Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 02: Asset Security

Learning Objectives

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

- Apply privacy terms to assess their relevance for compliance with industry standards
- Identify data classification considerations and procedures for protecting sensitive data
- Analyze the information classification criteria and objectives to handle data appropriately
- Demonstrate the data life cycle, data management, and data roles for better governance
- Differentiate baselining, scoping, and tailoring for security customization
- Assess data loss prevention methods for protecting critical data from unauthorized access or breaches

Overview of Asset Security and Data Classification

Asset

It is any resource with value to an organization, whether tangible or intangible.

This includes people, hardware, software, data, information, or reputation.

Asset Security

It refers to the measures and strategies used to protect valuable assets, such as data, infrastructure, and equipment, from unauthorized access, theft, or damage.

- Ensures confidentiality, integrity, and availability of assets
- Restricts access to authorized individuals
- Involves classifying assets and applying security controls
- Manages risks to prevent threats and breaches

Asset Classification

It means categorizing and grouping assets based on their business value. The following are the steps to begin the classification process:

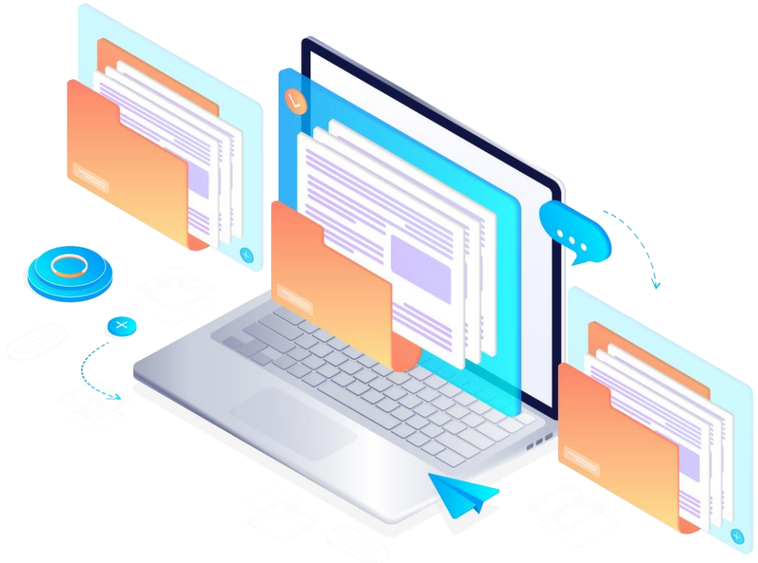
Prepare an asset inventory

Assign responsible owners

Apply classification levels to set security controls

Data or Information Classification

It is the process of assigning an appropriate classification level to a data asset to ensure proper protection.



Data Classification

The following are the characteristics:

Attaches the classification level throughout the data's life cycle

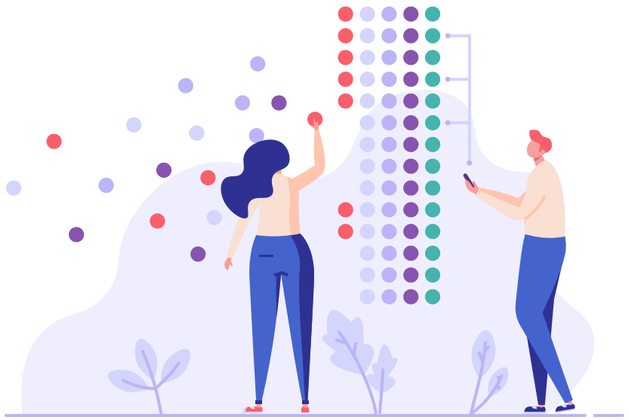
Identifies the data's value to the organization

It is a continuous process, not a one-time effort.

Need for Data Classification

The importance of data classification are as follows:

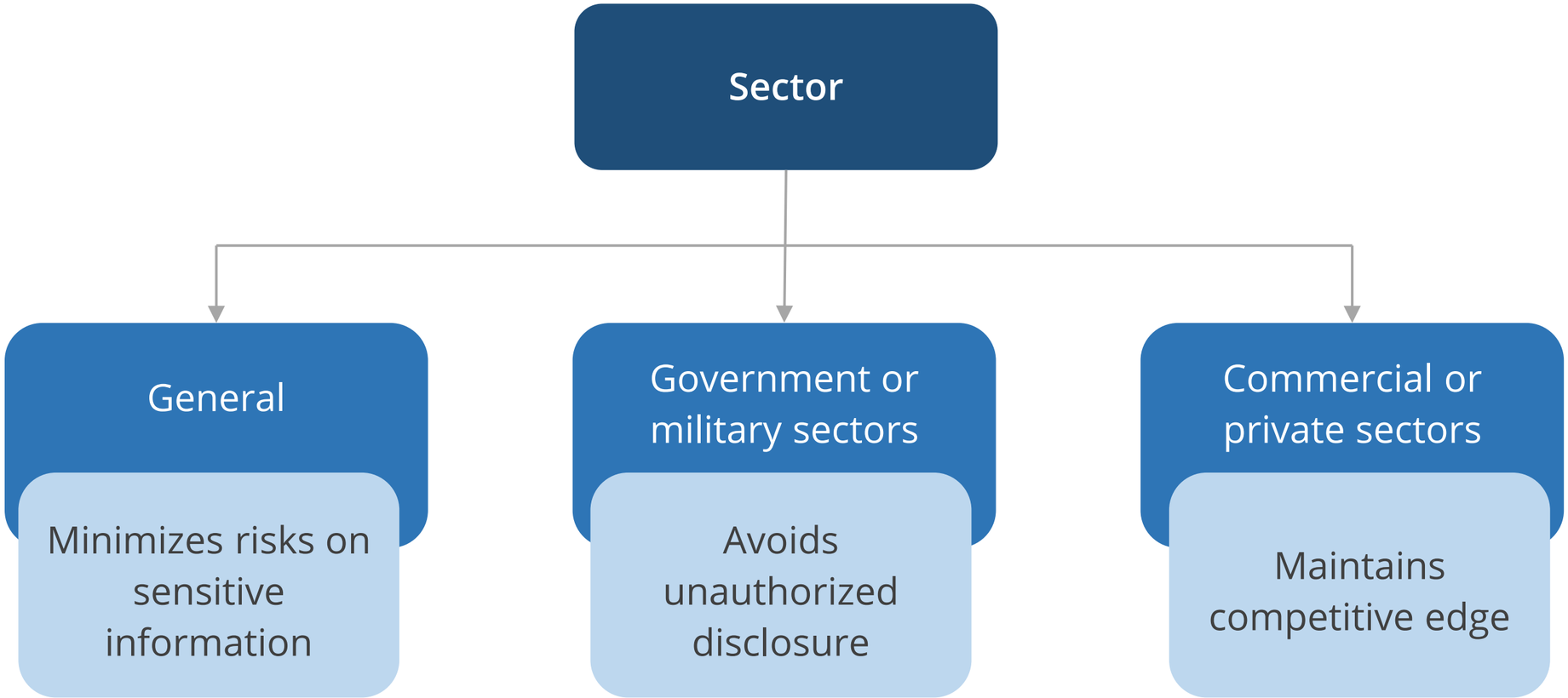
- Recognizes the value of data for strategic decision-making
- Mitigates the risk of significant problems from data loss
- Enhances the confidentiality, integrity, and availability of information



- Implements controls based on information sensitivity
- Standardizes information types and protection requirements
- Achieves an efficient cost-to-benefit ratio

Information Classification Objectives

It varies from sector to sector. The following are the objectives of each sector:



Information Classification Objectives: General Sector

It refers to non-specific or broad categories of information handling across various industries or public entities.

Below are the key classification of the general sector:

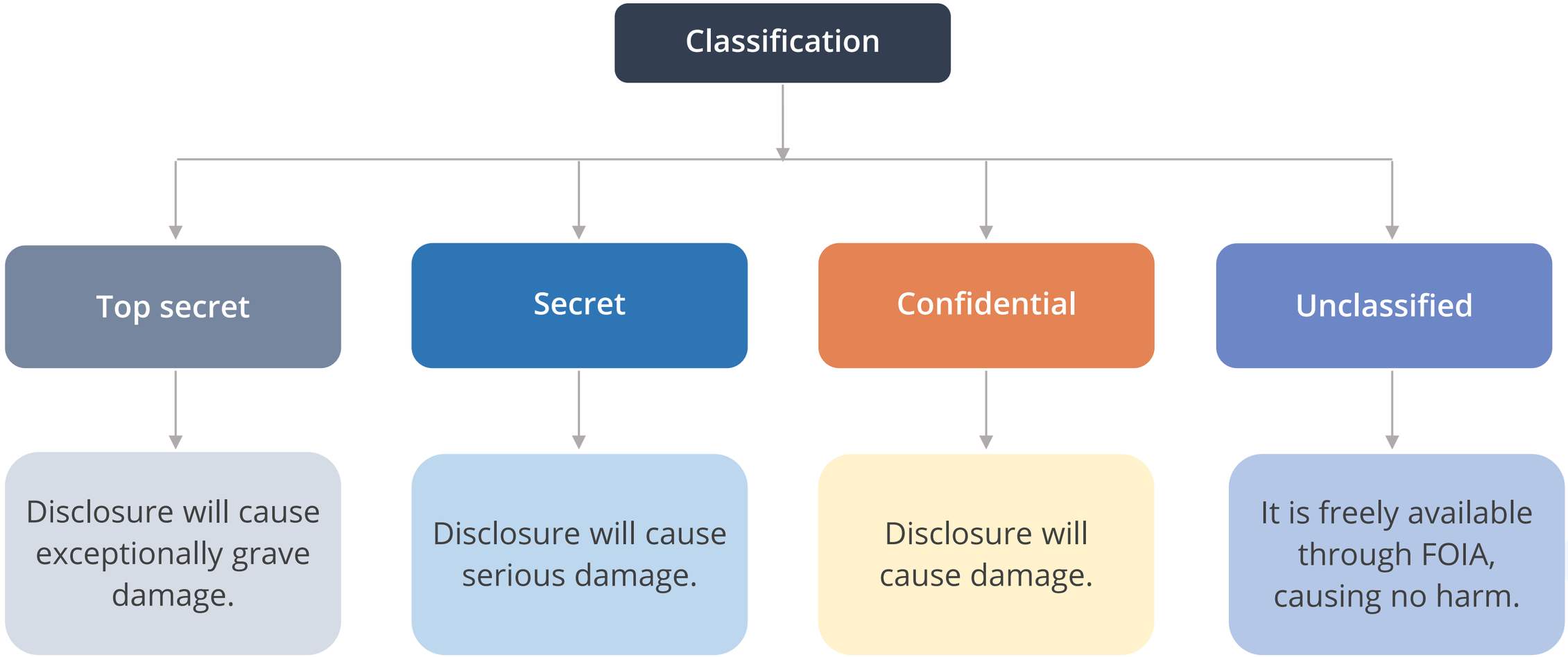
Sensitive information protection: Focuses on minimizing risks to sensitive data like personal, financial, or health information

Basic security protocols: Employs encryption, access control, and audits to safeguard data from breaches or unauthorized access

Information categorization: Classifies data from low to high sensitivity, ensuring appropriate handling and protection for each category

