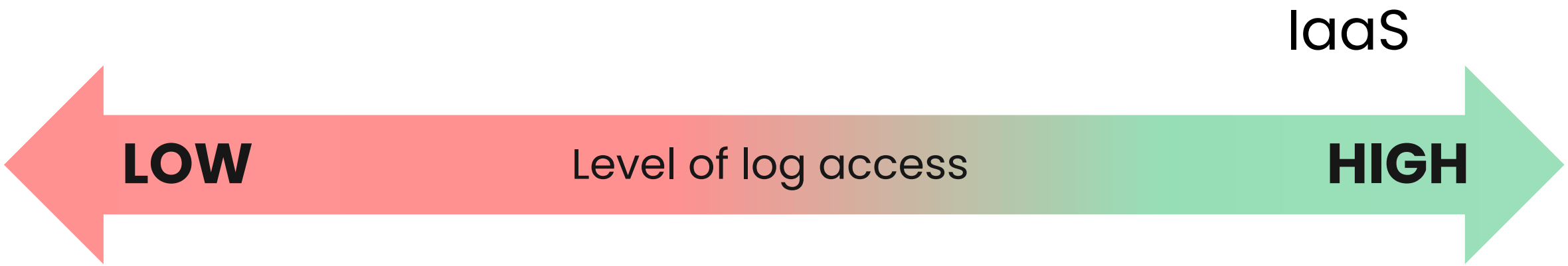
OWASP provides a comprehensive set of definitions and guidelines for identifying, labeling, and collecting data events

Ensures events are useful and pertinent to applications and security, whether in a cloud or traditional data center

Definition of Event Sources

Which events are important and available for capture will vary based on cloud service model employed (**IaaS**, **PaaS**, or **SaaS**)

EVENT SOURCES & EVENT ATTRIBUTES



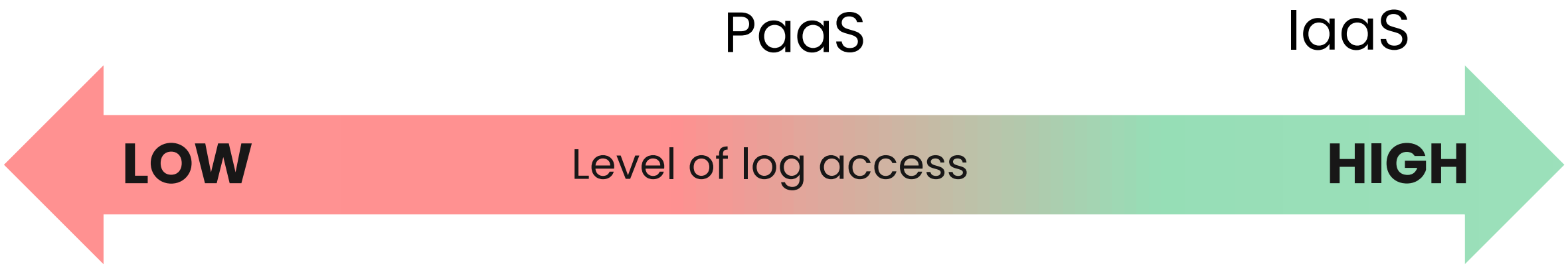
IaaS Event Sources

Within an IaaS environment, the cloud customer has the most access and visibility into system and infrastructure logs of any cloud service model.

Because the cloud customer has nearly full control over their compute environment, including system and network capabilities, virtually all logs and data events should be exposed and available for capture.

This is because the customer has more responsibility than in any other cloud model (see "Shared Responsibility Model" in Domain 1)

EVENT SOURCES & EVENT ATTRIBUTES



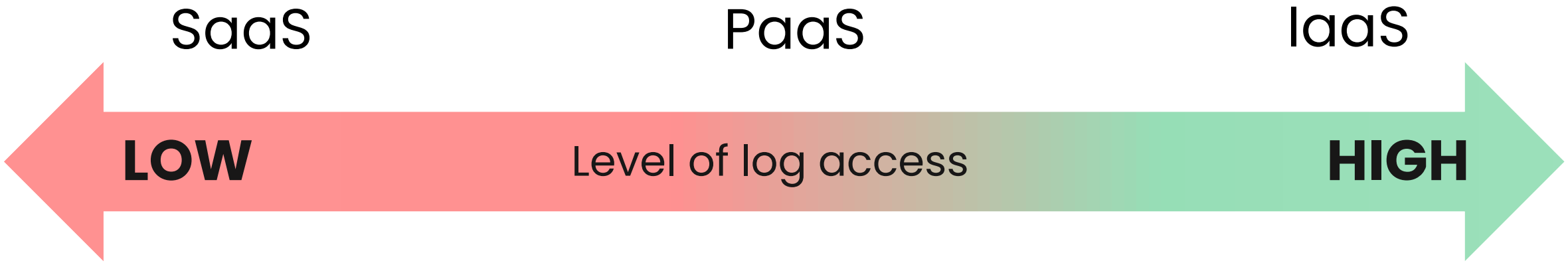
PaaS Event Sources

A PaaS environment does not offer or expose the same level of customer access to infrastructure and system logs as IaaS

However, the same level of detail of logs and events is available at the application level.

