Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 02: Asset Security

Learning Objectives

By the end of this lesson, you will be able to:

- Define and explain the privacy terms
- Describe data classification considerations and procedure
- Describe the information classification criteria and objectives
- List information levels, government, and private sector
- Explain data lifecycle, data management, data roles
- Discuss data remanence data security controls
- Define baselining, scoping, and tailoring
- Explain data loss prevention

Introduction to Asset Security

Importance of Asset Security

Recently, a hacker broke into one of the Nutri Worldwide servers by taking advantage of an application vulnerability. The server had various types of information at different levels of criticality.

The information on the server was secured with appropriate security controls. Although the hacker was able to gain access only to the information with a lower level of protection, the breach had a huge impact on the organization. It was later found that there was a flaw in the classification process, leaving even sensitive information with very little protection.

Privacy Terms

Privacy

- Information privacy is the privacy of personal information, and it usually relates to the personal data stored on computers.
- Information privacy is applicable to a collection of personal information, such as medical records, financial data, criminal records, political records, business-related information, or website data .
- Information privacy is also known as data privacy.

Privacy Terms

PII or Personally Identifiable Information

- PII is data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and for de-anonymizing data can be considered **PII.**

Privacy Terms

Protected Health Information

- Protected health information (PHI) is any health-related information that can be related to a specific person.
- In the United States, the Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of PHI.

Proprietary Data

Proprietary Data

- Proprietary data refers to any data that helps an organization maintain a competitive edge.
- It could be a software code developed, technical plans for products, internal processes, intellectual property, or trade secrets.

Data Policy

Data Policy

- A high-level document created by senior management that defines strategic long-term goals for data management throughout the organization
- Guides the framework for data management and addresses issues related to data access, legal matters, custodian duties, data acquisition, data handling, and other issues
- Should be dynamic and flexible

Data Policy

The elements to be considered during data policy creation are:

- Data privacy
- Ownership of data
- Cost
- Sensitivity and criticality of data
- Policies and processes
- Laws and regulations
- Liability

Data Quality

Quality as applied to data, has been defined as a fitness of data to serve its purpose in a given context.

The quality of data is determined by factors such as accuracy, completeness, reliability, relevance, and how up-to-date it is.

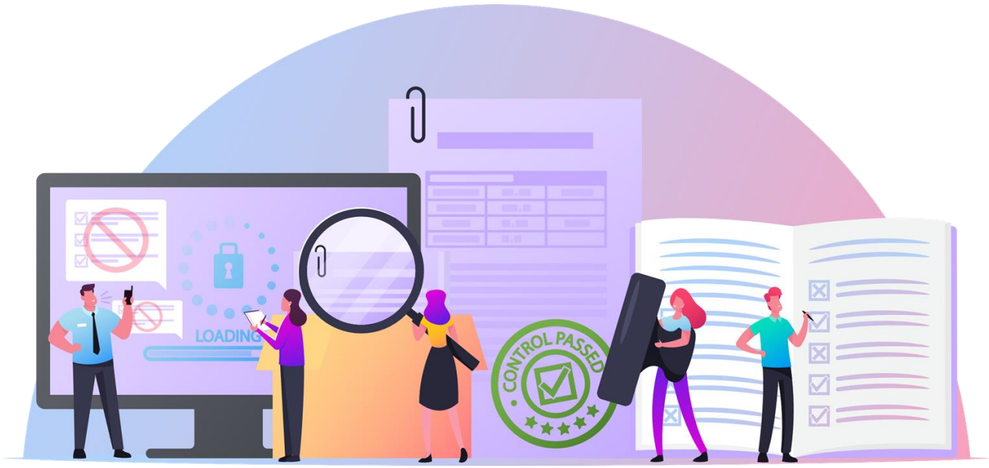
Data Quality

The applicability and use of data is greatly reduced if the data quality is lost.

Data Quality

Data quality principles apply at all stages of the data management process:

- Data collection or capturing
- Recording
- Identification
- Metadata recording
- Storage and archiving of data
- Presentation and dissemination of data
- Analysis and manipulation of data



Definitions

Sensitivity

A measure of the impact that improper disclosure of information may have on an organization

Criticality

A measure of the impact that the failure of a system, to function as required will have on the on the organization.

Real World Scenario

University of Delaware has defined the following three categories to understand how critical data is:

How critical is the data?	What could go wrong?
Non-critical	• Non-critical data is necessary for the University's ability to operate. • Loss of integrity or availability would only have **little to no short-term impact** on business continuity or operational effectiveness. • Some services or functions may be slightly delayed or degraded if non-critical data loses integrity or availability.

Information source: https://www1.udel.edu/security/data/criticality.html

Real World Scenario

University of Delaware has defined the following three categories to understand how critical data is:

How critical is the data?	What could go wrong?
Critical	• Critical data is important for the University's ability to operate. • Loss of integrity or availability would have **moderate short-term impact** on business continuity or operational effectiveness. • Key services or functions may be noticeably and disruptively delayed or degraded if critical data loses integrity or availability.

Information source: https://www1.udel.edu/security/data/criticality.html

Real World Scenario

University of Delaware has defined the following three categories to understand how critical data is:

How critical is the data?	What could go wrong?
Mission critical	• Mission critical data is vital for the University's ability to operate. • Loss of integrity or availability would have **significant short-term impact** and **possible long-term impact** on business continuity or operational effectiveness. • Key services or functions may be severely delayed, degraded, or may become impossible to deliver. • Prolonged loss of mission critical data may threaten the University's ability to recover.

Information source: https://www1.udel.edu/security/data/criticality.html

Identify and Classify Information and Assets

Asset Classification

Asset definition

An asset is any resource that has value to an organization.

An asset can be tangible or intangible. This includes people, hardware, software, data, information, or reputation.

Asset Classification

Asset classification

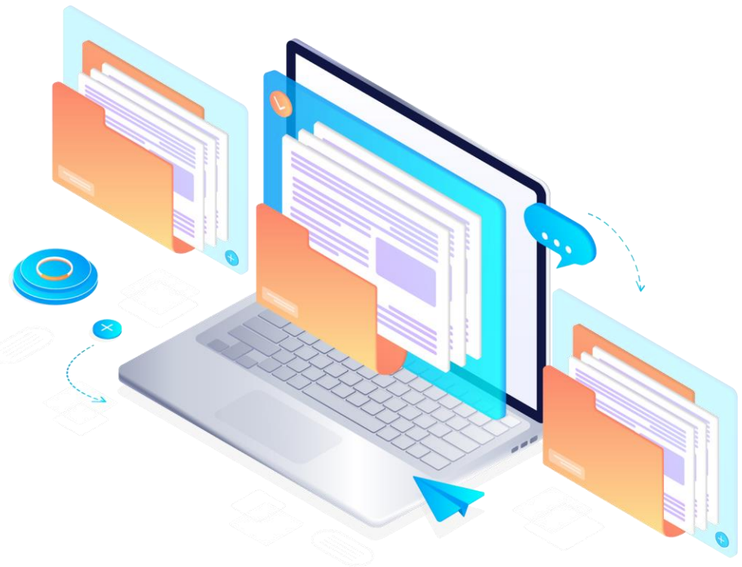
Asset classification means categorizing and grouping assets based on its business value.

- The first step in the classification process is to prepare an inventory of assets and determine the responsible asset owners.
- The levels of classification dictate a minimum set of security controls the organization will use to protect the asset.

Data Classification: Definition

Data Classification

Data classification can be defined as the process of assigning an appropriate level of classification to a data asset to ensure it receives an adequate level of protection.



Data Classification

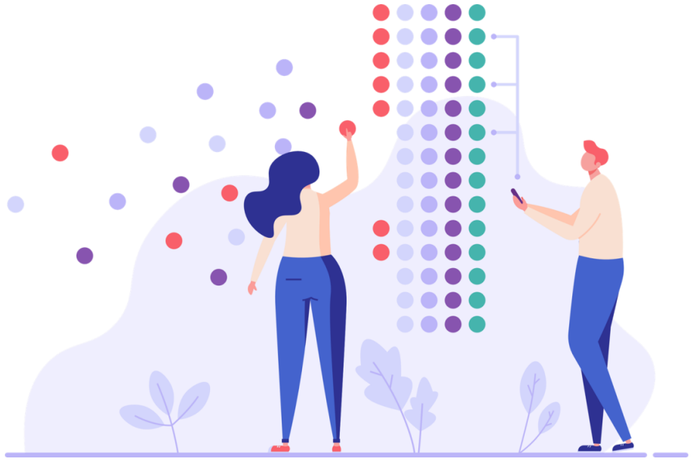
Characteristics of Data Classification

- The classification level should always be attached throughout the lifecycle of the information.
- It identifies the value of the data to the organization.
- It is an ongoing process and not one-time effort.

Need for Data Classification

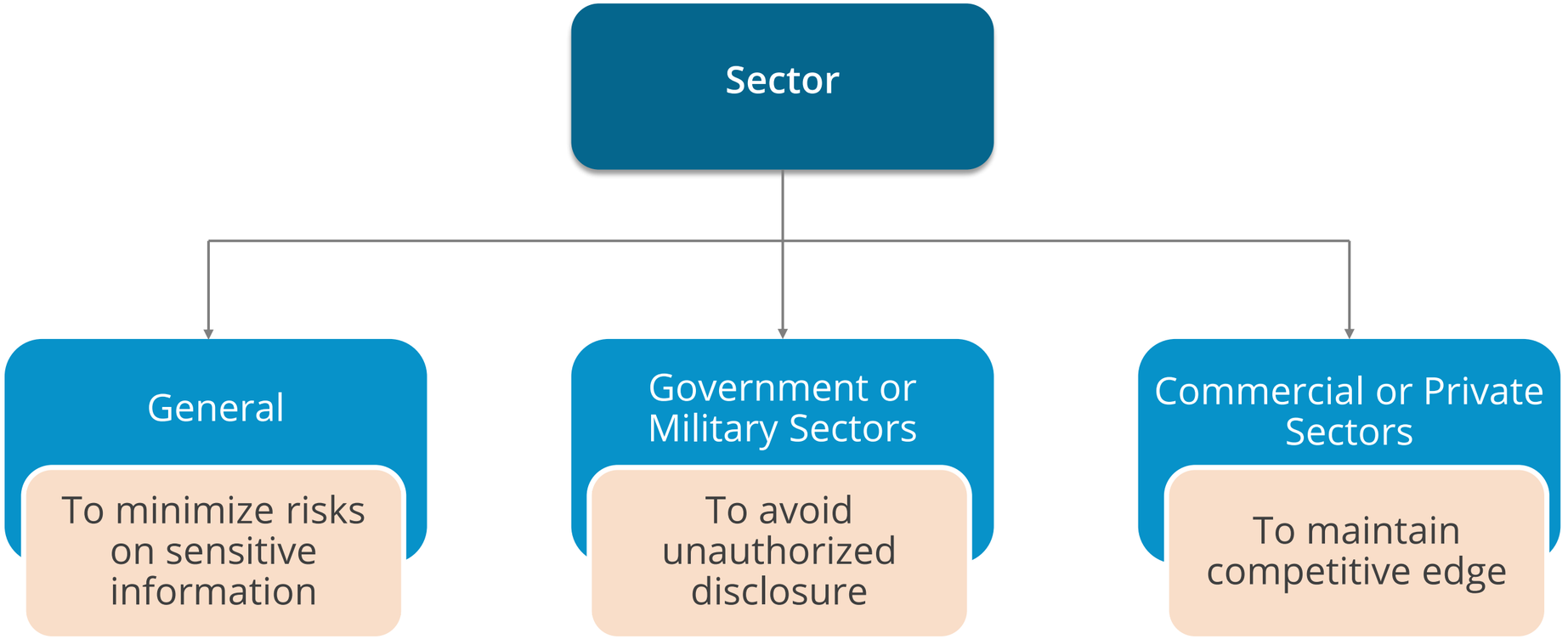
Why do we need classification?

- Some data is valuable to the people who take strategic decisions.
- Data loss could create a significant problem to the enterprise.
- Information classification enhances confidentiality, integrity, and availability.
- It focuses on proper implementation of controls depending on the sensitivity of information.
- It standardizes type of information and protection requirements.
- It helps to achieve efficient cost-to-benefit ratio.