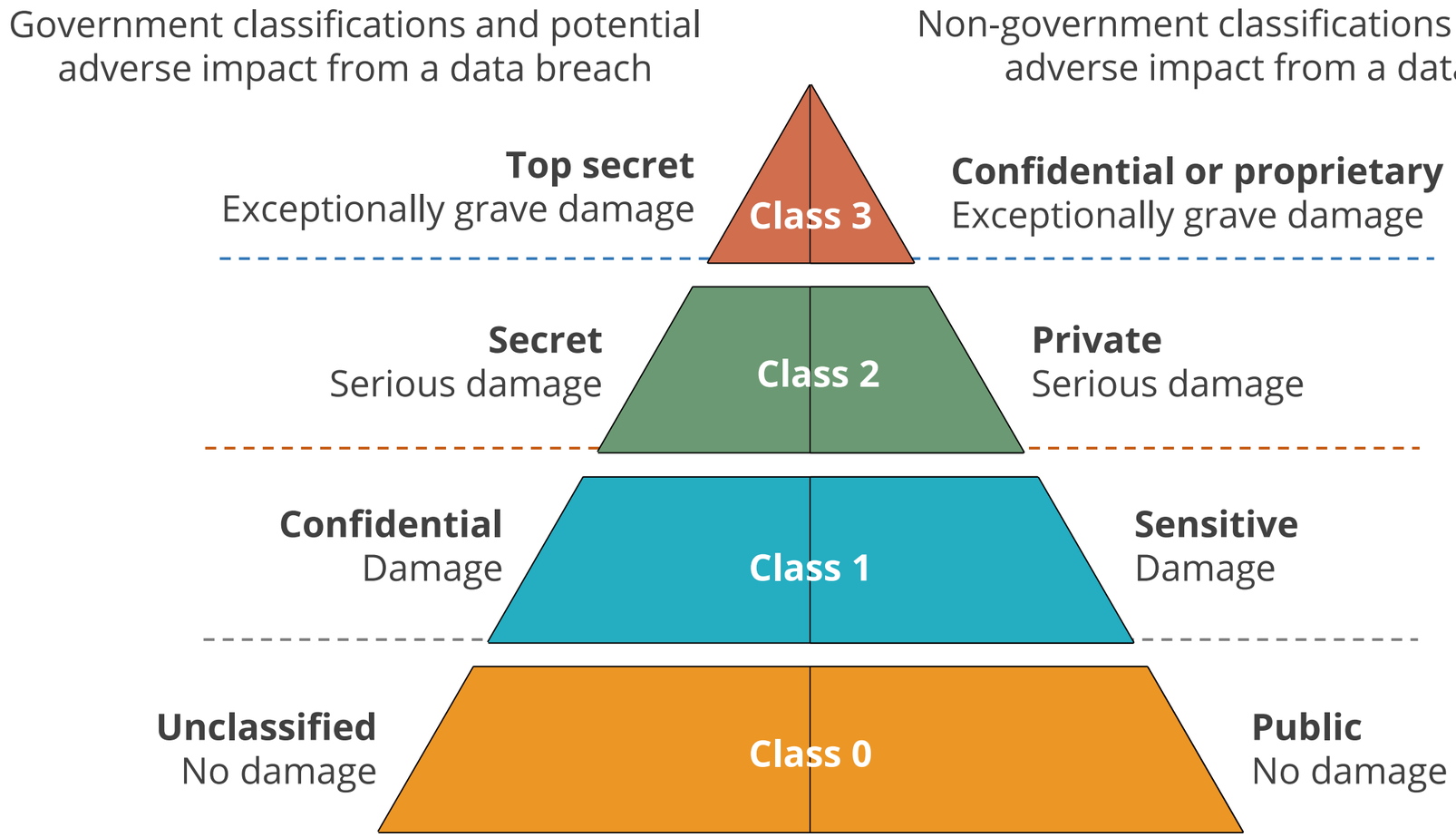
Information Classification: Government Sector

The chart below illustrates various classifications of the government sector and the potential damage from data disclosure.



Information Classification: Commercial or Private Sector

The following image illustrates the damage caused to government and non-government sectors in the case of a potential data breach:

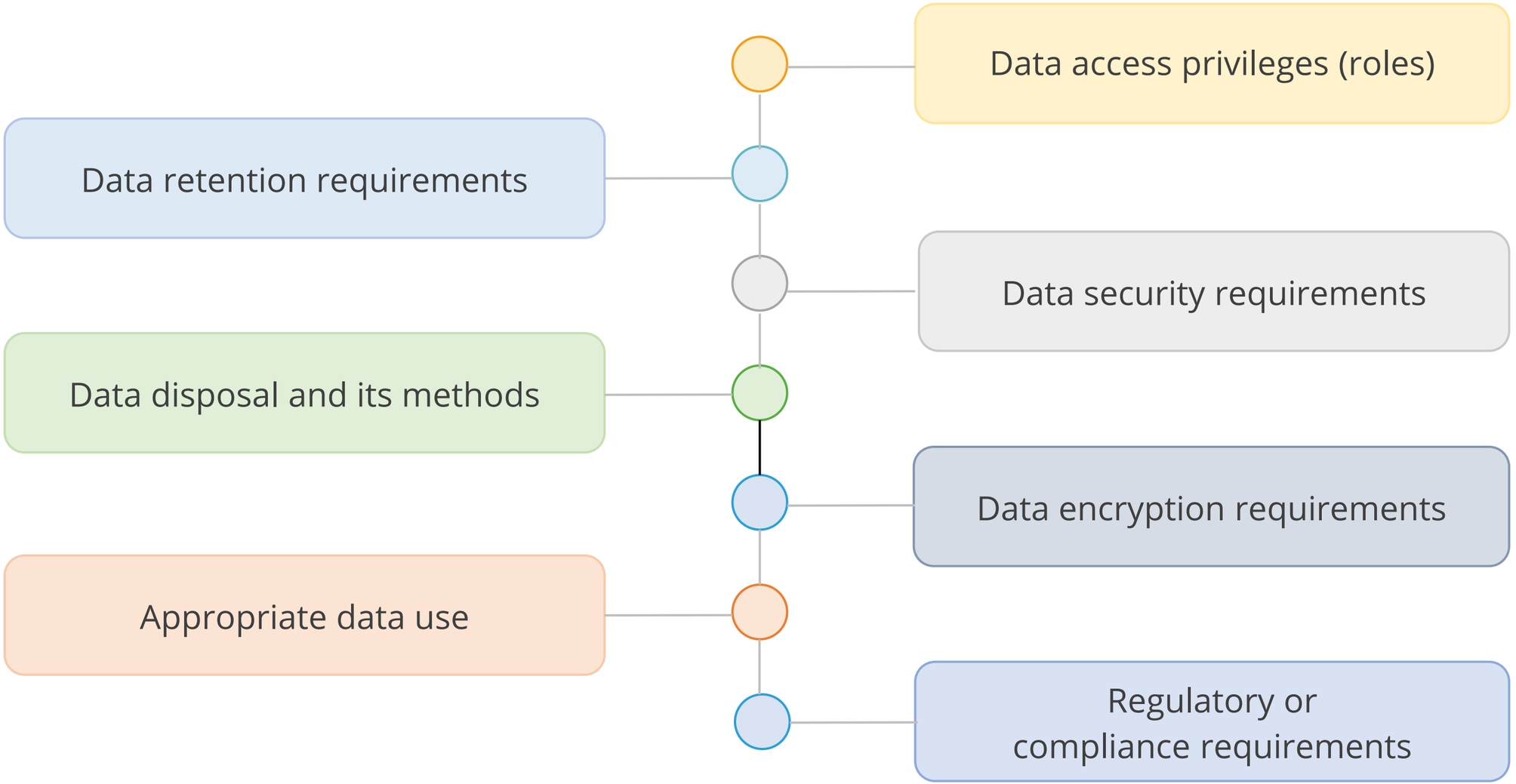


Information Classification: Commercial or Private Sector

This sector uses the following four-level information classification scheme:

Data Classification Considerations

When classifying data, a security practitioner considers the following:



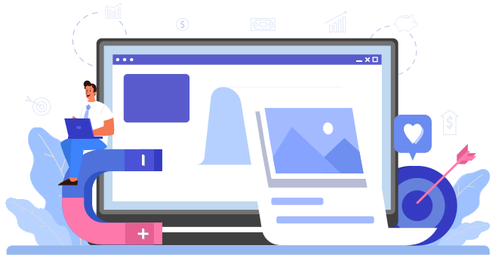
Role Responsible for Data Classification

Data owner

They are responsible for data classification to:

- Understand the data's use and value to the organization
- Review the data classification annually

Role Responsible for Data Classification

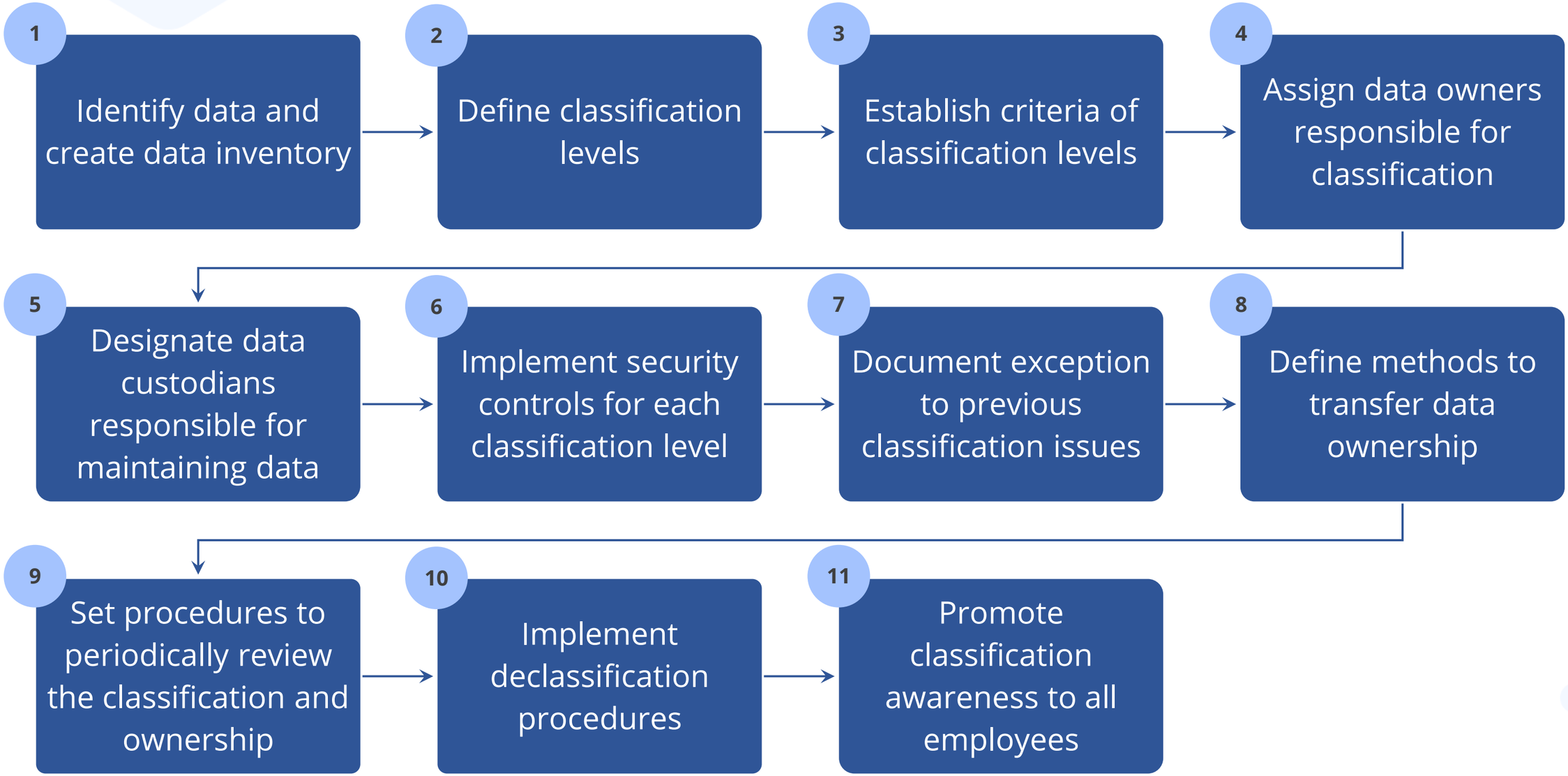


Organization

The responsibilities of the organization include:

- Documenting deviations and implementing corrective actions
- Retaining data according to the organization's policy and securely destroying it when no longer required

Data Classification Procedure



Quick Check

A new project team is tasked with securing sensitive company data. What is the primary goal of classifying this data?

A. Identify data owners

B. Identify data custodians

C. Determine information criticality

D. Identify the appropriate level of protection needs

Establishing Data Protection Measures

Data Policy

It is a dynamic and flexible high-level document created by senior management outlining the organization’s strategic long-term data management goals.