Responsibility for system and infrastructure in PaaS belongs to the cloud service provider (CSP)

EVENT SOURCES & EVENT ATTRIBUTES



SaaS Event Sources

Because in a SaaS environment the cloud service provider is responsible for the entire infrastructure and application, the amount of log data available to the cloud customer is less.

Customer responsibility is limited to access control, shared responsibility for data recovery, and feature configuration

Service responsibility equates to log visibility

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from OWASP:

Ultimately, logs should be able to answer the question:

"Who did what and when?"

Sufficient user ID attribution should be accessible, or it may be impossible to determine who performed a specific action at a specific time. This is called **identity attribution**.

This is a necessity for non-repudiation!

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

Ultimately, logs should be able to answer the question:

"Who did what, when, and from where?"

Sufficient user ID attribution should be accessible, or it may be impossible to determine who performed a specific action as a specific time. This is called **identity attribution**.

This is a necessity for non-repudiation!

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

WHO

- **Source address**
- **User identity** (*if known*)

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

WHAT

- **Type of event**
- **Severity of event**
- **Security-relevant event flag**
  (*if log contains non-security events*)
- **Description**

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

WHERE

- **Application identifier** (*name, version, etc.*)
- **Application address**
- **Service**
- **Geolocation**
- **Window/for/page** (*URL and HTTP method*)
- **Code location** (*script or module name*)

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

WHEN

- **Log date and time** (*international format*)
- **Event date and time**
- **Interaction identifier**

EVENT SOURCES & EVENT ATTRIBUTES

The **WHO**, **WHAT**, **WHERE**, and **WHEN** of logging from to OWASP:

OWASP maintains concentrated guidance for developers on building application logging mechanisms, especially related to security logging in the **OWASP Logging Cheat Sheets**

https://github.com/OWASP/CheatSheetSeries

Browse to the **/cheatsheets** folder and click on **Logging_Cheat_Sheet.md**

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Logs are worthless if you do nothing with the log data. They are made valuable only by **review**.

That is, they are valuable only if the organization makes use of them to identify activity that is unauthorized or compromising.

SIEM (Security Information Event Monitoring) tools can help to solve some of these problems by offering these key features:

- Log centralization and aggregation
- Data integrity
- Normalization
- Automated or continuous monitoring
- Alerting
- Investigative monitoring

We will cover SIEM in depth in Domain 5

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Log centralization and aggregation

Rather than leaving log data scattered around the environment on various hosts, the SIEM platform can gather logs from a variety of sources, including:

operating systems, applications, network appliances, user devices, providing a single location to support investigations.

Data integrity

The SIEM should be on a separate host with its own access control, preventing any single user from tampering.

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Normalization

SIEMs can normalize incoming data to ensure that the data from a variety of sources is presented consistently.

Automated or continuous monitoring

Sometimes referred to as correlation, SIEMs use algorithms to evaluate data and identify potential attacks or compromises.

Alerting

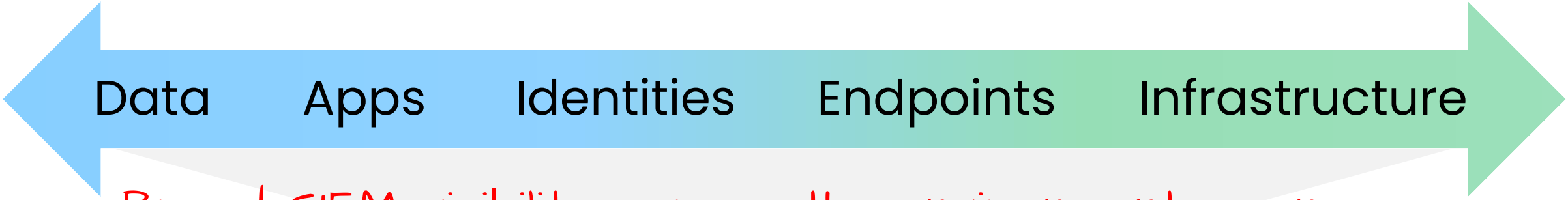
SIEMs can automatically generate alerts such as emails or tickets when action is required based on analysis of incoming log data

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Investigative monitoring

When manual investigation is required, the SIEM should provide support capabilities such as querying log files, generating reports.



Broad SIEM visibility across the environment means better context in log searches, & security investigations

SIEM

CHAIN OF CUSTODY

Tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle

Functions and importance of chain of custody?

Provides evidence integrity through convincing proof evidence was not tampered with in a way that damages its reliability.

Documents key elements of evidence movement and handling, including:

- Each person who handled the evidence
- Date and time of movement/transfer
- Purpose evidence movement/transfer

What if evidence is left unattended or handled by unauthorized parties?

Then, criminal defendants can claim the data was altered in a way that incriminates them, and thus the evidence is no longer reliable.

Foundational principle of evidence handling in legal proceedings!

NON-REPUDIATION

Non-repudiation is **the guarantee that no one can deny a transaction.**

Methods to provide non-repudiation

Systems enforce nonrepudiation through the inclusion of sufficient evidence in **log files**, including unique user identification and timestamps.

Digital Signatures prove that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed.

Based on asymmetric cryptography (a public/private key pair)

It's the digital equivalent of a handwritten signature or stamped seal.

Multiple accounts make non-repudiation more difficult

Shared accounts make non-repudiation virtually impossible!

THANKS

FOR WATCHING!