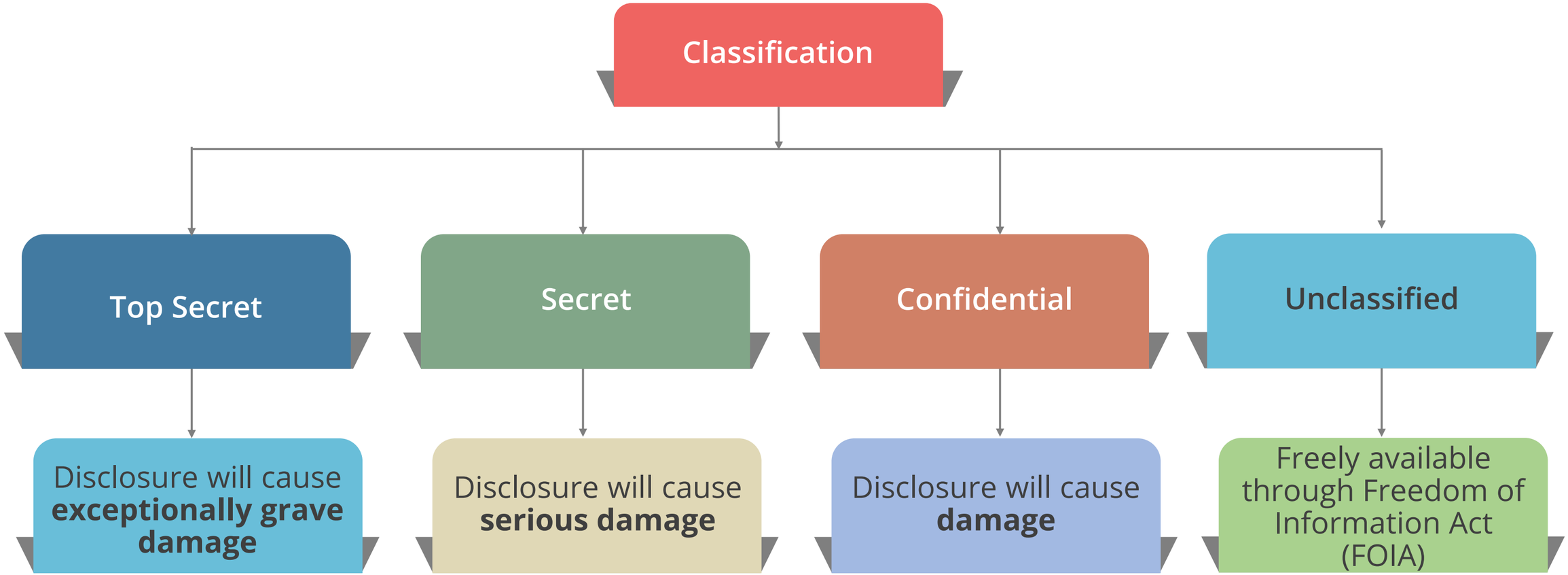
Information Classification Objectives

The objective of an information classification scheme varies from sector to sector. The following infographic shows objectives of each sector:



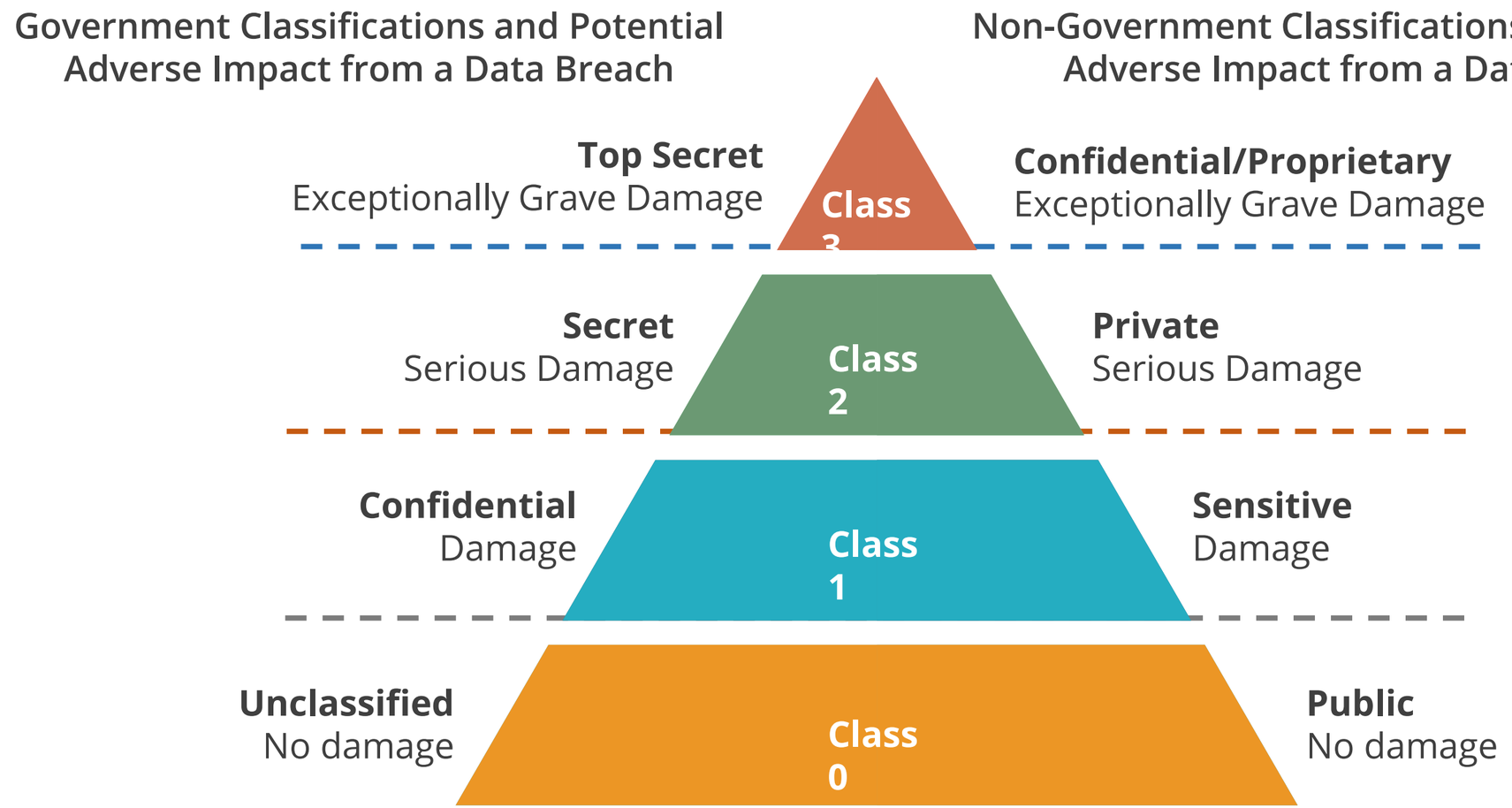
Information Classification: Government Sector

The following chart shows different classifications of Government sector and potential damage incase of a data disclosure:



Information Classification: Government Sector

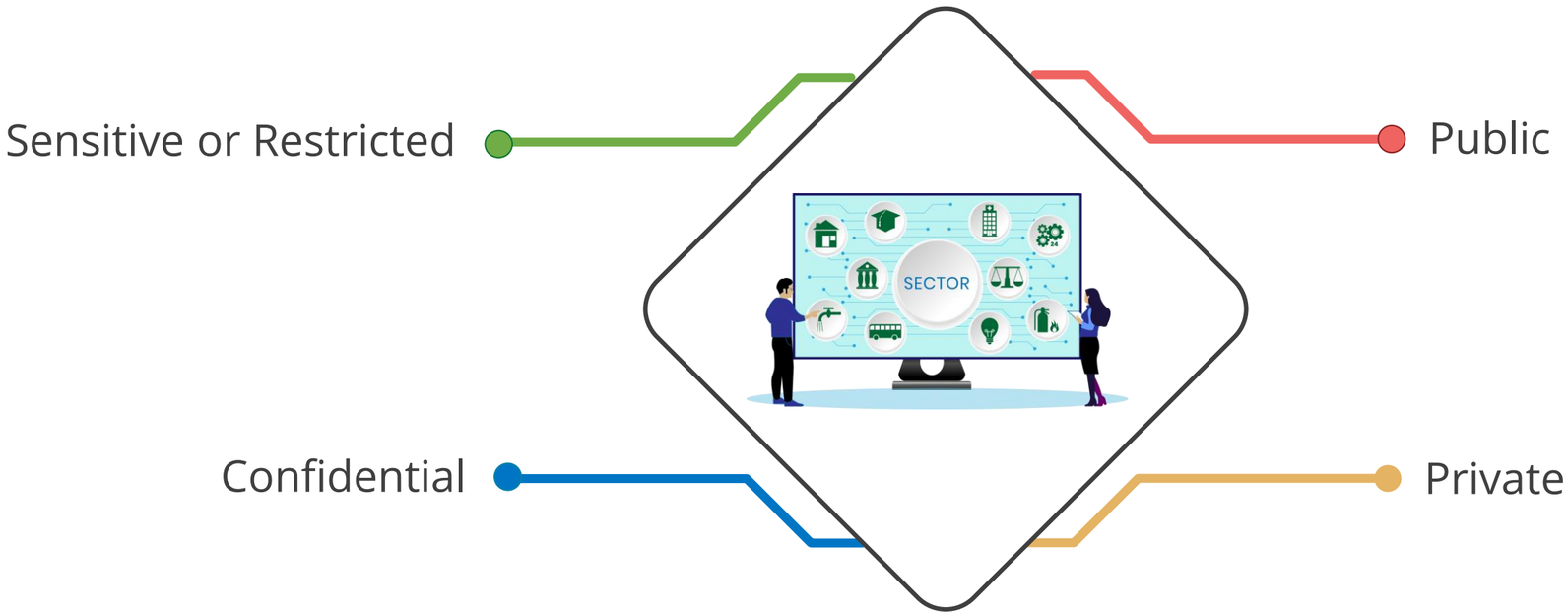
The following image illustrates the damage caused to Government and non-Government sectors incase of a potential data breach:



Commercial or Private Sector Classification

The information classification scheme followed by the commercial or private sector has four levels.

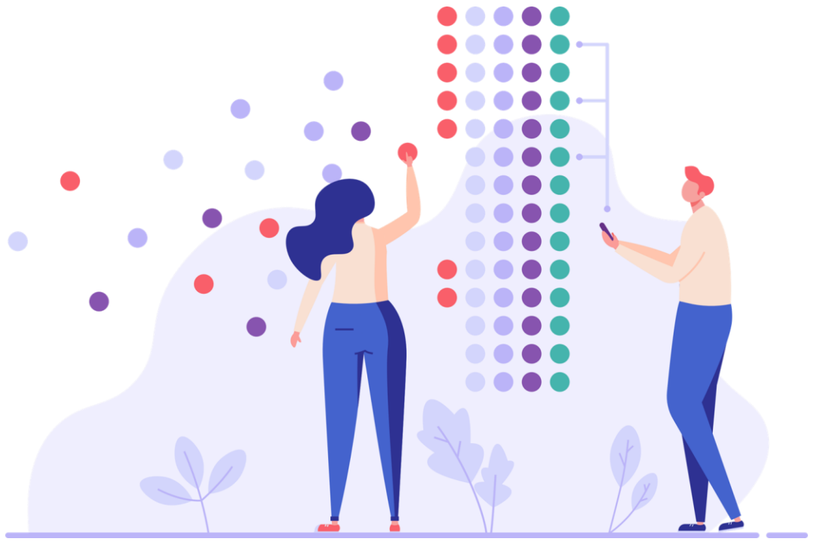
Commercial or private sector classification:



Data Classification Considerations

When classifying data, a security practitioner takes the following into consideration:

- Data access privileges (roles)
- Data retention requirements
- Data security requirements
- Disposal of data and its methods
- Data encryption requirements
- Appropriate use of data
- Regulatory or compliance requirements

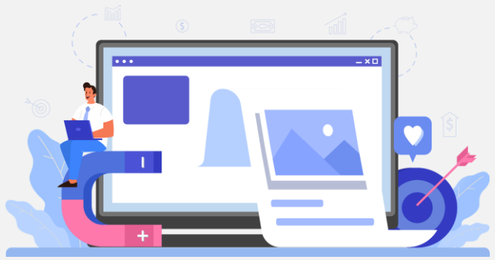


Role Responsible for Data Classification

The data owner is responsible for data classification.
The data owner:

- Knows the use and value of the data to organization
- Annually reviews the data classification