It guides the framework for data management and addresses issues related to:

- Data access
- Legal matters
- Custodian duties
- Data acquisition
- Data handling

Data Policy

The elements to be considered during data policy creation are:

Data privacy

Ownership of data

Cost

Sensitivity and criticality of data

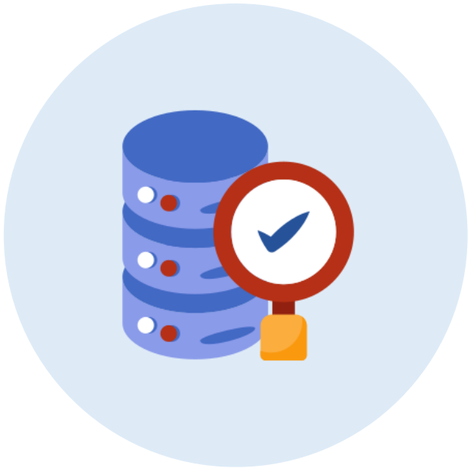
Policies and processes

Laws and regulations

Liability

Data Quality

It is defined as the fitness of data to serve its purpose in a given context.



It is determined by factors such as accuracy, completeness, reliability, relevance, and how up-to-date the data is.

The usefulness and applicability of data significantly decrease if its quality is compromised.

Data Quality

The principles of data quality are applied throughout the data management process, including:

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

Data Sensitivity and Criticality

Sensitivity

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

Criticality

A measure of the impact system failure may have on the organization

Data Criticality Categorization

The University of Delaware has defined the following three categories to assess data criticality:

Categories	Impact of issues
Non-critical	• It 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.

Source: https://www1.udel.edu/security/data/criticality.html

Data Criticality Categorization

Categories	Impact of issues
Critical	• It is important for the University's ability to operate. • Loss of integrity or availability would have a **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.

Source: https://www1.udel.edu/security/data/criticality.html

Data Criticality Categorization

Categories	Impact of issues
Mission critical	• It 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.

Source: https://www1.udel.edu/security/data/criticality.html

Data Breach

It is a security incident in which information is accessed without authorization.

Impact

Harms businesses and consumers by causing significant costs, damaging reputations, and requiring time to repair

Common exposures

Personal information such as credit card numbers, social security numbers, and healthcare records

A key goal of managing sensitive data is to prevent data breaches.

Causes of Data Breach

1. Criminal hacking
2. Human error
3. Social engineering
4. Malware
5. Unauthorized use
6. Physical action

Managing or Protecting Sensitive Data

Protecting sensitive data is crucial to prevent:

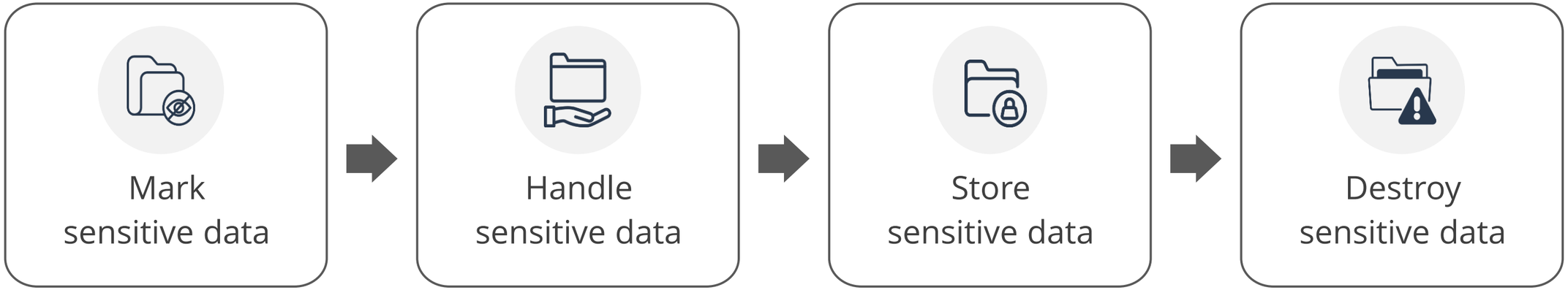
Identity theft

Financial loss

Reputational damage

Managing or Protecting Sensitive Data

Proper handling of data is essential to minimize data breaches. Here are the steps to handle data correctly:



Marking Data

It (often called labelling) is the process of marking sensitive information to indicate its classification level.

When users understand the data's value, they are more likely to take appropriate measures to control and protect it according to its classification.

Types of Labels

Physical label

- It indicates the security classification for the data stored on media or processed on a system.
- The computer or system should have a label indicating the highest classification of information that it processes.
- It remains on the system or media throughout its lifetime.

Digital label

- It is labeled using digital marks or labels.
- A simple method is to include the classification as a header and/or footer in a document or embed it as a watermark.
- A benefit of these methods is that they also appear on printouts.

Data Handling

It refers to the secure transportation of media throughout its lifetime.

Data is managed based on its classification, with highly classified information needing stricter protection.

Policies must ensure systems and media are properly labeled and handled accordingly.

Securing Data

The following are essential strategies for protecting sensitive data across various areas of security:

Digital protection

- Store sensitive data securely to prevent any loss
- Encrypt data as the primary method of protection
- Use AES 256 for strong encryption
- Choose applications that support AES 256 encryption

Physical security

- Follow basic physical security practices for storing sensitive data on physical media
- Store portable disk drives or backup tapes in locked safes or vaults
- Secure these devices within a room that includes additional physical controls

Environmental security

- Implement environmental controls to protect sensitive media
- Use temperature and humidity controls like HVAC (Heating, Ventilation, and Air Conditioning) systems

Collaborative Data, Asset, and Configuration Management

Data Ownership

An information or data owner is an individual or group responsible for creating, acquiring, purchasing, and managing information.

Data Ownership

The responsibilities of a data owner are as follows:

- Assessing the impact of information on the organization's mission and goals
- Estimating the cost of replacing the information
- Understanding internal and external requirements
- Identifying and destroying information at the end of its life cycle

Data User

It 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 user include:

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

Data user

Data Custodian

They are responsible for the safe custody, storage, and transportation of data, implementing the business rules, the technical environment, and database structure.

Data Custodian

The responsibilities of a data custodian are as follows:

Ensure data is backed up according to standard procedures

Restrict access to authorized personnel only

Assign data stewards for each dataset

Maintain data integrity throughout technical processes

Implement security controls to protect data

Audit data content and track changes regularly

Asset Inventory

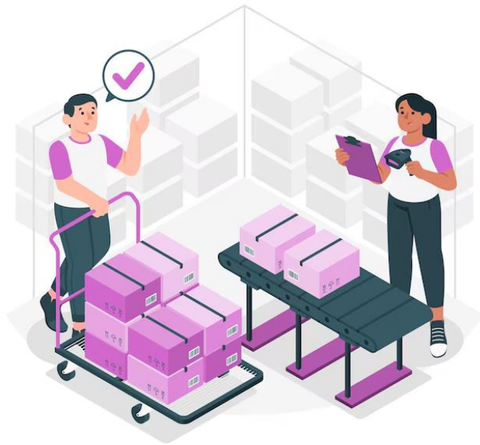
The first step in the asset classification process is to prepare an **asset inventory** and determine the location of the assets.

An **asset owner** is responsible for the day-to-day management of an asset, including 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.

Asset Management

The following are the two aspects of asset management:



Inventory management

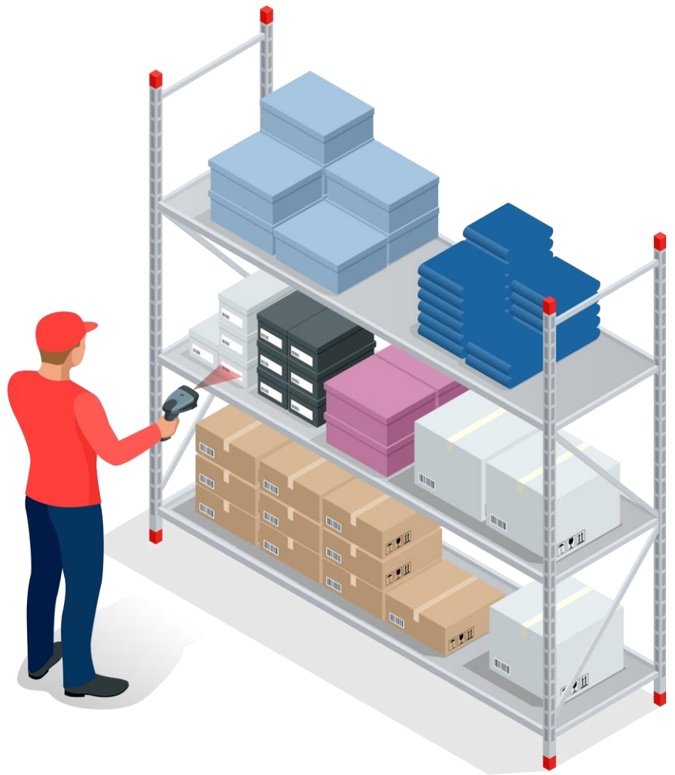
Configuration management

Inventory Management

It involves capturing asset details, locations, and owners. IT assets can be both software and hardware.

IT asset management (ITAM)

It integrates financial, inventory, and contractual functions to support IT asset life cycle management and strategic decision-making.



Configuration Management

It systematically handles changes to maintain asset or system integrity over time using appropriate policies, procedures, techniques, and tools.

Configuration management database (CMDB)

It stores information on IT system components used in an organization and the relationships between these components.

Backlog Management

It involves managing the information life cycle by developing and executing architectures, policies, procedures, and practices.

The activities range from the administrative to the technical aspects of data handling.

Data Management

It involves collecting, organizing, storing, and protecting data to ensure its:

Quality

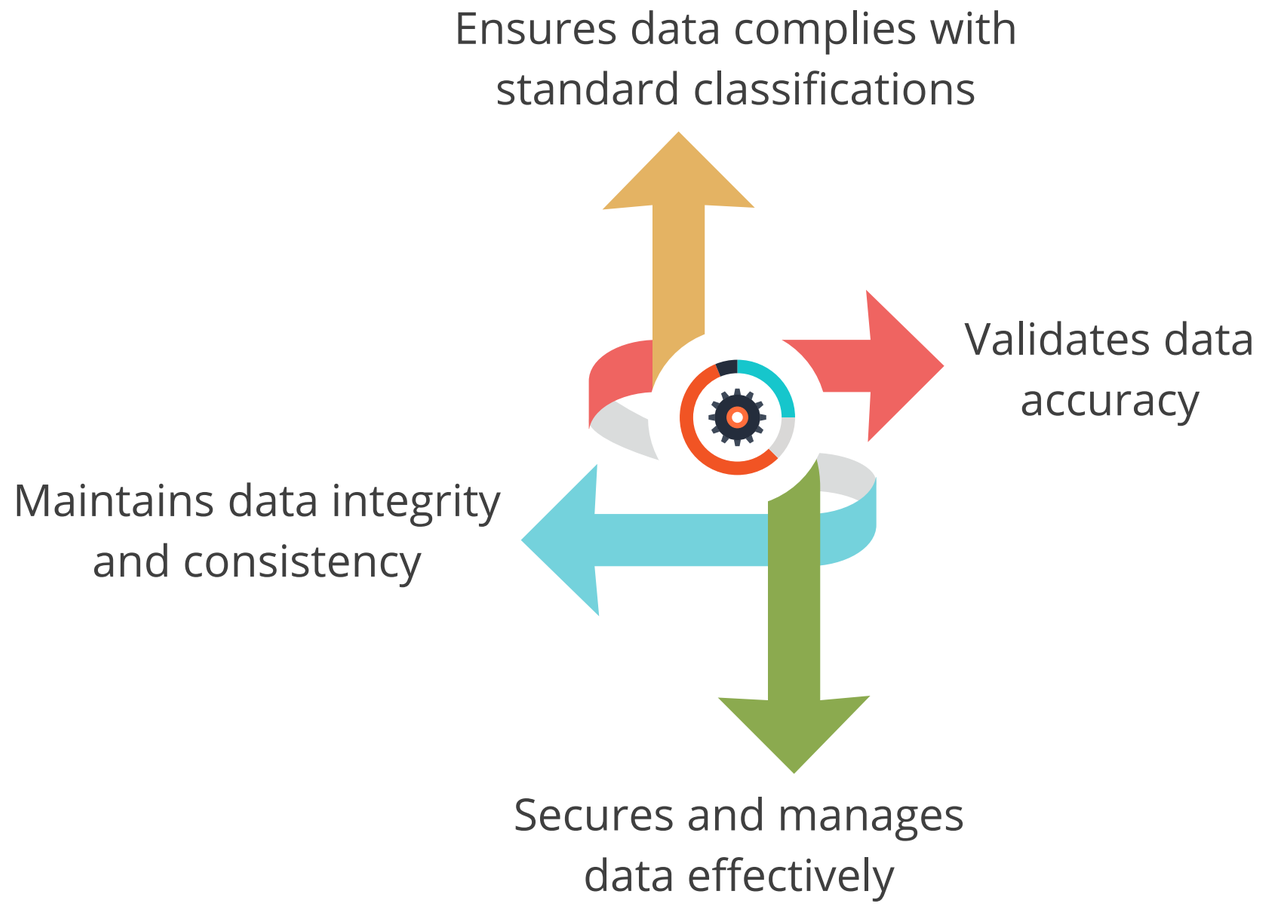
Accessibility

Security

It helps organizations make informed decisions, improve efficiency, and gain valuable insights.

Data Management

The following are the importance of data management:



Quick Check

You are a data custodian for a company, responsible for managing and protecting data. Which of the following tasks falls outside your role?

A. Safe custody

B. Intellectual property rights

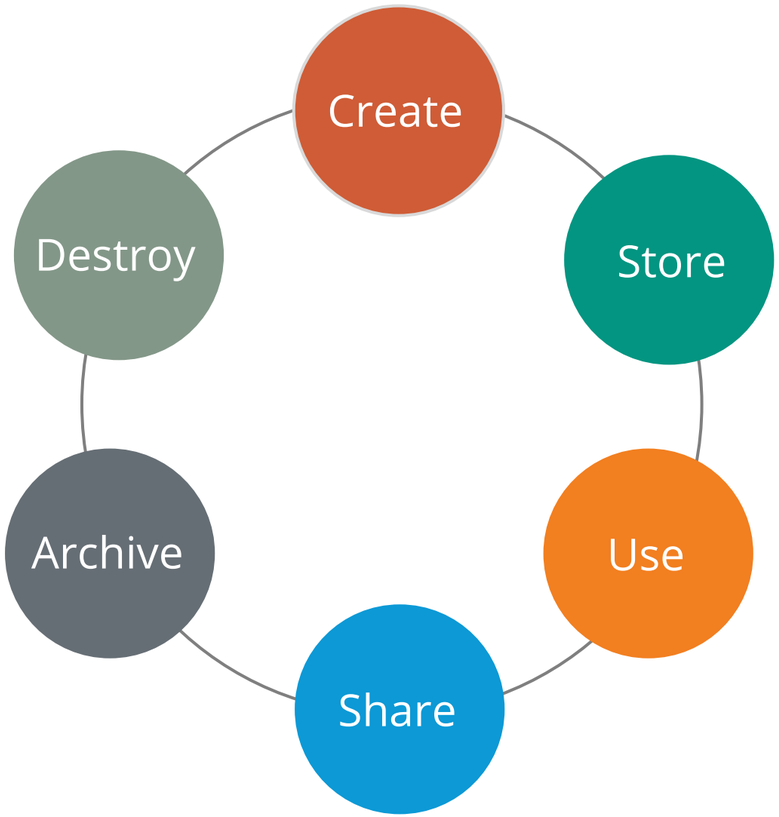
C. Transport of data

D. Storage

Overview of Data Life Cycle

Data Life Cycle

It refers to the stages that data goes through from its creation to its eventual deletion or archiving.
Here are the key stages of the data life cycle:



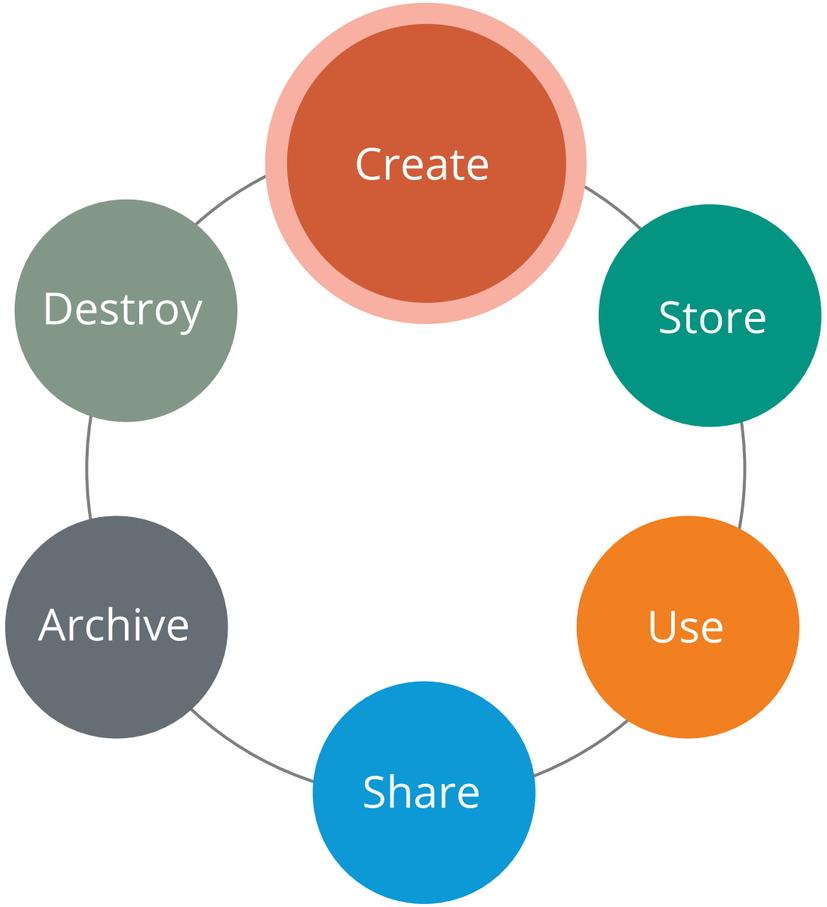
Its understanding is crucial for effective data management, governance, and compliance.

Data Life Cycle: Create

This phase involves generating or acquiring new digital content or altering or updating existing content.

- **Data created remotely:**
  Encrypt data before uploading to the server to protect against vulnerabilities like man-in-the-middle attacks

- **Data created in server:**
  Encrypt data immediately upon creation during remote manipulation



Data Collection

It is done during the create phase. To ensure compliance with privacy laws, it must adhere to the following principles:

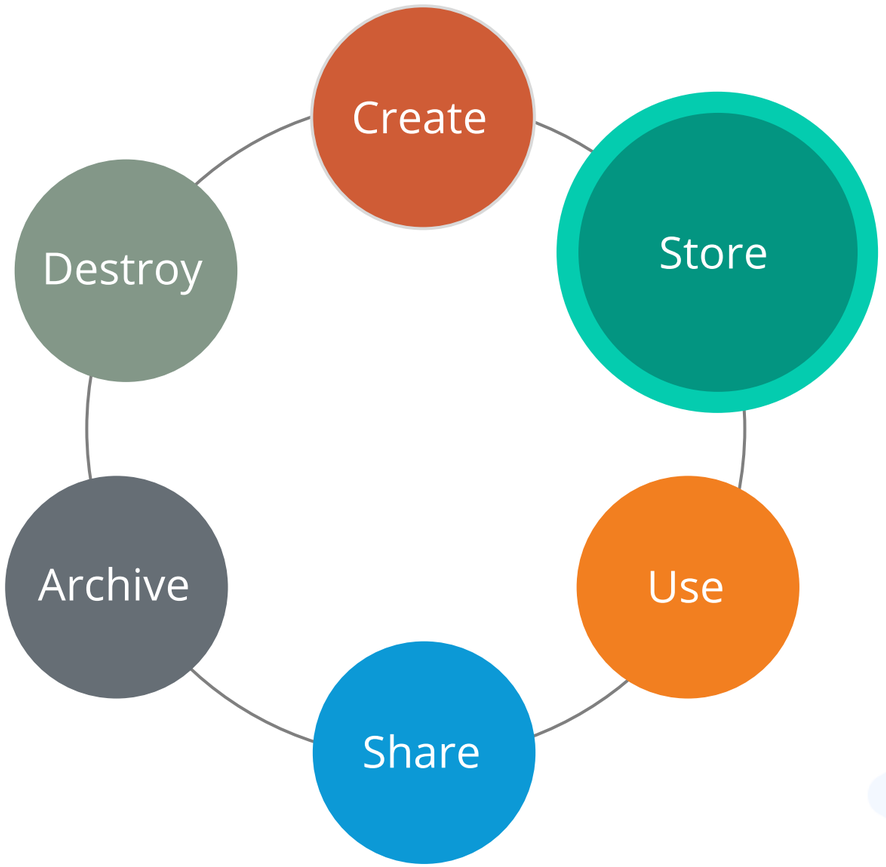
- Collect personal data only if it is relevant to the intended purpose
- Obtain data through lawful and fair means
- Specify the purpose for collecting personal data at the time of collection
- Use collected data solely for the purposes specified at the time of collection
- Obtain explicit consent from data subjects for the collection and use of their data

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

Data Life Cycle: Store

The following are the ways to ensure data security while storing it:

- **Store immediately:** Save digital data as soon as it is created
- **Implement controls:** Encrypt data, define access policies, monitor usage, log activities, and ensure backups
- **Protect content:** Secure data against attackers by properly configuring access control lists (ACLs), scanning files for threats, and accurately classifying data



Data Storage Location

Transferring personal data across borders can be contentious under global data protection laws.

Understanding the distinctions between data residency, data sovereignty, and data localization is crucial.

Data residency

Refers to the chosen geographic location where a business stores its data, often for regulatory, tax, or policy reasons

Data sovereignty

Indicates that data stored in a specific location is subject to the laws of that country

Data localization

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 that allows federal law enforcement to compel US-based technologies company, via subpoena or a warrant, to provide trans-border access to data, regardless of whether the data is stored in the United States or on foreign soil.

The various aspects of this act include:

- It is generated from the United States vs. Microsoft case, where the FBI issued a warrant for emails stored on Microsoft's Ireland servers.
- It does not supersede or change the local laws of another country.
- It provides additional safeguards for companies or courts to challenge requests conflicting with data privacy rights.
- Potential conflict between the CLOUD Act and GDPR, if a US citizen is in the European Union, is subject to a CLOUD Act warrant.