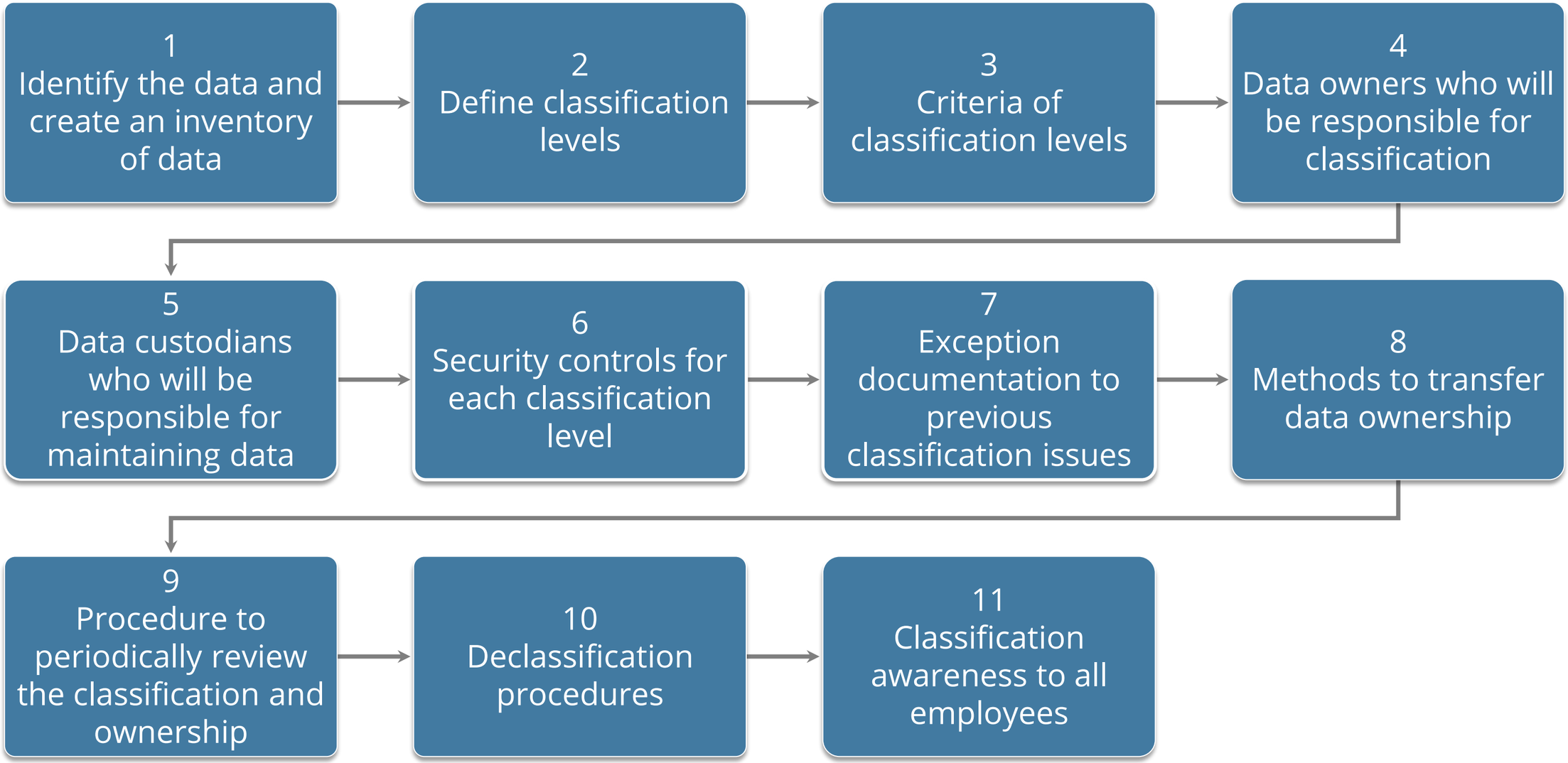
Role Responsible for Data Classification



The responsibilities of the organization are to:

- Document deviations and take corrective action
- Ensure the data is retained based on the organization's retention policy and subsequently destroyed in a secure manner

Data Classification Procedure



Establish Information and Asset Handling Requirements

Data Handling Requirements

- Data policy helps to mark, store, handle, and destroy sensitive information.
- Information handling requires all information assets to be clearly marked and labeled.
- Information classification helps to properly handle the information.

Data Handling Requirements

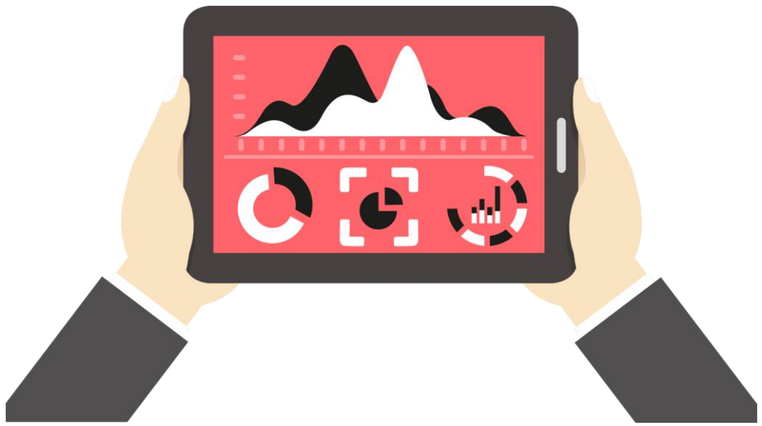
Handling media that stores sensitive information requires controls

- Mark, store, and handle based on the information classification

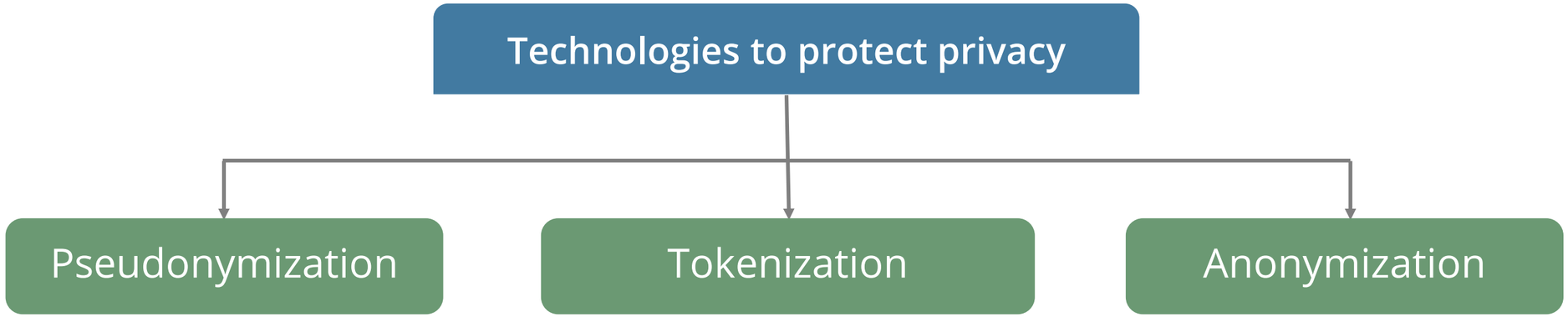
Data Handling Requirements

Record retention involves the following:

- Information and data should be retained if it is required by the organization.
- Retention policies must also consider legal and regulatory requirements.



Protecting Privacy



Protecting Privacy: Pseudonymization

Pseudonymization

- It refers to the process of using pseudonyms to represent other data.
- It can be done to prevent the data from directly identifying an entity, such as a person.
- For example, consider a medical record held by a doctor's office. Instead of including personal information, it could refer to the patient as *Patient 23456* in the medical record. The doctor's office would still need the personal information, and it could be held in another database linking it to the patient's pseudonym.

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	Xxxxx
Marco	Loqfh	xxxxx
Lex	Mcv	Xxxxx
Les	Mcv	Xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx

Protecting Privacy: Data Anonymization

Direct identifier

- Direct identifiers include information that relate specifically to an individual and can be used in isolation to uniquely identify an individual.
- Examples of direct identifiers include Social Security number, full name, email address, telephone number, health insurance number, medical record number, full-face photographs, or biometric record, such as fingerprints.

Indirect identifier

- Indirect identifiers include information that can be combined with other information to identify specific individuals.
- For example, a combination of gender, date of birth, geographic indicators, and other descriptors.

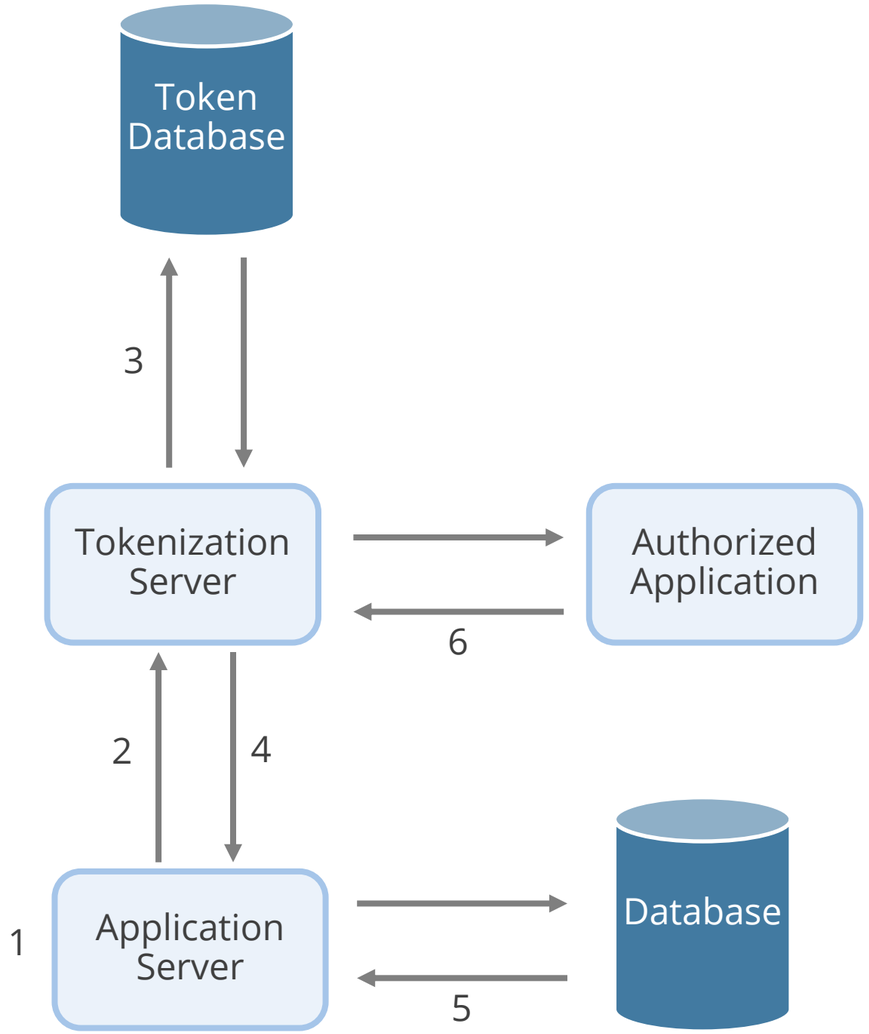
Data anonymization

- Anonymization is the process of removing the indirect identifiers to prevent data analysis tools or other intelligent mechanisms from collating or pulling data from multiple sources to identify sensitive information.

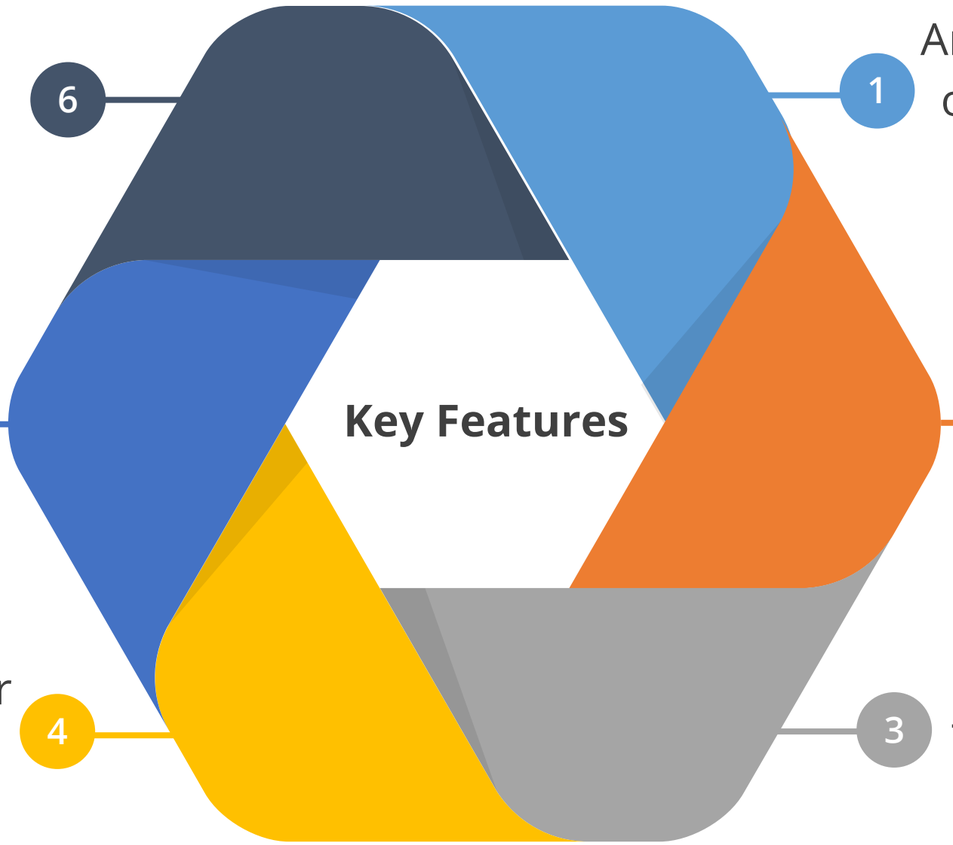
Protecting Privacy: Tokenization

Tokenization

- It is the process of substituting a sensitive data element with a nonsensitive equivalent referred to as a token.
- Tokenization is a technology which:
  - Replaces the original data with nonsensitive placeholders
  - Is used to safeguard the sensitive data in a secure, protected, and regulated environment



Protecting Privacy: Tokenization



1. An application collects or generates a piece of sensitive data.
2. Data is sent to the tokenization server. It is not stored locally.
3. The tokenization server generates the token. The sensitive data and the token are stored in the token database.
4. The tokenization server returns the token to the application.
5. The application stores the token rather than the original data.
6. When the sensitive data is needed, an authorized application or user can request it.

Some Recent Attacks on Privacy

Marriott International

- **Date:** 2014-18
- **Impact:** 500 million customers
- **Details:** In November 2018, Marriott International announced that cyber thieves had stolen data of approximately 500 million customers. The breach occurred on systems supporting Starwood hotels starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

Some Recent Attacks on Privacy

Adult FriendFinder

- **Date:** October 2016
- **Impact:** More than 412.2 million accounts
- **Details:** The FriendFinder Network, which included casual hookup and adult content websites like Adult FriendFinder, Penthouse.com, iCams.com, and Stripshow.com, was breached sometime in mid-October 2016. The hackers collected twenty years of data on six databases that included names, email addresses, and passwords.

Software Licensing

To avoid copyright infringement, the organization must secure the original copies of the licensed software.

Considerations for software licensing:

- Avoid creating and installing illegal copies of software
- Identify unauthorized software installations
- Manage licenses properly
- Appoint a software or media librarian who will control the media and software assets

Provision Resources Securely

Data Ownership

An information owner or a data owner can be an individual or a group who has created, acquired, or purchased the information and is directly responsible for it.

Data Ownership

- Determining how the organization's mission and strategic goals will be impacted by the information
- Determining the cost of replacing the information
- Understanding the requirements of entities within and outside the organization
- Recognizing when the information has reached the end of its life cycle and then destroying it

The responsibilities of a data owner

Data Custodian

- Be responsible for the safe custody, storage, and transportation of data, implementing the business rules, the technical environment, and database structure
- Help protect the integrity and security of data by ensuring it is properly stored and protected
- Ensure the data is backed up in accordance with the standard backup procedures
- Allow only authorized and controlled access
- Identify data stewards for every dataset
- Ensure data integrity is maintained in technical processes
- Ensure security controls safeguard the data
- Audit data content and changes

Data custodian

Asset Inventory

An **asset owner** is responsibility for the day-to-day management of an asset. Responsibilities include updating the inventories and carrying out audits.

Asset inventory management refers to the tools and processes needed to keep an up-to-date record of all hardware and software within the organization.

The first step in the classification process is to prepare an **asset inventory** and determine the location of the assets.

Asset Management

Asset management can be understood through the concepts of inventory management and configuration management.

Inventory management

Inventory management involves capturing details about the assets, their location, and their owners. IT assets can be both software and hardware.

IT asset management (ITAM) combines financial, inventory, and contractual functions to support life cycle management of IT assets and strategic decision making for the IT environment.

Asset Management

Asset management can be understood through the concepts of inventory management and configuration management.

Configuration management

Configuration management is the systematic handling of changes in a way that ensures the integrity of the asset or system over time using the appropriate policies, procedures, techniques, and tools.

A configuration management database (CMDB) is a database containing relevant information on the information system components used in an organization's IT services and the relationships between those components.

Data Management

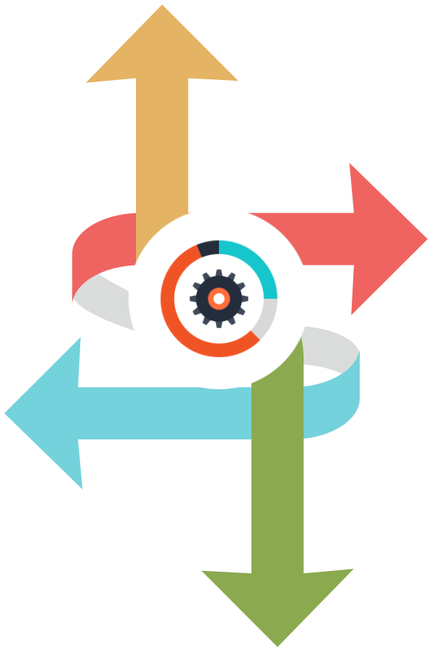
Backlog management

- It involves managing the information life cycle needs of an enterprise in an effective manner by developing and executing architectures, policies, procedures, and practices.
- The activities range from the administrative to the technical aspects of data handling.

Data Management

Need for data management

Ensure data complies to standard classifications



Ensure data validity

Secure and maintain data

Ensure data integrity and consistency

Manage Data Life Cycle

Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

Data owner is accountable for ensuring that specific data is protected. Data owners determine data sensitivity labels and the frequency at which data backed up.

The general responsibilities of the data owner include:

- Ensure compliance with the organization policies and all regulatory requirements as they relate to the information asset
- Assign an appropriate classification to information assets
- Determine appropriate criteria for obtaining access to information assets

Data owner

Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

Data custodian is responsible for maintaining and protecting the data.

The general responsibilities of the data owner include:

- Implement recommended practices to support well-managed data
- Assign and remove access to others based upon the direction of the data owner
- Produce reports or information for others
- Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of the information asset dataset

Data custodian

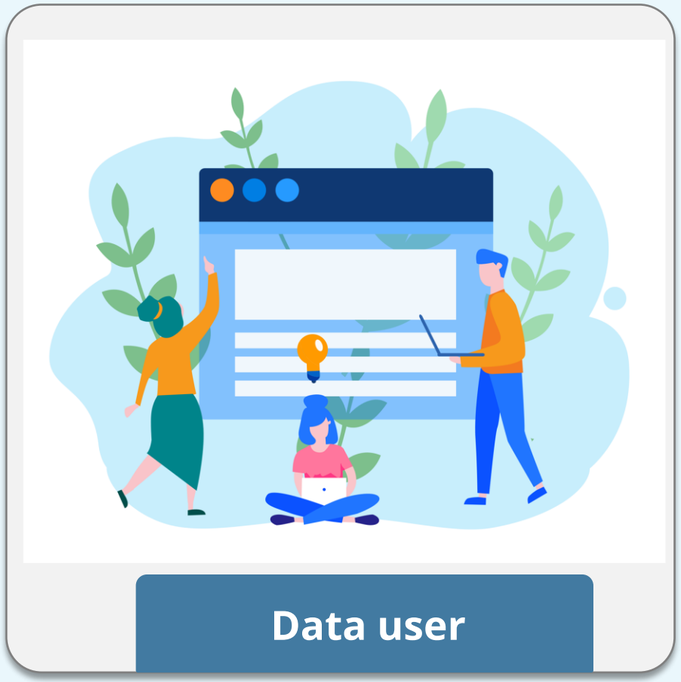
Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

Data user is any employee, contractor, or third-party provider who is authorized by the data owner to access information assets.

The general responsibilities of the data owner include:

- Adhere to policies, guidelines, and procedures pertaining to the protection of information assets
- Report actual or suspected security and policy violations to the appropriate authority



Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

Data controller determines the purposes for which and the means by which personal data is processed.

Data controller responsibilities:

- Collecting the personal information of your customers, site visitors, and other targets.
- Changing or modifying the data that you get.
- Finding from where and how to use the data and towards what purpose.
- Deciding how long the data is kept, and when to dispose of it.

Data controller

Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

Data processor processes data on behalf of the data controller. The data processor is usually a third-party external to the company.

- Unlike data controllers, a data processor does not bear the legal responsibility and accountability for the data.

Data processor

Data Roles

There are six data roles in the life cycle of data. Each one is described in the following slides.

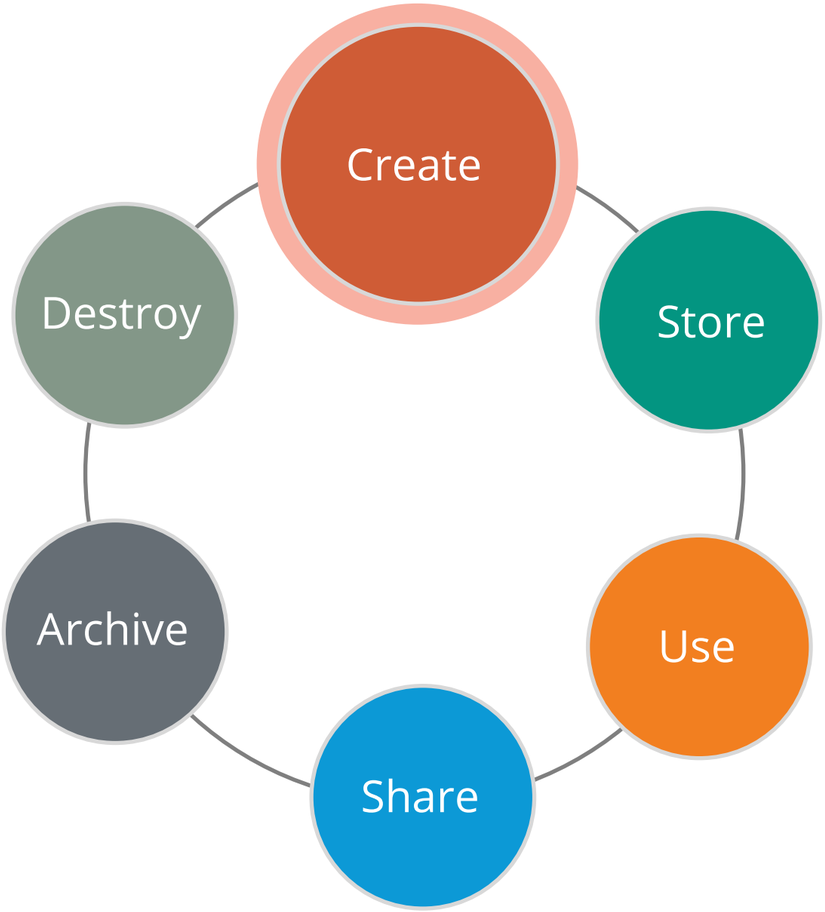
Data subject is a **natural** person or individual who is the subject of personal data.

Data Life Cycle: Create

The create phase involves generation or acquisition of new digital content or altering or updating existing content.

- **Data created remotely:**
  Data created remotely should be encrypted before uploading to the server to protect against obvious vulnerabilities, such as man-in-the-middle attacks.

- **Data created in server:**
  Data created in server via remote manipulation should be encrypted upon creation.



Data Collection

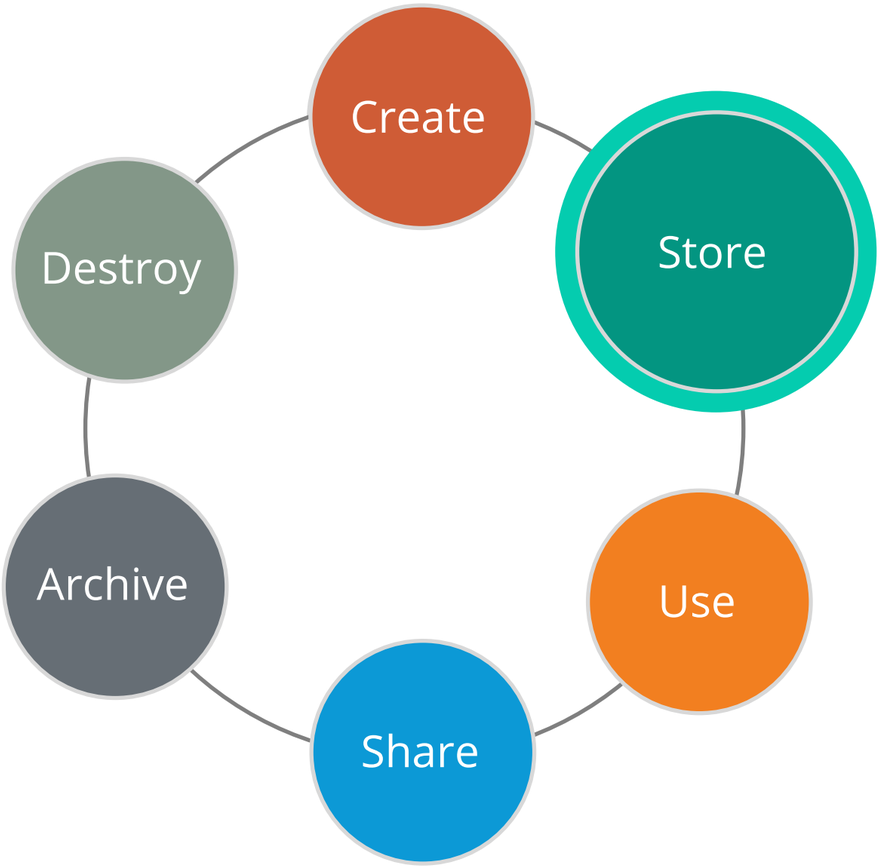
Privacy laws generally include a requirement that **personal data** must not be collected unless it is relevant.