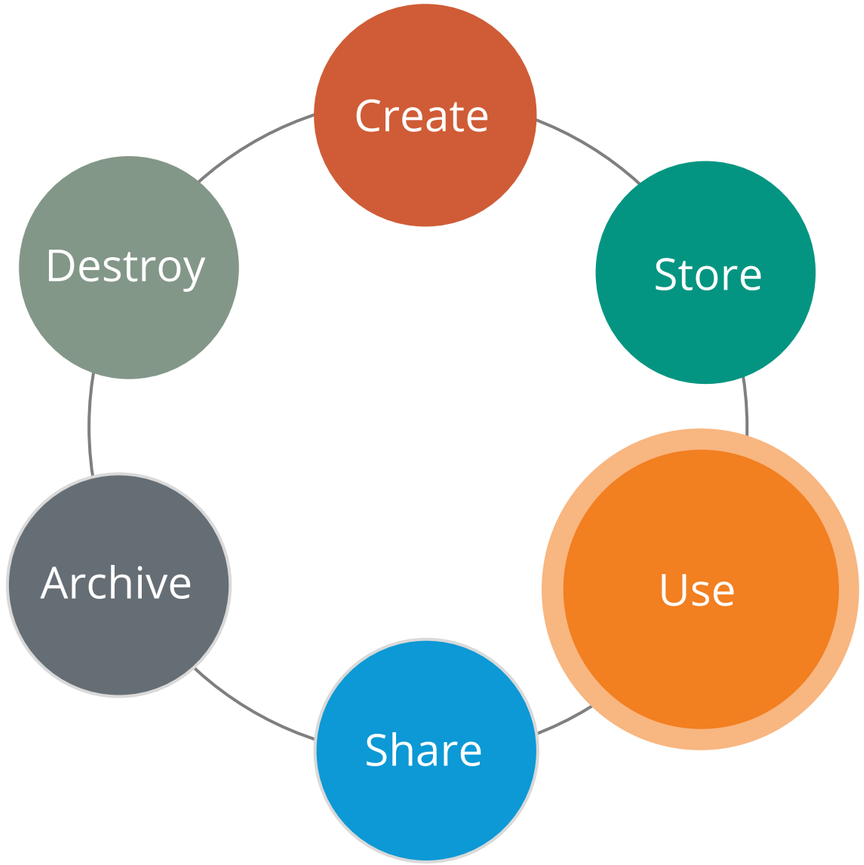
Source: https://en.wikipedia.org/wiki/CLOUD_Act

Data Life Cycle: Use

Data is most vulnerable when in use, as it may be transported to unsecured locations, like workstations, where it must be unencrypted for processing.

Key controls for protecting data in use are as follows:

- Implement data loss prevention (DLP)
- Apply information rights management (IRM)
- Use database and file access monitors

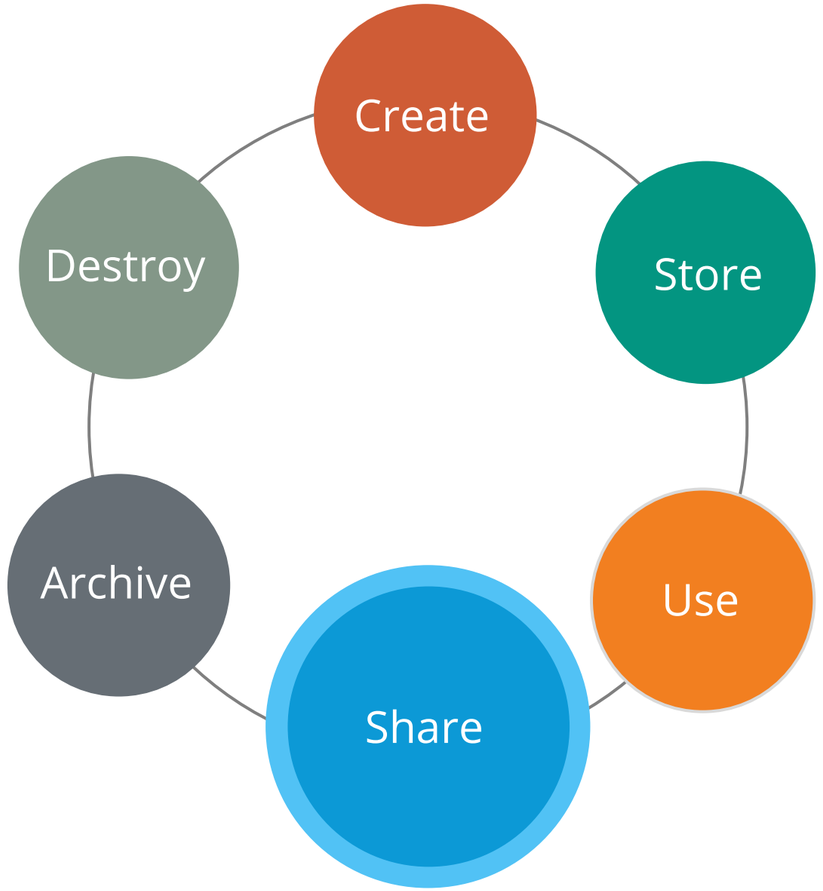


Data Life Cycle: Share

Data exchanged with users, customers, and partners can be challenging to secure once shared, as it is no longer under the organization's control.

Key measures for securing shared data are as follows:

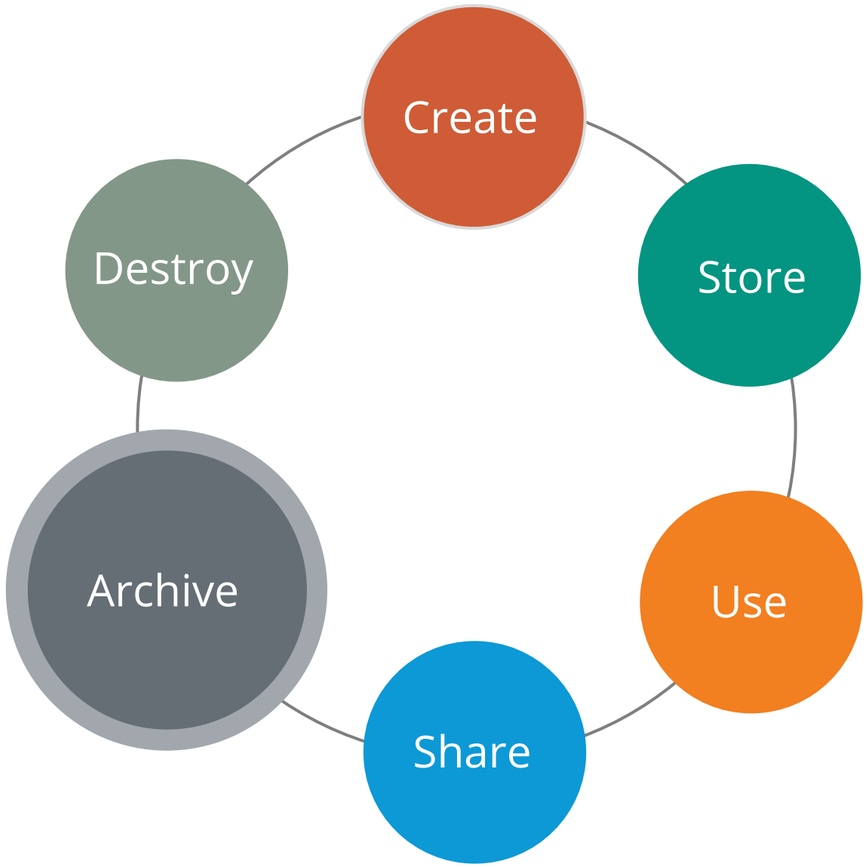
- Detect unauthorized data sharing
- Implement information rights management (IRM) to maintain control over shared information



Data Life Cycle: Archive

It is the process of identifying and moving inactive data from current production systems to specialized long-term 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 it be ensured that backups can and will work when needed?



Data Retention

It involves retaining and managing data for a specified period along with the methods used to accomplish these tasks.

A data retention policy balances the legal, regulatory, and business data archival requirements against data storage costs, complexity, and other data considerations.

Data Retention: Steps

The following are the 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
- Regularly audit practices for record retention and destruction
- Review the retention policy periodically
- Maintain the documentation of the policy, its implementation, training, and audits as the best practice

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

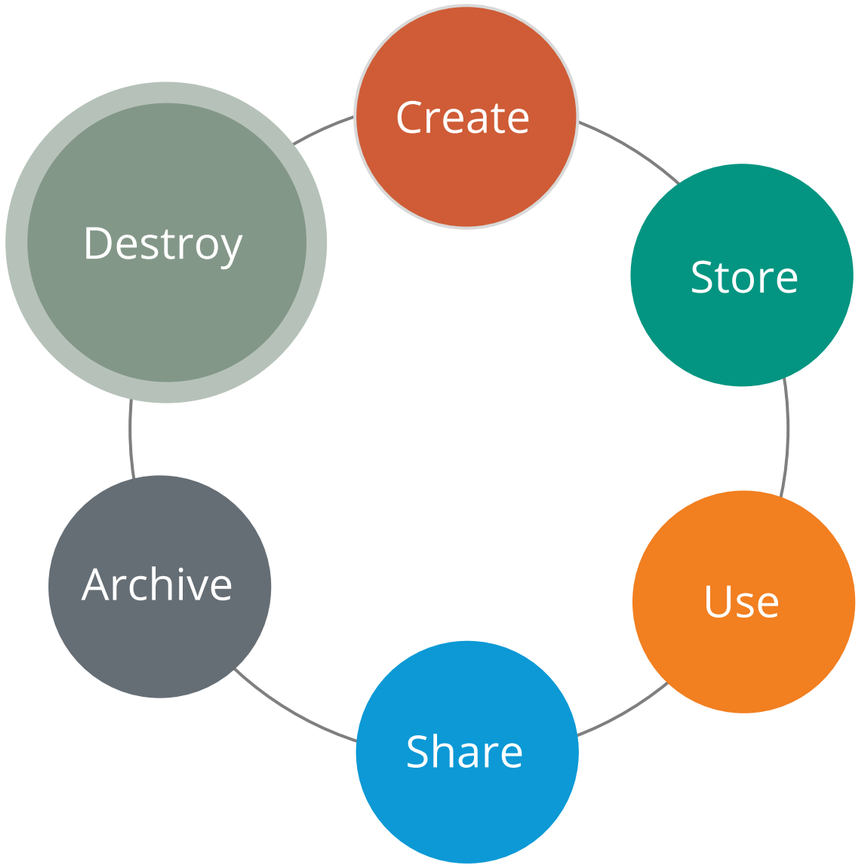
A magnetic drive is used to archive an organization's data.

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

In this phase, data is permanently destroyed using physical or digital means such as crypto shredding. This phase also involves:

- Erasing pointers logically or destroying the data
- Ensuring compliance with relevant regulations regarding data destruction

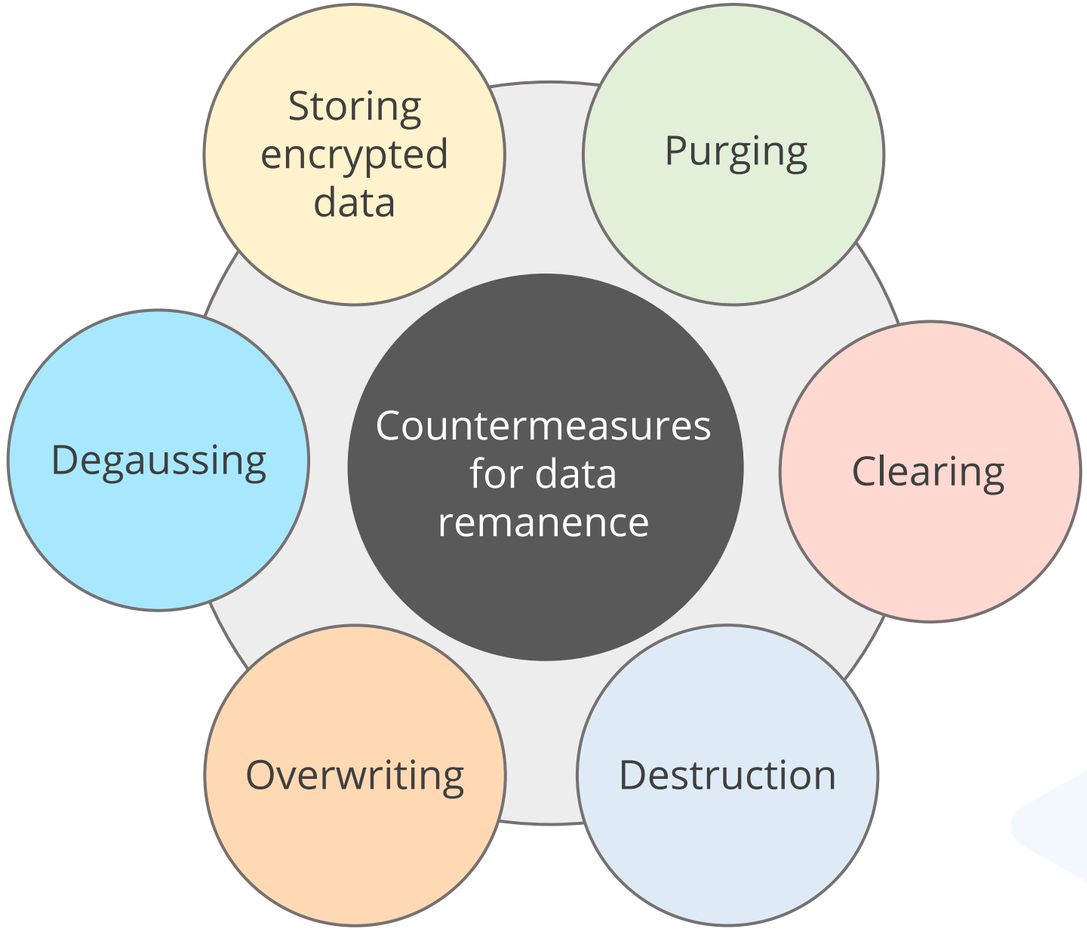


Data Remanence

It is the residual representation of digital data that persists even after attempts to erase or remove it.