- Such data should be obtained by **lawful** and **fair** means.
- The **purposes** for which personal data are collected should be **specified** at the time of data collection.
- The collected data cannot be used for any other purposes other than the specified purpose.
- **Data subjects** must give their **consent** for the data collected.

The create phase necessitates activities like categorization and classification; labeling, tagging, and marking; and assigning metadata.

Data Life Cycle: Store

- Digital data is committed to some sort of storage repository and typically occurs nearly simultaneously with creation.
- Controls such as encryption, access policy, monitoring, logging, and backups should be implemented to avoid data threats.
- Content can be vulnerable to attackers if access control lists (ACLs) are not implemented well, files are not scanned for threats, or files are classified incorrectly.



Data Location

Data residency

Data residency refers to where a business specifies that their data is stored geographically.
This is usually done for regulatory, tax, or policy reasons.

Data sovereignty

Data sovereignty means that the data stored in a particular country is also subject to the laws of that country.

Data localization

Data localization laws restricts data flow by limiting the physical storage of data within the borders of the country where the data is generated.

Real World Scenario

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) signed into law in March 2018, is a United States federal law to allow federal law enforcement to compel U.S. based technologies company via subpoena or a warrant to provide trans-border access to data regardless of whether the data is stored in the U.S. or on foreign soil.

The genesis for this bill is United States v. Microsoft, a case from a 2013 drug trafficking investigation, during which the FBI issued an SCA warrant for emails that a U.S. citizen had stored on one of Microsoft's remote servers in Ireland. Microsoft refused to comply with the request and argued that the SCA did not cover data stored outside the United States.

The CLOUD Act does not supersede, ignore, or change another country's local law. In fact the CLOUD Act provides additional safeguards for the companies or courts to challenge requests that conflict with the privacy rights of another country the data is stored in.

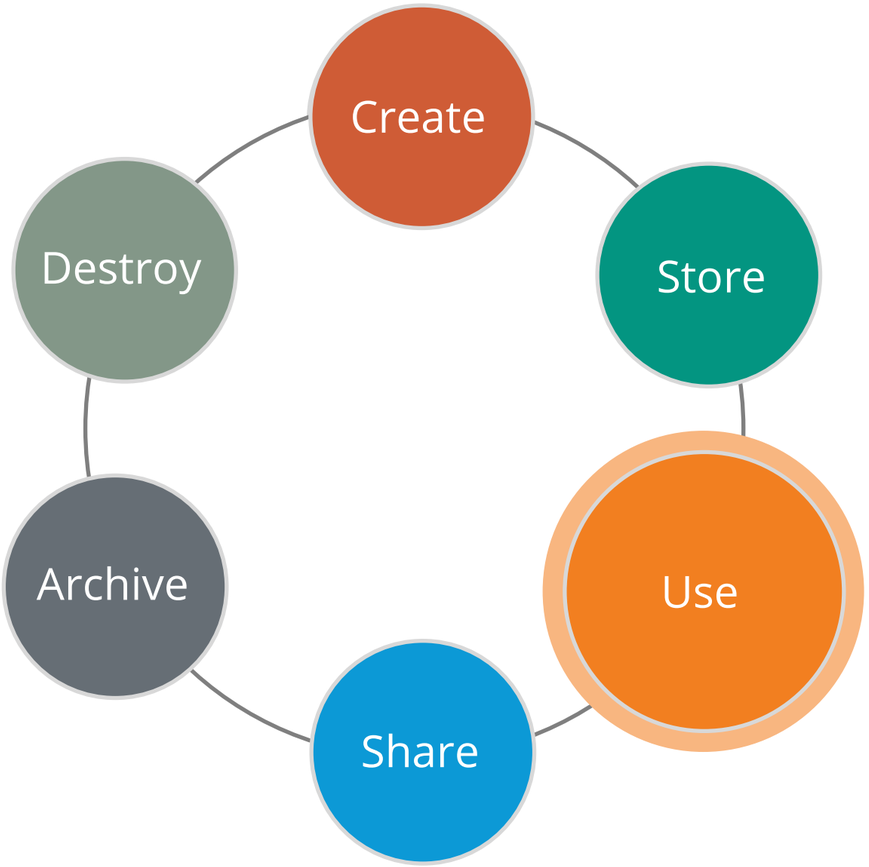
There is a potential for conflict between the CLOUD Act and GDPR, if a U.S. citizen who resides in the EU is the subject of a CLOUD Act warrant.

Information source: https://en.wikipedia.org/wiki/CLOUD_Act

Data Life Cycle: Use

Data is viewed, processed, or otherwise used in a variety of activities.

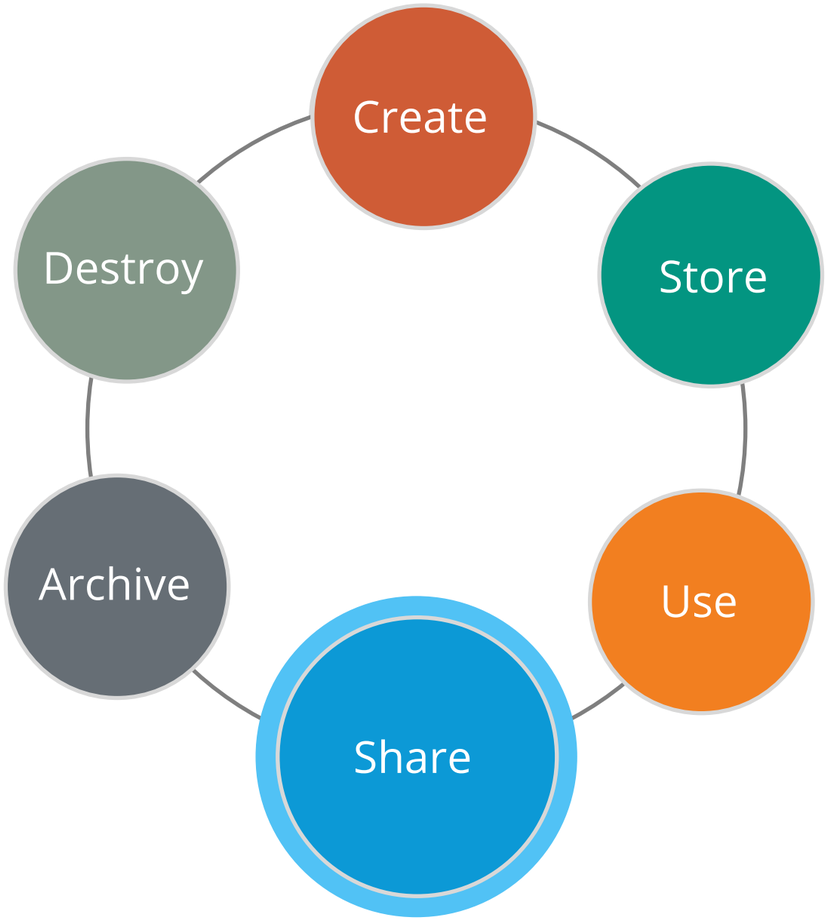
- Data is most vulnerable when in use as it might be transported into unsecure locations, such as workstations, where it must be unencrypted to be processed.
- Controls such as data loss prevention (DLP), information rights management (IRM), and database and file access monitors should be implemented to audit data access and prevent unauthorized access.



Data Life Cycle: Share

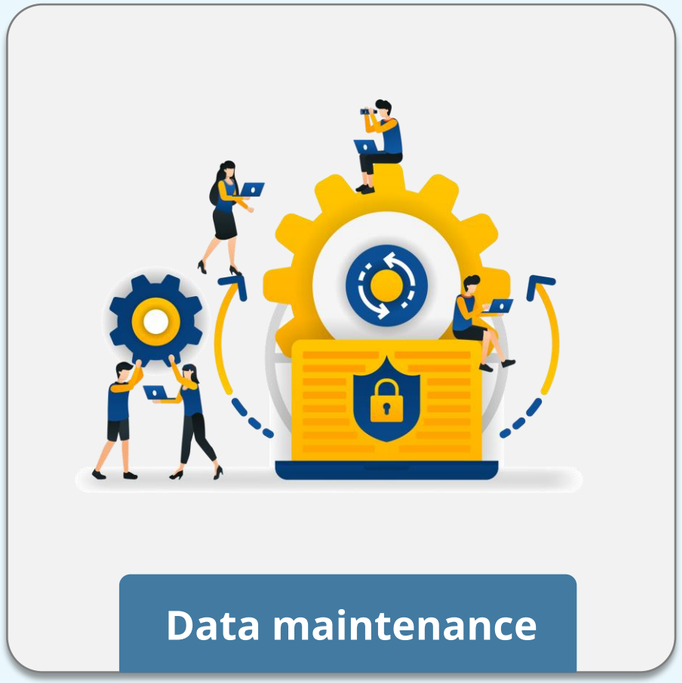
Data is exchanged between users, customers, and partners.

- Not all data should be shared, and not all sharing should present a threat.
- As data that is shared is no longer in the organization's control, maintaining security can be difficult.
- **DLP** technologies can be used to detect unauthorized sharing, and **IRM** technologies can be used to maintain control over the information.



Data Maintenance

- Data maintenance is the process of continually improving and regularly checking data to ensure it is in good health.
- The ongoing correction and verification of data is essential to ensuring that the data remains accurate, complete, accessible, and usable for its intended purposes.



Data Maintenance

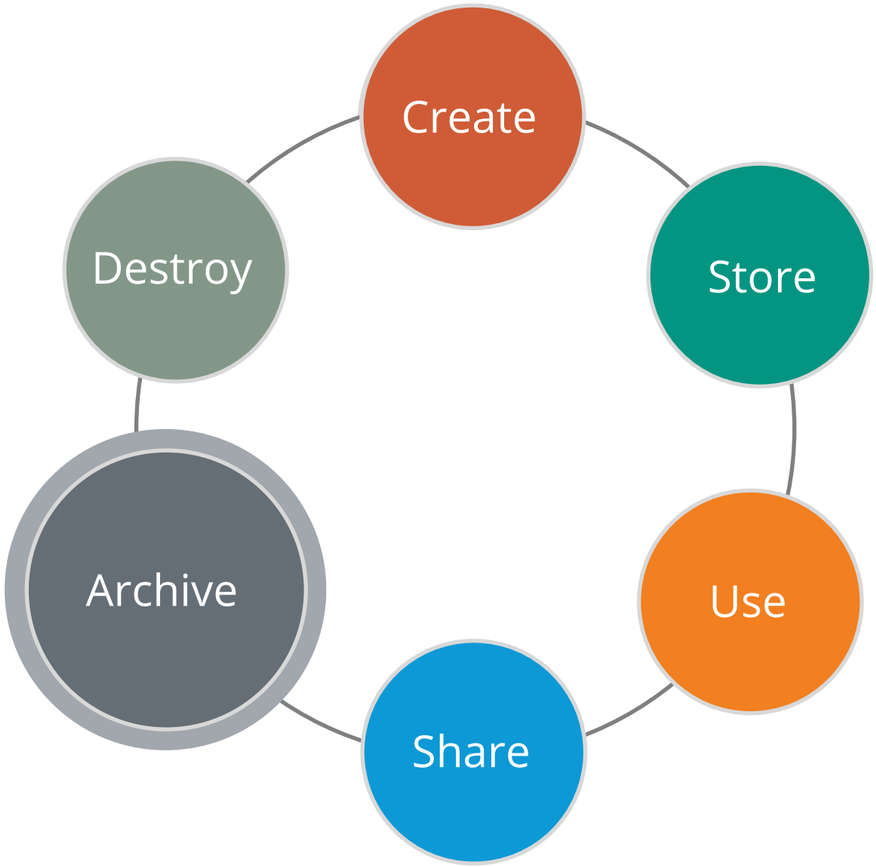
Data cleansing is a one-off process in which the data that is incomplete, incorrect, improperly formatted, duplicated, or irrelevant is either removed or updated.

Data cleansing

Data Life Cycle: Archive

Data archiving is the process of identifying and moving inactive data out of current production systems and into specialized long-term archival storage systems.

Format	How is the data represented and stored?
Regulatory requirements	How long must the data be retained and other requirements for its preservation?
Technologies	What specific software applications are used to create and maintain the archives?
Testing	How can you ensure that backups can and will work when needed?



Data Retention

Data Retention

- Data retention involves retaining and maintaining data for a period along with the methods used to accomplish these tasks.
- The policy balances the legal, regulation, and business data archival requirements against data storage costs, complexity, and other data considerations.