Managing data remanence:

- Recognize that data remanence can persist on hard disk drives (HDDs) if data wiping methods fail
- Familiarize with various storage technologies to effectively manage data remanence issues



Data Remanence: Cold Boot Attack

It is a security vulnerability that exploits the residual data left in memory (RAM) after a computer is powered off.

They are typically 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.

A **password reset attack** is a similar attack that performs a forced reset without fully powering off the system.

Data Destruction

Data can be destroyed in the following five ways:

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

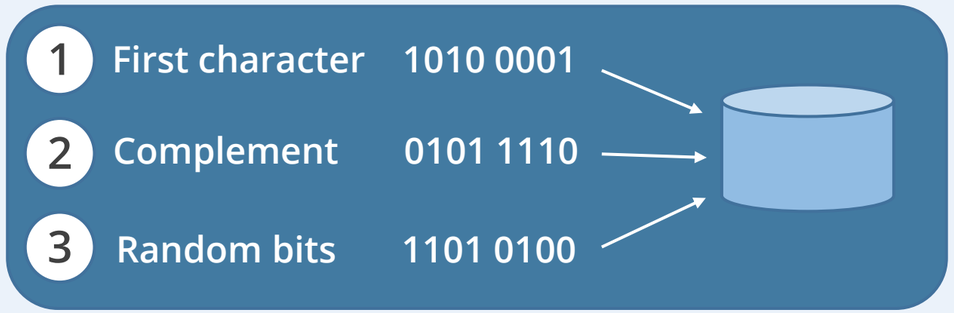
- It is a simple deletion process that removes only the catalog reference, leaving the files intact.
- This method is not suitable for data destruction, as it can be easily recovered using widely available tools.

Data Destruction

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

- It is the process of preparing media for reuse by ensuring that cleared data cannot be retrieved using traditional recovery methods.
- Unclassified data is written over all the addressable locations on the media.
- Data recovery requires special laboratory techniques.
- It is used when preparing media for reuse at the same classification level.

The following image illustrates the clearing process:



Data Destruction

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

- It represents a more intense form of clearing, involving multiple repetitions to ensure thorough data removal.
- It combines with degaussing to completely remove data and ensure that it cannot be recovered using any known means.
- It is used when preparing media for reuse at a lower classification level.

Data Destruction

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

- It combines processes to ensure data is completely removed from the system and guarantees that it cannot be recovered by any means.
- This includes erasing non-volatile memory, removing external drives, and sanitizing them to destroy data.

Data Destruction

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

- It generates heavy magnetic fields to realign the magnetic fields in magnetic media, making it effective only on magnetic media and not affecting CD, DVD, or SSD.

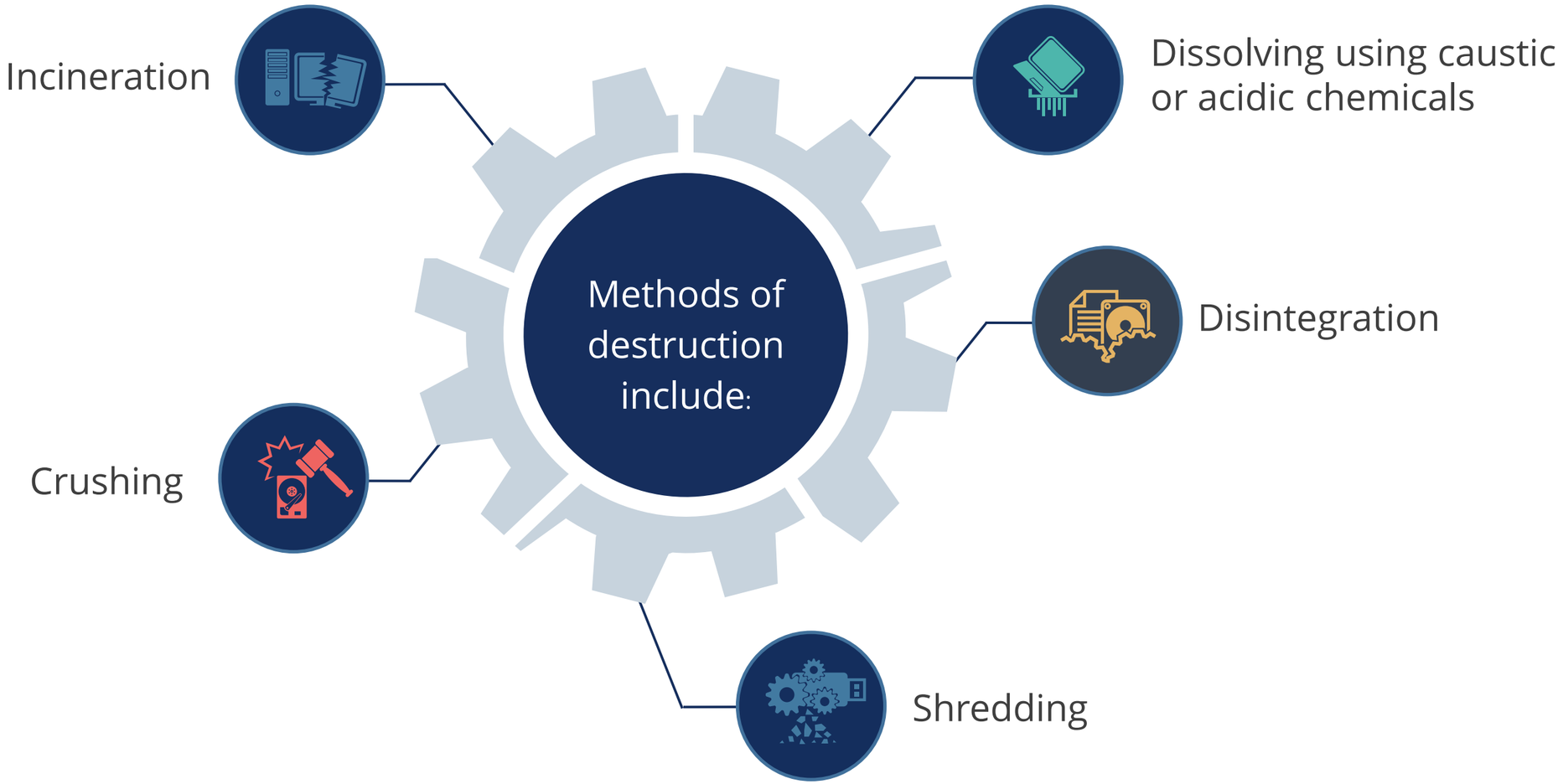
- Degaussing techniques for magnetic media include:
  - AC erasure: Degausses the medium by applying an alternating field with gradually reduced amplitude
  - DC erasure: Saturates the medium by applying a unidirectional field

Physical 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.

Physical Data Destruction Methods

There are five methods for physically destroying data. They are as follows:



Quick Check

A company outsources payroll services to a third-party company. Which of the following roles most likely applies to the third-party payroll company?

A. Data owner

B. Data controller

C. Data processor

D. Data handler

Ensuring Appropriate Asset Retention

Asset Retention

It is the process of managing and securing physical and digital assets for a set time, ensuring proper handling and access.

Asset Retention

Appropriate asset retention requires the maintenance of end-of-life (EOL) and end-of-support (EOS).

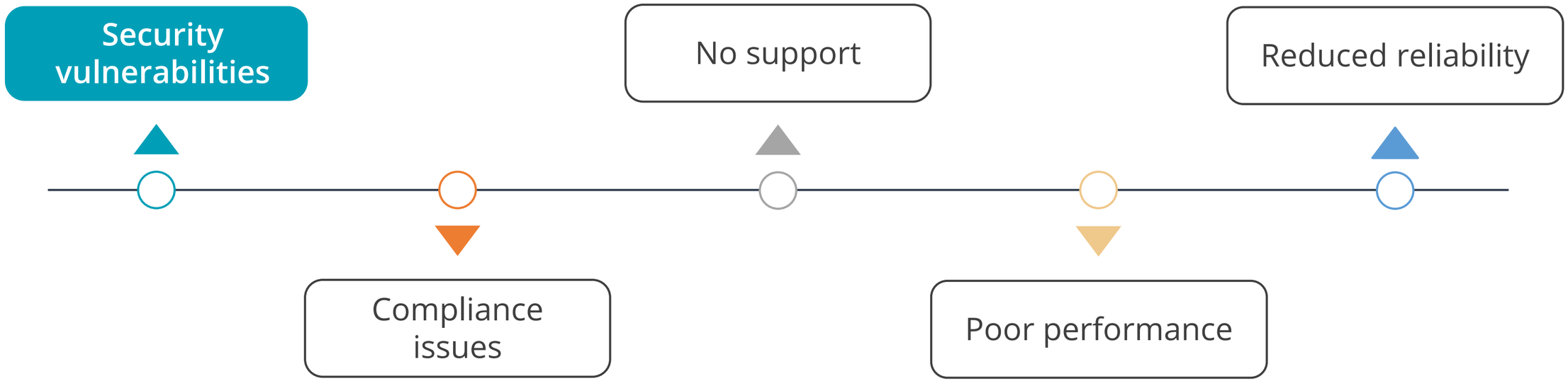
End-of-life (EOL)

- In this, a vendor ceases manufacturing a product and stops taking orders for it, though support may still be available from the manufacturer or third parties.
- This phase is also sometimes referred to as **end of sale**.

End-of-support (EOS)

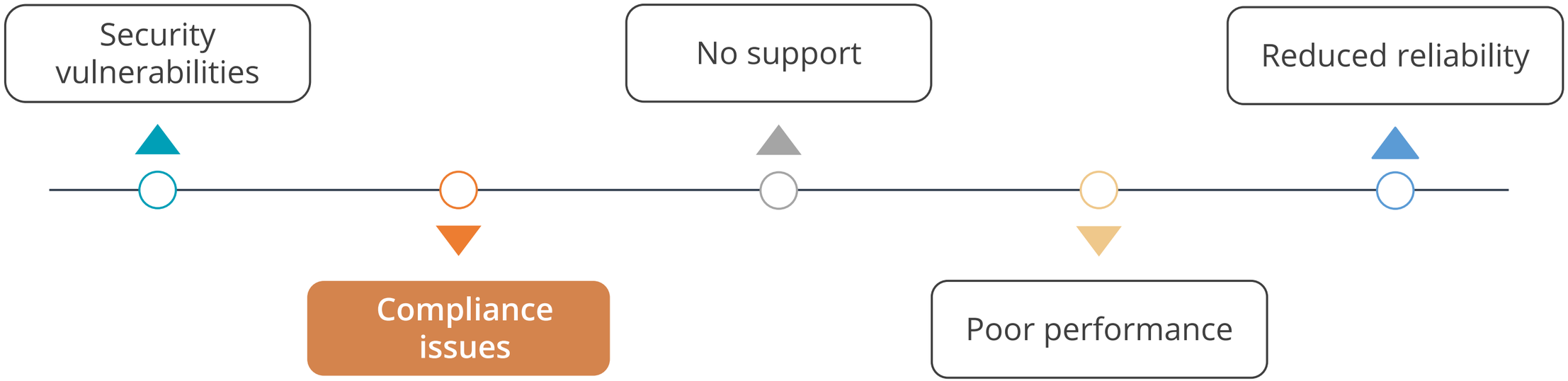
- In this, a vendor no longer provides any form of support for a product, including security updates, technical support, or content updates.
- Once a product reaches EOS, it is no longer maintained by the manufacturer.

Potential Risk of EOL/EOS Systems



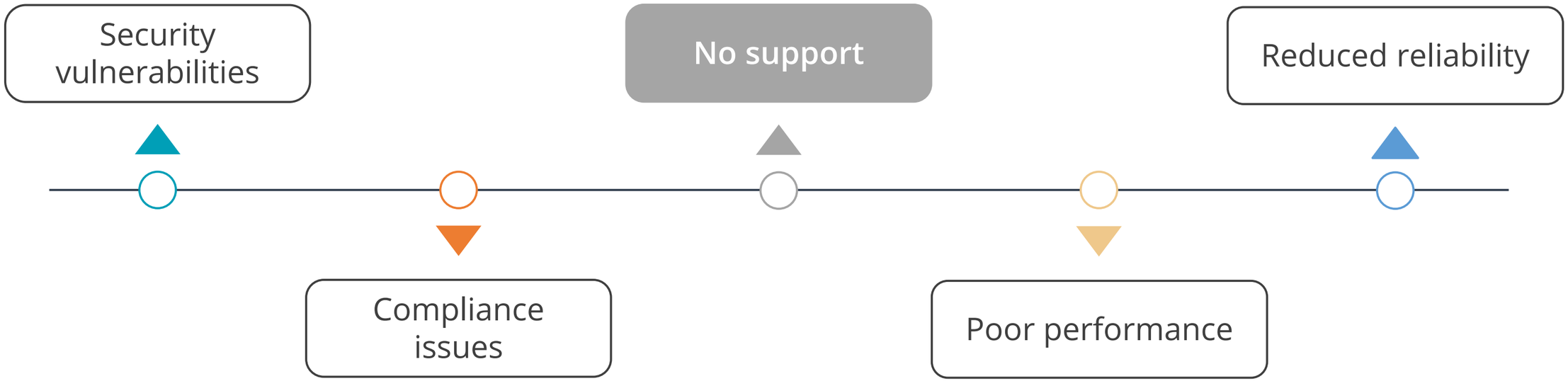
- When a vendor stops issuing security patches, systems become vulnerable to attacks.
- Firewalls and anti-malware systems cannot protect against unpatchable vulnerabilities, leaving them exposed to exploitation by hackers.

Potential Risk of EOL/EOS Systems



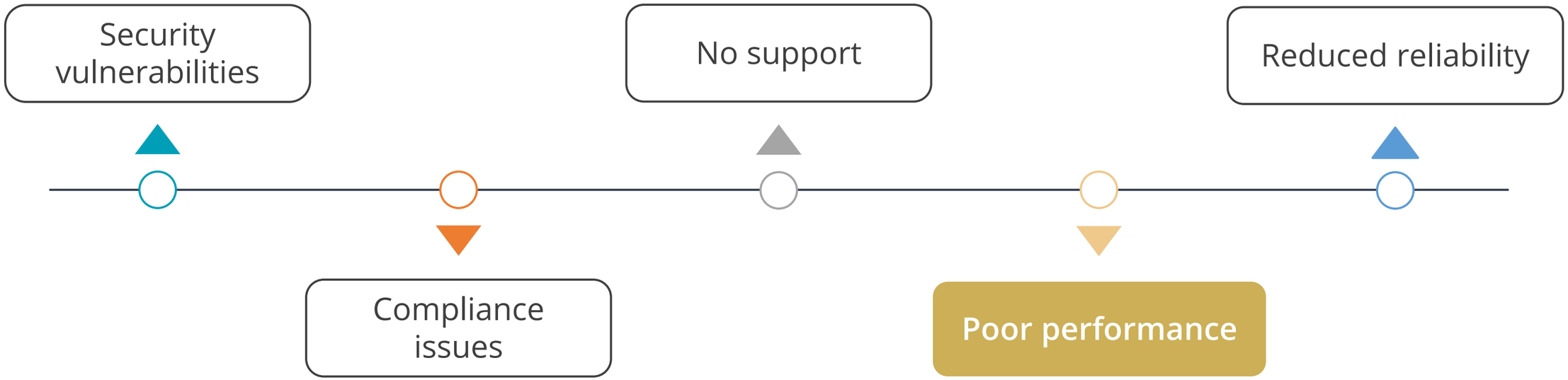
Regulated industries like healthcare and finance, which deals with sensitive data, may prohibit the use of EOL systems.

Potential Risk of EOL/EOS Systems



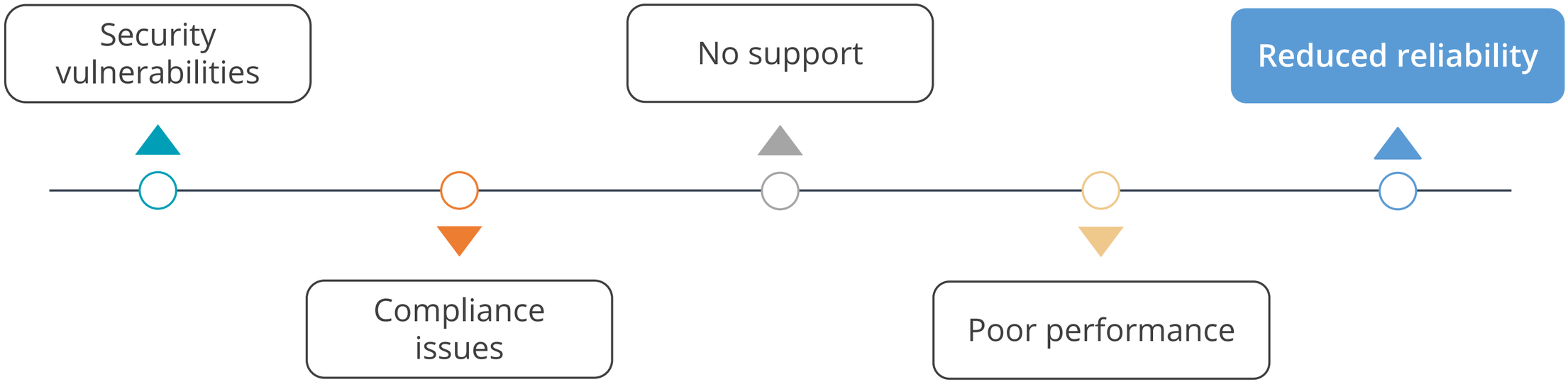
With the vendor no longer providing support, there is no official way to troubleshoot or resolve system issues if they arise.

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.

Quick Check

The company that Katie works for provides its staff with cell phones for employee use, with new phones issued every two years. What scenario best describes this type of practice when the phones are still usable and receiving operating system updates?

A. EOL

B. Planned obsolescence

C. EOS

D. Device risk management

Determine Data Security Controls

States of Data

The three states of data represents how and where data is stored, transferred, or processed.

Data at rest

- It refers to any data stored on media, such as system hard drives, external USB drives, storage area networks (SANs), and backup tapes.

Data in transit or data in motion

- It involves data transmitted over a network.
- It includes data sent over internal networks, whether wired or wireless, as well as data transmitted over public networks like the Internet.

Data in use

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

Data Security Controls

They protect sensitive data based on its state, whether stored (at rest) or transferred (in transit).

The following outlines specific controls for each state:

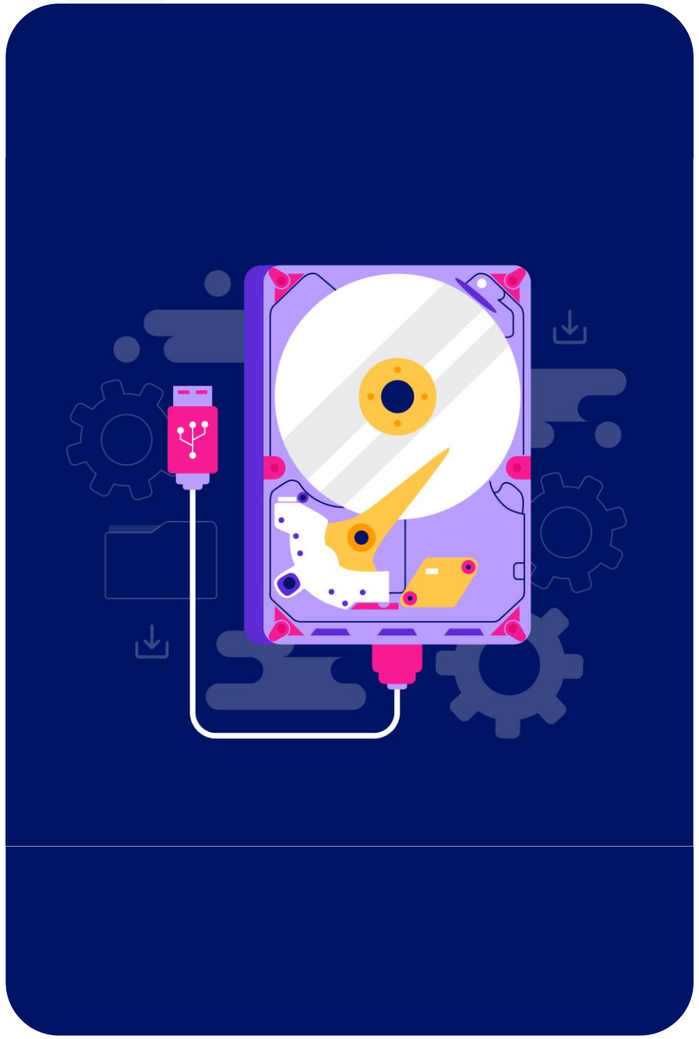
Data at rest

- **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:** Encrypts data but leaves the routing information visible
- **Link encryption:** Encrypts data as well as routing information

Data at Rest: Best Practices



- Implement full disk encryption for protecting data in hard drives
- Implement access control to control access to systems or data
- Implement hashing to protect the integrity of data
- Take regular backups of data and store one copy in at least one offsite location
- Provide users with only the minimum access necessary to perform their jobs
- Regularly review access permission to ensure that user rights are up-to-date and appropriate

Data in Transit: Best Practices

- Implement Secure Socket Layer (SSL) or Transport Layer Security (TLS) for secure communications
- Encrypt messages before transmitting emails
- Apply Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) for encryption
- Utilize end-to-end encryption for intranet communication
- Employ Internet Protocol Security (IPsec) for secure Virtual Private Network (VPN) connectivity
- Use Secure Shell (SSH) for network device administration
- Secure wireless networking with Wi-Fi Protected Access 2 (WPA2)