Data Retention

Steps for building a sound retention policy:

- Evaluate the regulatory requirements, business needs, and legal obligations
- Classify assets based on their value to the organization
- Determine asset retention periods and destruction practices
- Create a record retention policy
- Train the staff on retention policy requirements

Data Retention

Steps for building a sound retention policy:

- Regularly audit practices for record retention and destruction
- Review the retention policy periodically
- As the best practice, maintain the documentation of the policy, its implementation, training, and audits

Data Retention

A good data retention policy includes the following:

Data formats

Data security

Data-retrieval procedures for the enterprise

Data classification

Legislation, regulation, and standard

Retention periods

Discussion

Discussion

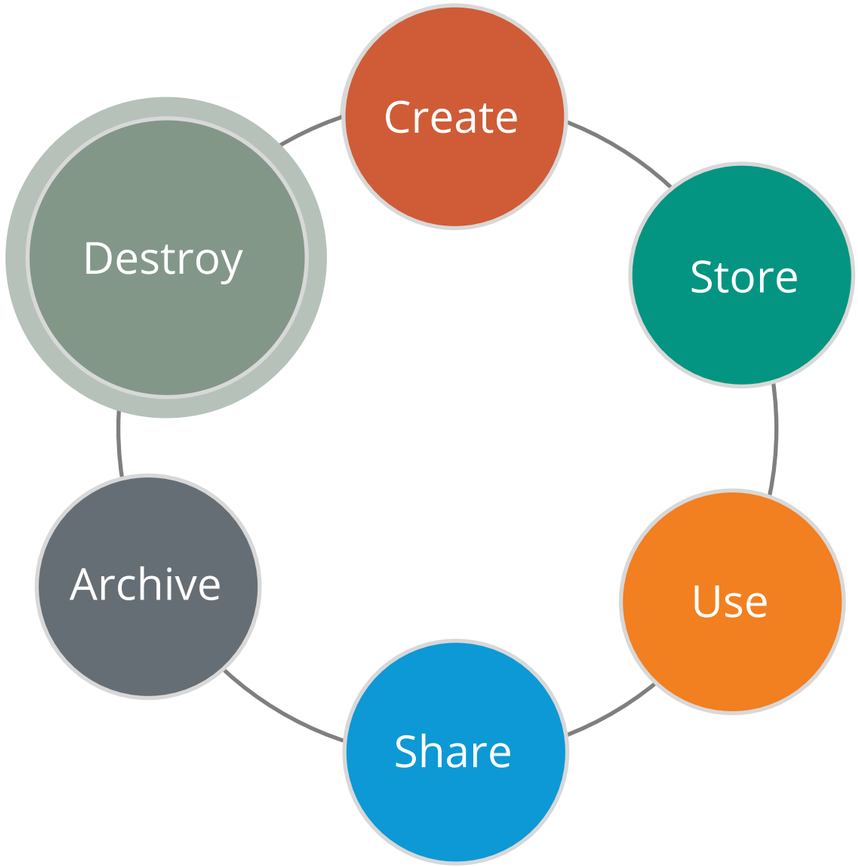
A magnetic drive is used to archive an organization's data.

What information about the data can be on the label that is placed on the front side of the media so that it is more visible?

Data Lifecycle: Destroy

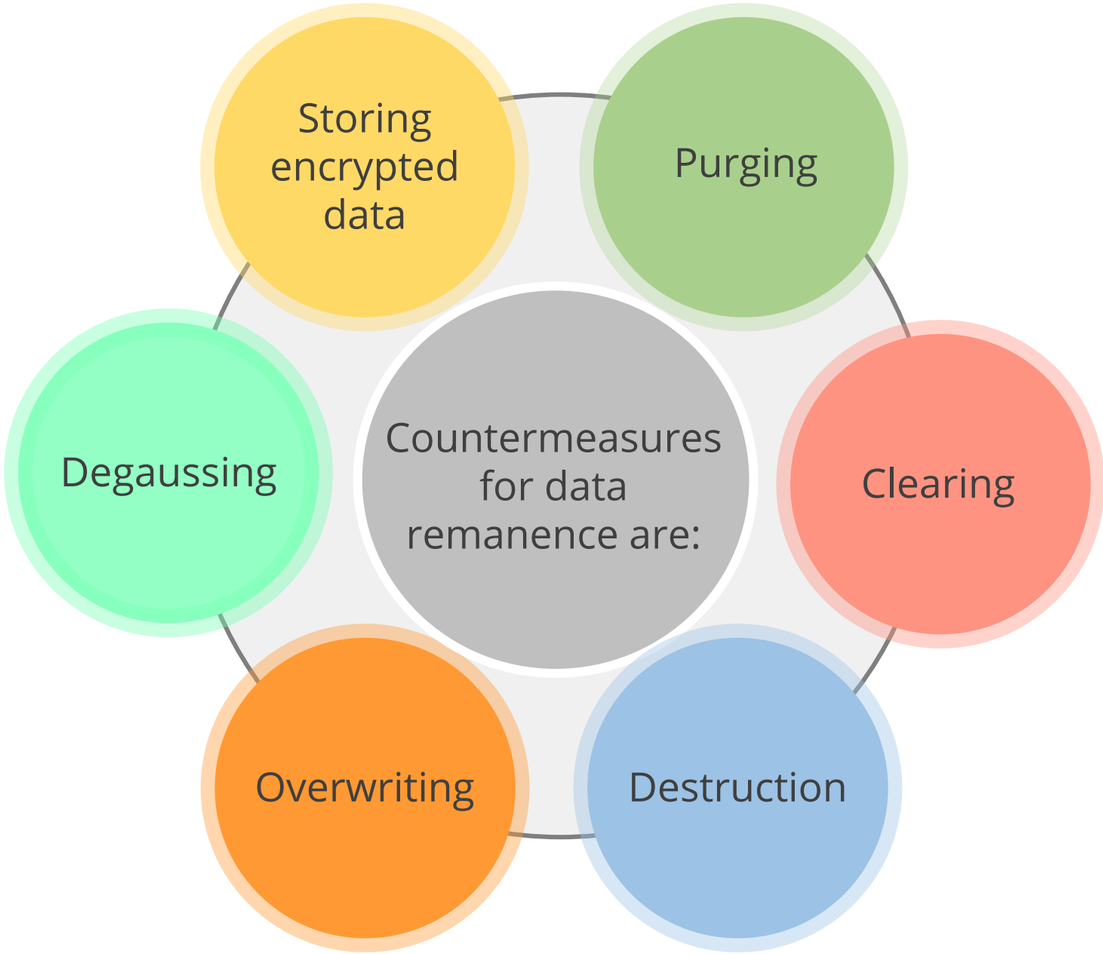
Data is permanently destroyed using physical or digital means (e.g., crypto shredding).

- Data destruction can mean logically erasing pointers or permanently destroying data using physical or digital means.
- Consideration should be made according to regulation.



Data Remanence

- The residual representation of digital data that remains even after attempting to erase or remove the data is called data remanence.
- Data remanence in HDD happens if the method used to clean the HDD fails.
- Security practitioners must be familiar with the different technologies employed in storage devices to deal with issues of data remanence.



Data Destruction

There are 5 major ways to destroy data. Each of them is explained in the following slides:

- Erasing
- Clearing (overwriting)
- Purging
- Sanitization
- Degaussing

- Erasing is a simple deletion process.
- The process removes only the catalog reference and not the files.
- Not the best practice to destroy data, because anyone can retrieve the data using widely available tools.

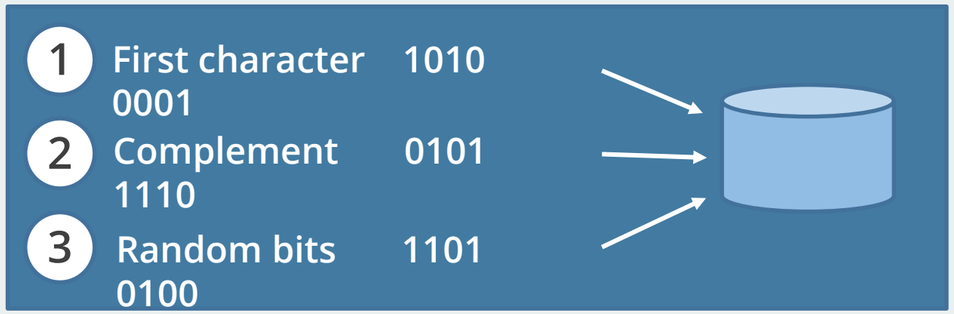
Data Destruction

There are 5 major ways to destroy data. Each of them is explained in the following slides:

- Erasing
- Clearing (overwriting)
- Purging
- Sanitization
- Degaussing

- Process of preparing the media for reuse with assurance that cleared data cannot be retrieved using traditional means of recovery.
- Unclassified data is written over all the addressable locations on the media.
- Data recovery requires special laboratory techniques.
- This method is used in those cases when you want to prepare media for reuse at the same classification level.

The following image illustrates the clearing process:



Data Destruction

There are 5 major ways to destroy data. Each of them is explained in the following slides:

- Erasing
- Clearing (overwriting)
- **Purging**
- Sanitization
- Degaussing

- More intense form of clearing; repeats the clearing process multiple times
- Provides assurance that data cannot be recovered using any known means
- Can be combined with degaussing to completely remove data
- Used in those cases when one wants to prepare media for reuse at lower classification level

Data Destruction

There are 5 major ways to destroy data. Each of them is explained in the following slides:

- Erasing
- Clearing (overwriting)
- Purging
- **Sanitization**
- Degaussing

- Sanitation is the combination of processes that ensures data is removed from the system.
- It ensures data cannot be recovered by any means.
- Sanitation process includes ensuring non-volatile memory is erased, external drives removed and sanitized in order to destroy data.

Data Destruction

There are 5 major ways to destroy data. Each of them is explained in the following slides:

- Erasing
- Clearing (overwriting)
- Purging
- Sanitization
- Degaussing

- Generates heavy magnetic fields which realign the magnetic fields in magnetic media, only effective on magnetic media (does not affect, CD/DVD/SSD)
  - AC erasure: Medium is degaussed by applying alternating field that is reduced in amplitude over time
  - DC erasure: Medium is saturated by applying a unidirectional field

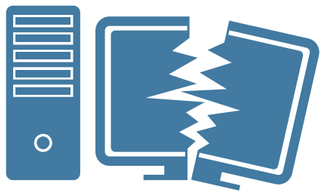
Data Destruction Methods

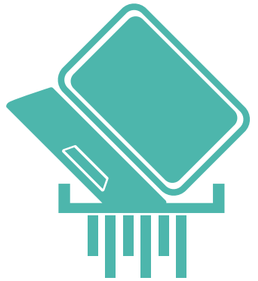
- Destruction is the final stage in the life cycle of media and is the most secure method of sanitizing media.
- When destroying media, it is important to ensure that the media cannot be reused or repaired, and that data cannot be extracted from the destroyed media.

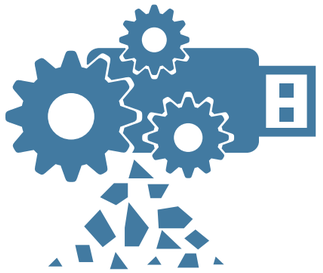
Data Destruction Methods

Broadly, there are 5 methods to destroy data:

- Incineration
- Crushing
- Shredding
- Disintegration
- Dissolving using caustic or acidic chemicals







Data Remanence: Cold Boot Attack (Case Study)

- In computer security, a **cold boot attack** (or to a lesser extent, a **platform reset attack**) is a type of a side-channel attack in which an attacker with physical access to a computer performs a memory dump of the computer's random access memory by performing a hard reset of the target machine.
- Typically, cold boot attacks are used to retrieve encryption keys from a running operating system for malicious or criminal investigative reasons.
- The attack relies on the data remanence properties of DRAM and SRAM to retrieve memory content that remain readable in the seconds to minutes after power has been removed.

Ensure Appropriate Asset Retention

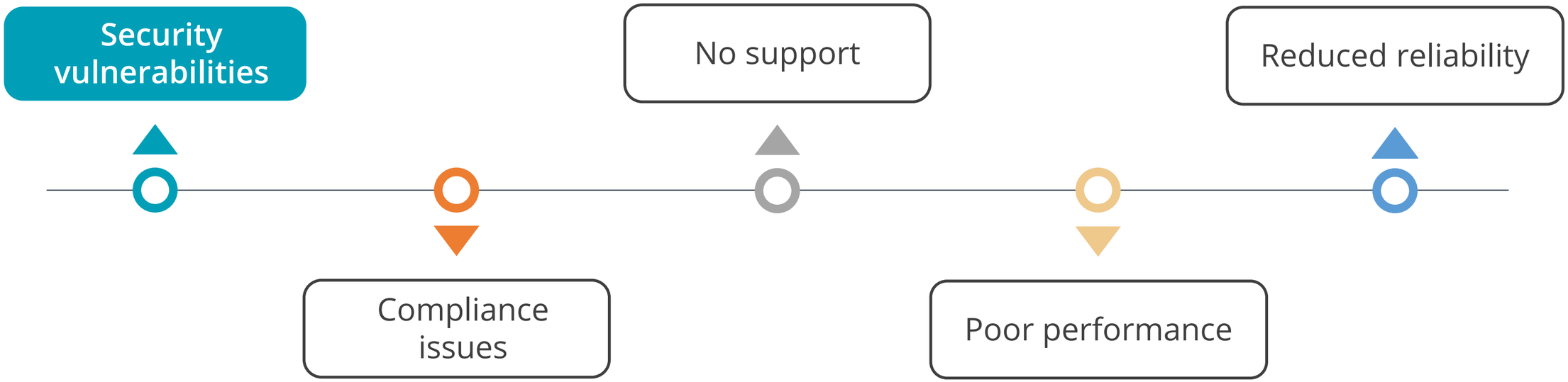
Asset Retention

Appropriate asset retention requires the maintenance of EOL or EOS.

End-of-life (**EOL**) refers to the date where a vendor no longer manufactures a particular product and does not takes orders for this product.
Some manufacture refer to this as ‘End of ‘Sale’.

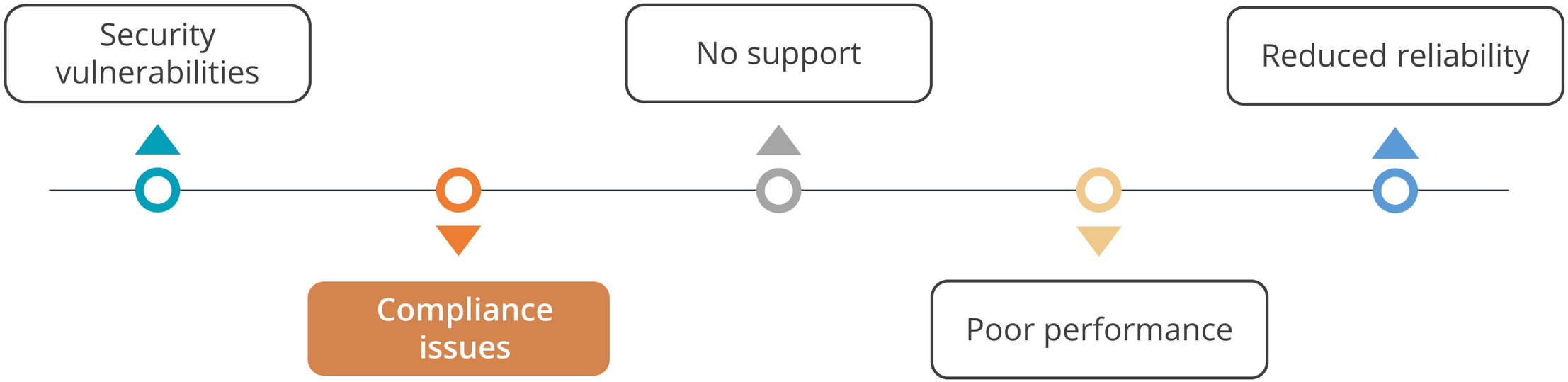
- **End-of-Support (EOS)** refers to the date where vendor no longer provides support for a particular product.
- Upon end of support, manufacturers do not provide any new security updates, non-security updates, free or paid assisted support options or online technical content updates.

Potential Risk of EOL/EOS systems



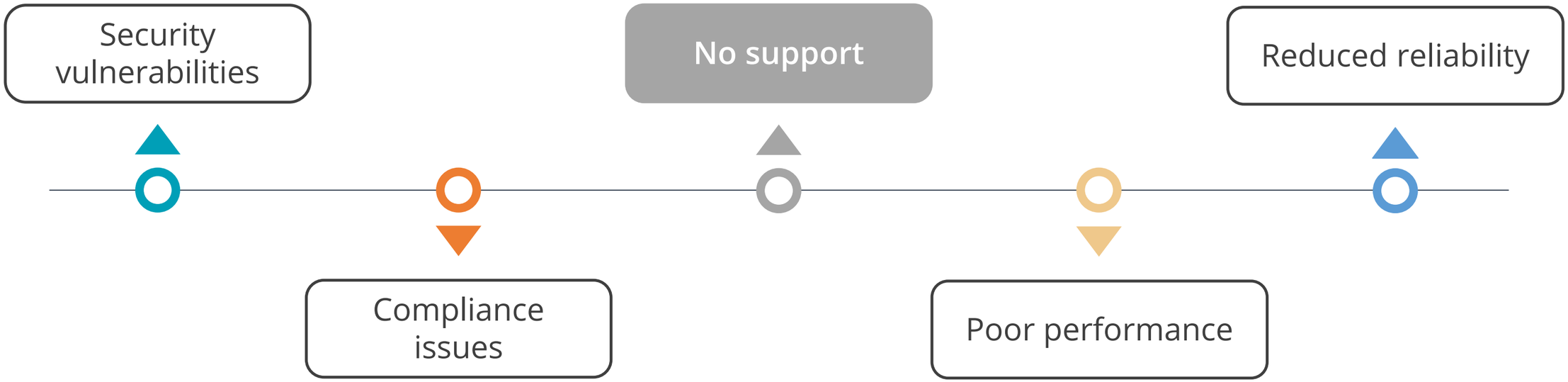
When a vendor stops issuing security patches, your system is left vulnerable to security attacks. A firewall and anti-malware systems cannot provide sufficient protection against unpatchable vulnerabilities, which may be exploited by hackers.

Potential Risk of EOL/EOS systems



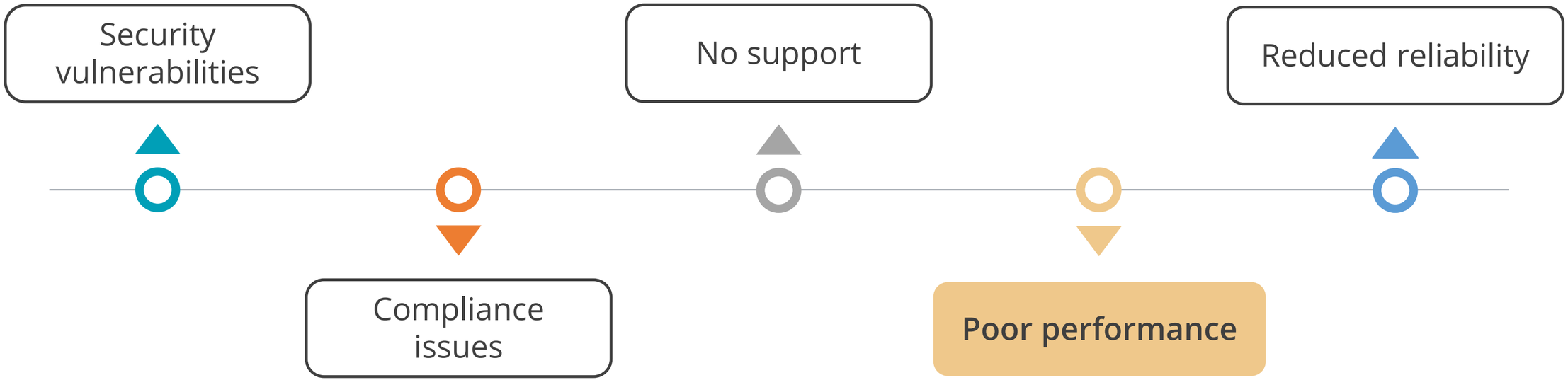
Regulated industries like healthcare and finance which deals with sensitive data may prohibit the use of EOL systems.

Potential Risk of EOL/EOS systems



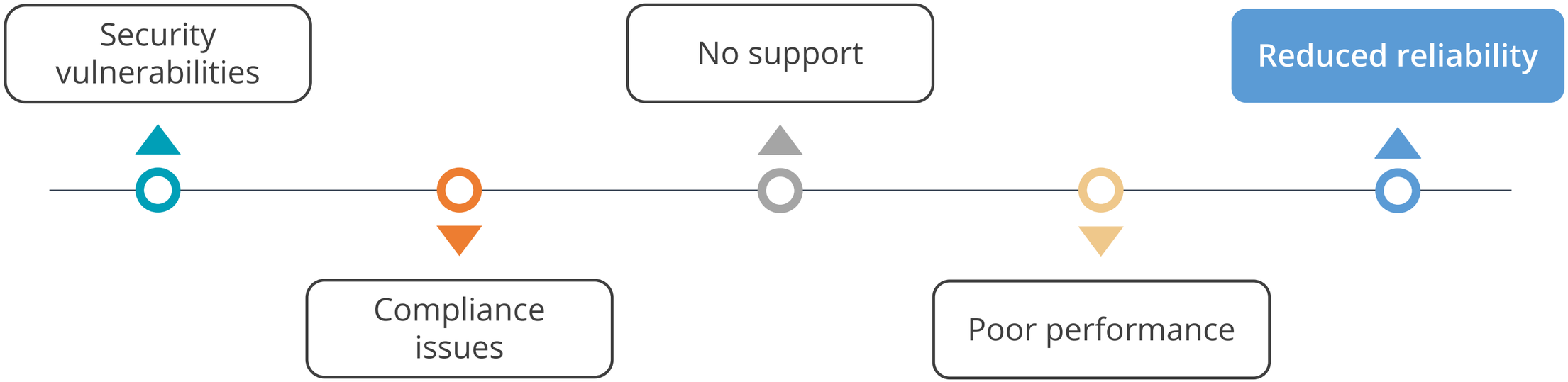
Since the vendor no longer provides any support, there's no official means to receive help troubleshooting and getting the system running again if any issues occur.

Potential Risk of EOL/EOS systems



Running legacy systems may result in poor performance and reduced productivity.

Potential Risk of EOL/EOS systems



EOL and out-of-warranty systems are prone to break down more often which could impact business operations.

Determine Data Security Controls and Compliance Requirements

Understanding States of Data

The states of data are:

Data at rest

- Data at rest is any data stored on media, such as system hard drives, external USB drives, storage area networks (SANs), and backup tapes.

Data in transit

- Data in transit, also called data in motion, is any data transmitted over a network.
- This includes data transmitted over an internal network using wired or wireless methods and data transmitted over public networks such as the Internet.

Data in use

- Data in use refers to data in temporary storage buffers while an application is using it.

Data Security Controls

Security controls for stored data and data on the network are described below.

Data at Rest

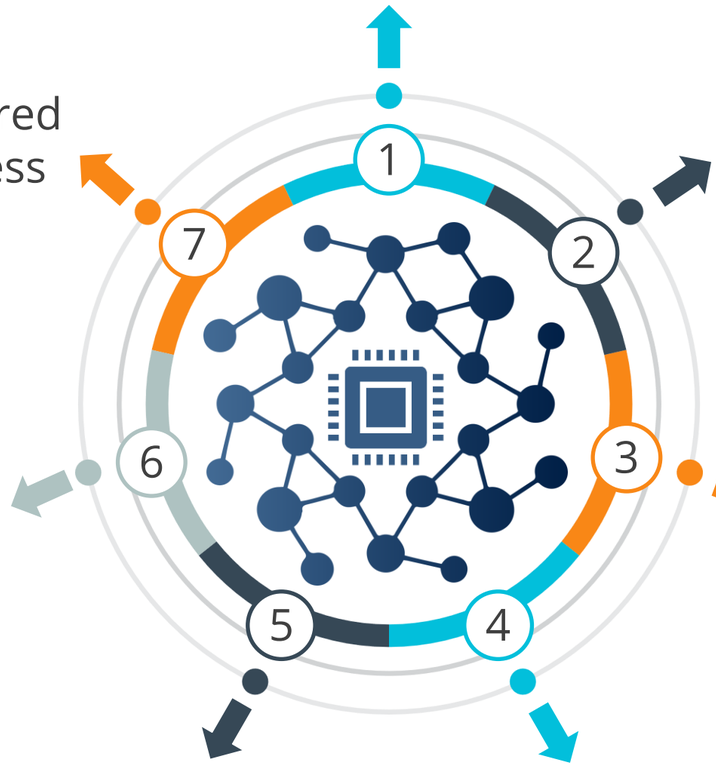
- Security controls include encryption, hashing, compressing, strong passwords, labeling, marking, storage, and documentation.
- **Encryption tools**: Self-encrypting USB drives and file and media encryption software

Data in Transit

- Security controls include cryptographic functions such as encryption and hashing.
- **End-to-end Encryption:** Data is encrypted, but the routing information remains visible
- **Link Encryption:** Data as well as routing information is encrypted

Data in Transit: Best Practices

Practices for securing data in transit:



1. Use of Secure Socket Layer (SSL) or Transport Layer Security (TLS)
2. Message encryption before transmitting emails
3. Use of Pretty Good Privacy (PGP) and Secure or Multipurpose Internet Mail Extensions or S or MIME for encryption
4. Using end-to-end encryption for intranet communication
5. Internet Protocol Security (IPsec) for secure Virtual Private Network (VPN) connectivity
6. Secure Shell (SSH) for the administration of network devices
7. Wireless networking secured with Wi-Fi Protected Access 2 (WPA 2)

Scoping and Tailoring

- NIST SP 800-53 discusses security control baselines as a list of security controls.
- Single set of security controls cannot be not applied to all situations, so organizations have selected a set of baseline security controls and tailor it to its needs.
- Scoping or tailoring is the act of adding or removing controls as needed to get the right level of protection.

Scoping	Tailoring
The process of determining and limiting general recommendations by removing aspects that do not apply to a specific environment or an organization.	Customizing and altering details of general recommendations to apply more specifically to an environment or an organization.

Standards Selection

- An organization can decide to select security standards or specific controls set to protect their assets.
- The organization can further scope and tailor these controls to adapt to their unique environment and requirements.
- When selecting controls, it is important to balance the value of the asset and the cost of the control to protect it.
- Some standards such as **PCI DSS** are mandatory for an organization processing major credit cards.

Security Baselining

- Baselines provide a starting point and ensure a minimum-security standard. One common baseline that organizations use is imaging.
- As an introduction, administrators configure a single system with the desired settings, capture it as an image, and then deploy the image to other systems. This ensures all systems are deployed in a similar secure state.
- After deploying systems in a secure state, auditing processes periodically check the systems to ensure they remain in a secure state.
- Example: Microsoft Group Policy can periodically check systems and reapply settings to match the baseline.

Business Scenario

Hilda Jacobs, general manager - IT Security at Nutri Worldwide Inc., was given the responsibility of selecting the appropriate data security controls as part of asset security.

Hilda selected the controls according to the organization's different requirements for the data at rest and data in transit based on the existing risk. She also created a best practices document by referring to available standards for data security.

Question: For implementing an information security management system, which standard should Hilda Jacobs refer to?

Business Scenario

Hilda Jacobs, general manager - IT Security at Nutri Worldwide Inc., was given the responsibility of selecting the appropriate data security controls as part of asset security.

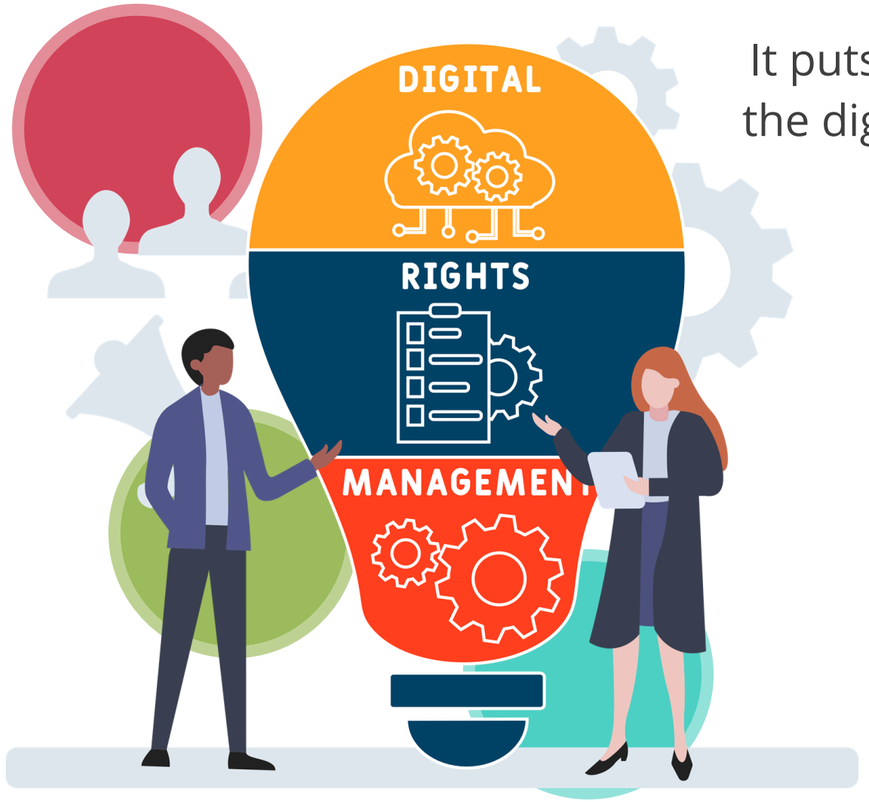
Hilda selected the controls according to the organization's different requirements for the data at rest and data in transit based on the existing risk. She also created a best practices document by referring to available standards for data security.

Question: For implementing an information security management system, which standard should Hilda Jacobs refer to?
Answer: ISO 27001

Digital Rights Management (DRM)

DRM is a class of technology used for copyright protection of digital media.

It puts restriction on copying the digital content purchased by consumers.



It uses cryptography to prevent unauthorized redistribution of digital media.

A special software or device is required to access DRM protected content.

Data Loss Prevention

DLP refers to a set of controls and practices put in place to ensure that data is only accessible and exposed to those users and systems authorized to have it.

The goals of a DLP strategy for an organization are to manage and minimize risk, maintain compliance with regulatory requirements, and show due diligence on the part of the application and data owner.

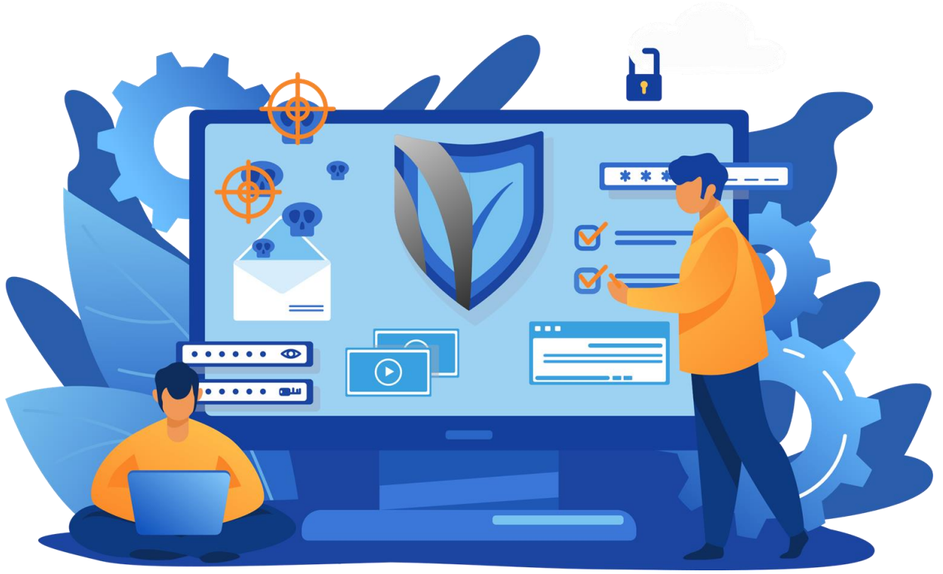
DLP should be integrated as a part of the risk management approach.

DLP is concerned with external parties.

Data Loss Prevention

DLP technology determination aspects

- Sensitive data awareness
- Policy engine
- Interoperability
- Accuracy (most critical)



DLP Approach

Implementation, testing, and tuning

- Test for false positives and false negatives
- Misuse cases prioritization and testing

Data inventory

- Identify the data
- Classify the data

Data protection strategy

- Perform risk assessment
- Determine the DLP solution

Data flows

- Plot the data flow over the life cycle

Types of DLP

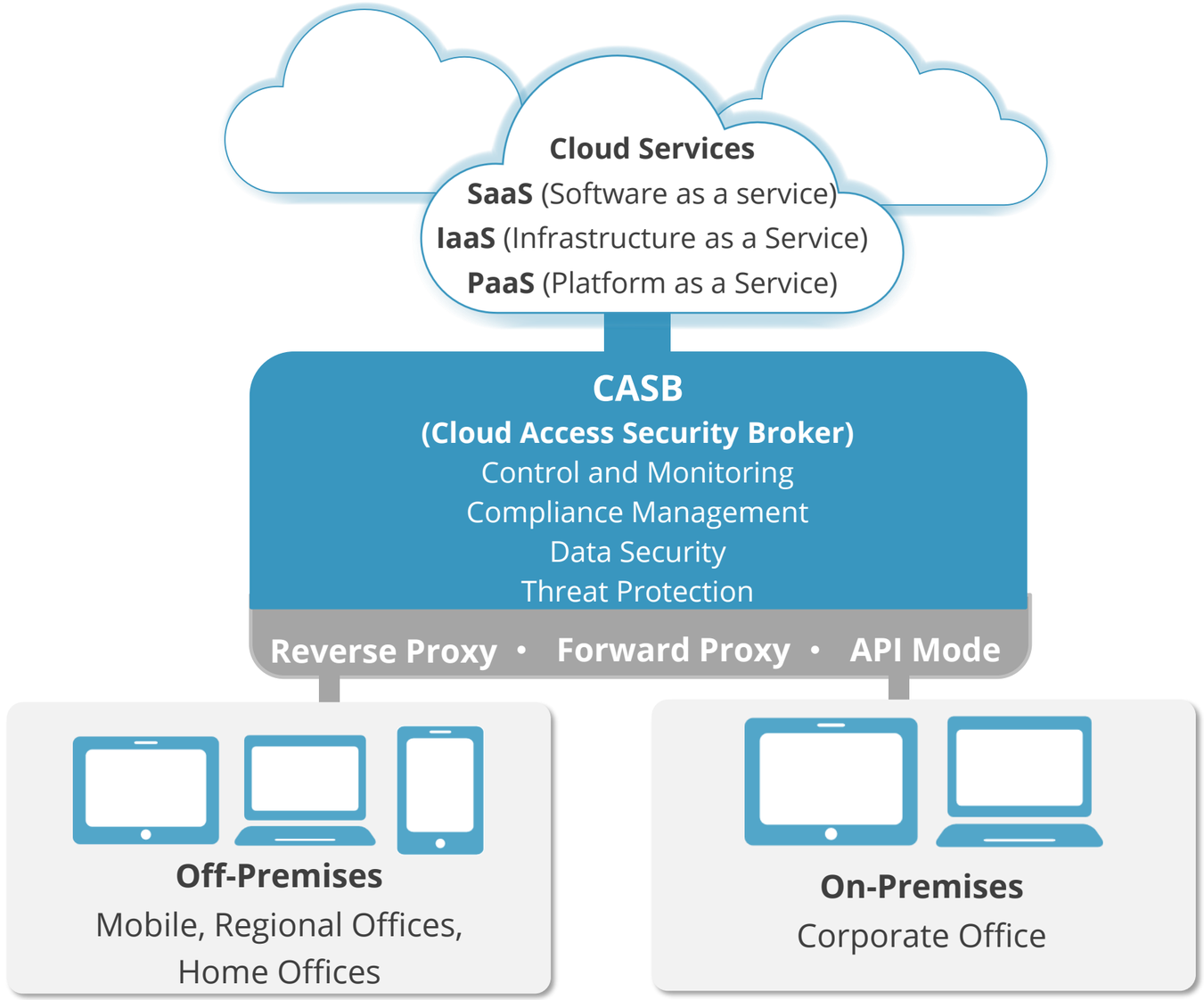
Network DLP	• Applies DLP to data in motion
	• Normally implemented as dedicated appliances at the perimeter
	• Some of the drawbacks are:
	  ◦ Does not protect data on devices that are not on the organization network
	  ◦ Higher cost forces organizations to deploy only at network choke points instead of throughout the network

Endpoint DLP	• Applies DLP to data in use and data in rest
	• An agent is installed on end-systems
	• Some of the drawbacks are:
	  ◦ Complexity
	  ◦ Agent management
	  ◦ Unaware to data-in-motion protection violations

Hybrid DLP	• Deploys both EDLP and NDLP • Most expensive and complex approach • Offers the best coverage and protection

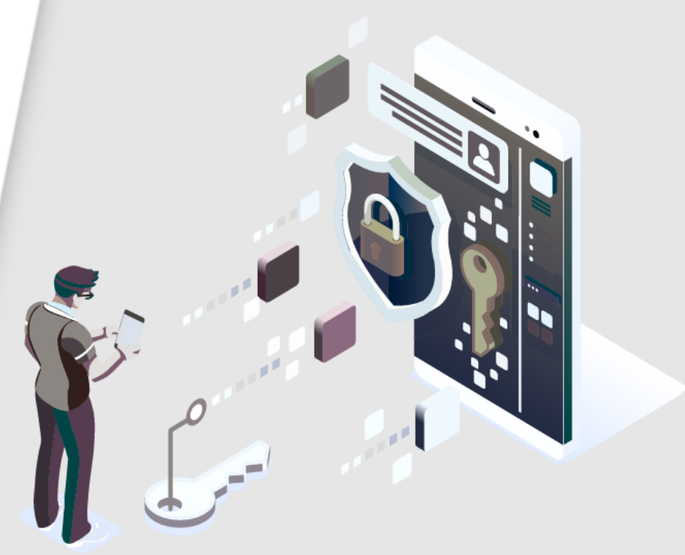
Cloud Access Security Broker

A **cloud access security broker** (**CASB**), also known as cas-bee, is an on-premises or cloud-based software that sits between cloud service users and cloud applications and monitors all activity and enforces security policies.



Key Takeaways

- Asset security covers different requirements, including the concepts, principles, and standards, to secure assets.
- Asset security addresses how information is collected, handled, processed, and secured throughout the IT life cycle.
- Asset security highlights the use of various controls to provide different levels confidentiality, integrity, and availability of all IT services throughout the organization.
- Security practitioners must understand and implement security controls for both data at rest and data in transit.
- Security professionals must be familiar with leading security standards and the bodies responsible for these.



This concludes **Asset Security**.

The next domain is **Security Architecture and Engineering.**