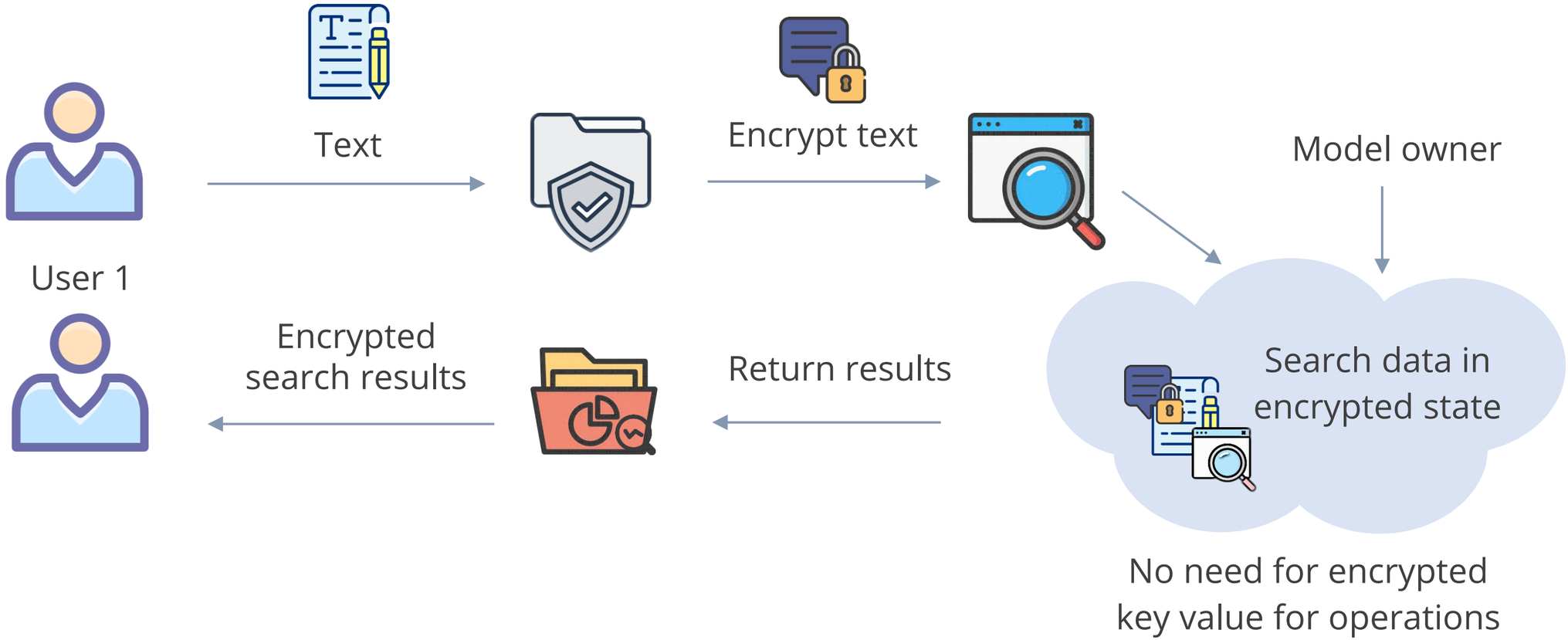
Protecting Data in Use: Homomorphic Encryption

It converts data into ciphertext that can be analyzed and manipulated as if it were in its original form.
The benefits of homomorphic encryption are:

It allows complex mathematical operations on encrypted data without compromising security.

It enables computations directly on encrypted data, improving safety for third-party data handling.

Protecting Data in Use: Homomorphic Encryption



Protecting Data in Use: Confidential Computing

It utilizes cryptography to secure data while it is being processed in a cloud environment.
Its key features include:

- Performs data decryption using a Trusted Execution Environment (TEE) only when authorized programs access the data, ensuring secure processing
- Uses TEEs as secure enclaves with strict access controls to verify authorized applications
- Prevents malware applications from accessing data, as they lack the necessary decryption keys
- Facilitates secure processing on edge devices, addressing failures in physical access controls

Scoping and Tailoring

- NIST SP 800-53 outlines security control baselines as a set of security controls.
- Since a single set of controls cannot fit all situations, organizations select a baseline and tailor it to their specific needs.

Scoping or tailoring involves adjusting this control set by adding or removing controls to achieve the appropriate level of protection.

Scoping	Tailoring
It is the process of refining general recommendations by removing elements that do not apply to a specific environment or organization.	It is the process of customizing general recommendations to fit a specific environment or organization.

Standards Selection

An organization can choose security standards or specific control sets to protect its assets and tailor them to its unique environment and needs.

Balancing the value of the asset with the cost of implementing controls is crucial.

Example

Standards like PCI DSS are mandatory for organizations handling major credit card transactions.

Security Baselining

It provides a starting point and ensures minimum security standards.

A common baseline used is imaging.

Administrators configure a single system with desired settings, capture it as an image, and deploy it to other systems, ensuring uniform security.

Post-deployment, auditing processes periodically verify that systems maintain their secure state.

Example

Microsoft group policy can periodically check and reapply settings to match the baseline.

Quick Check

Your organization is customizing its IT security guidelines to better fit its specific environment. What process would this involve?

A. Scoping and selection

B. Scoping and tailoring

C. Baselining and tailoring

D. Tailoring and selection

Privacy and Technologies

Privacy Terms

They refer to key concepts, regulations, and definitions related to data privacy and protection and are crucial for understanding how personal data is managed, shared, and safeguarded.

Personally Identifiable Information (PII)

It refers to any data that can identify or distinguish a specific individual or de-anonymize data.

Privacy Terms

Protected Health Information (PHI)

- It is any health-related information linked to an individual.
- In the United States, the Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of PHI.

Privacy Terms

Proprietary data

- It 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.

Privacy Impact Assessment (PIA)

It is conducted by organizations with access to sensitive data to evaluate how their processes impact individual privacy.

It helps identify and manage privacy risks associated with new projects, systems, and policies.

PIA Goals

The key objectives are as follows:

Ensure compliance with relevant legal, regulatory, and policy privacy requirements

Evaluate risks of privacy breaches and assess their potential impacts

Identify and implement privacy controls to mitigate unacceptable risks

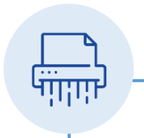
Privacy Impact Assessment: Steps

Identify the source and type of information gathered, who collected it, how, and why

Determine how and when the information will be used, who is authorized to use it, and how they will be identified

Identify the security controls for data retention, transfer, and sharing, including format and location

Define how, when, and why sensitive information will be disclosed, by whom, and to whom



Establish how and when the sensitive information will be destroyed, and by whom

Advantages of PIA

Acts as an early warning system to identify privacy issues

Supports informed decision-making

Prevents costly and embarrassing privacy errors

Builds public trust and confidence in the organization

Shows evidence of proactive efforts to mitigate privacy risks

Shows stakeholders that the organization is committed to privacy

PIA Process

1. **Project initiation:** Define the PIA scope based on the organization and project
2. **Data flow analysis:** Map how personal information is handled, identify information clusters, and diagram its flow through the organization
3. **Privacy analysis:** Complete privacy questionnaires, followed by reviews and discussions of privacy issues
4. **Privacy impact analysis:** Document privacy risks and potential implications and discuss mitigation strategies

Protecting Privacy

The following are the technologies to protect privacy:

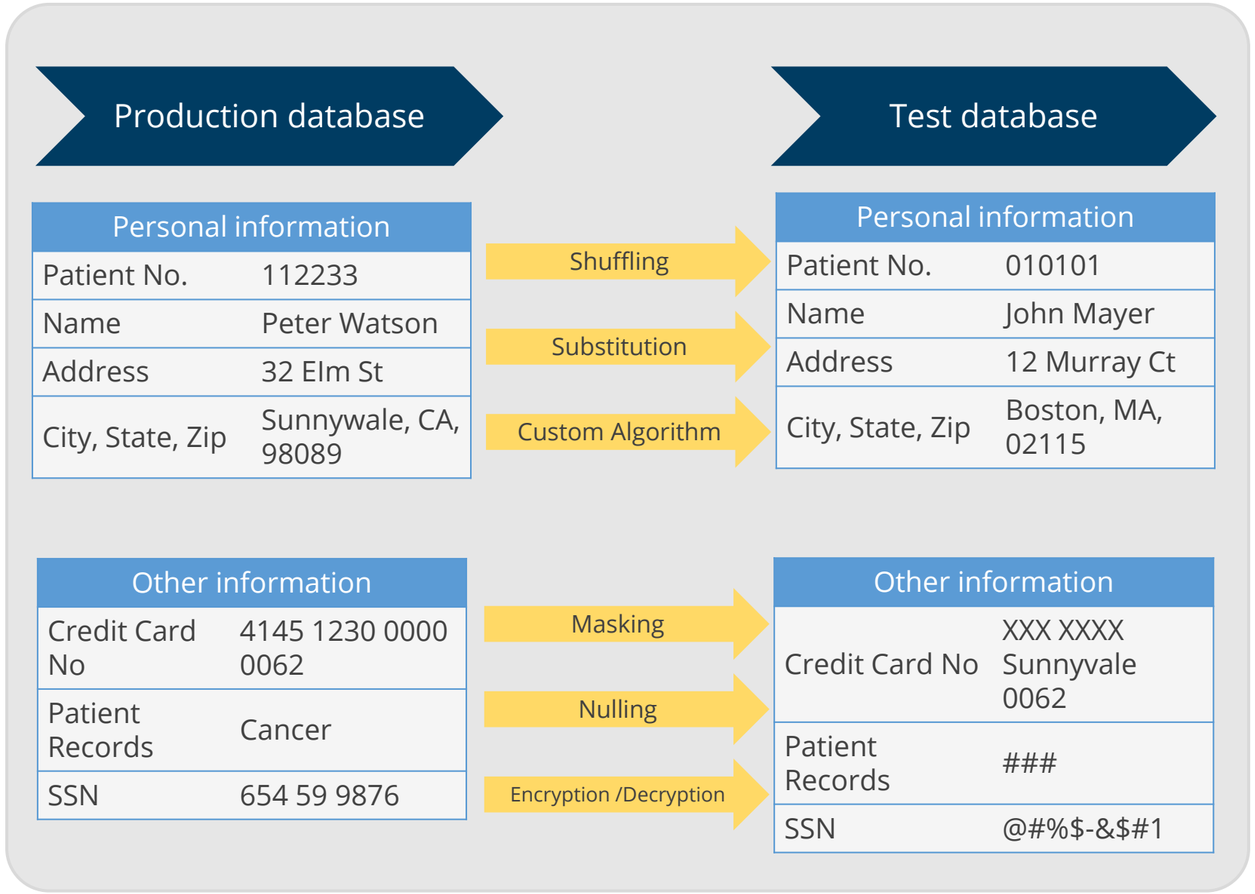
Some Recent Attacks on Privacy

Meta (Facebook)

- **Date:** 2021-22
- **Impact:** 533 million users
- **Details:** In 2021, the personal information of over 533 million Facebook users was exposed due to a massive data breach, highlighting the vulnerabilities of large companies to data breaches. The impact of this breach continues to be felt as the leaked data can be used for various malicious activities such as identity theft, phishing scams, and targeted advertising.

Data Masking or Obfuscation

It is the process of hiding, replacing, or omitting sensitive information from a specific data set.



- Both techniques are used to test platforms where suitable test data is unavailable.
- They are typically applied when migrating tests or development environments to the cloud or when protecting production environments.
- Data masking is typically used to protect specific data sets, such as PII or commercially sensitive data, or comply with certain regulations, such as HIPAA or PCI DSS.

Data Masking Methods

Random substitution	Replaces or appends the value with a random value
Algorithm substitution	Replaces or appends the value with an algorithm-generated value
Shuffle	Shuffles different values within the same column of the data set
Masking	Hides certain parts of the data using specific characters, often applied to credit card formats like XXXX Sunnyvale XX65 5432
Deletion	Removes the data or uses a null value to obscure it

Types of Data Masking: Static Data Masking (SDM)

It permanently alters sensitive data in database copies.

Purpose	Creates a sanitized database copy where all sensitive information is altered that can be shared with non-production users
Process	Generates a new data copy with masked values
Application	For efficient creation of clean non-production environments

Types of Data Masking: Dynamic Data Masking (DDM)

Also known as on-the-fly masking, it replaces sensitive data in transit while keeping the original data intact and unaltered.

Process	Adds a masking layer between the application and the database
Application	For protecting production environments effectively

Example

Hide full credit card numbers from customer service representatives while keeping the data available for processing

Pseudonymization

It is the process of using pseudonyms to represent other data, preventing the direct identity of an entity.

Name	Token or pseudonym	Anonymized
Clyde	qOerd	Xxxxx
Marco	Loqfh	xxxxx
Lex	Mcv	Xxxxx
Les	Mcv	Xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx

Example

In a medical record at a doctor's office, a patient might be identified as Patient 23456 instead of the personal details, which are stored in a separate database linked to the patient’s pseudonym.

Data Anonymization

It removes indirect identifiers to prevent data analysis tools or other mechanisms from aggregating or pulling data from multiple sources to reveal sensitive information.

Direct identifier

- It directly identifies an individual and can be used alone to uniquely pinpoint them.
- **Example:** Social security number, full name, email address, telephone number, health insurance number, medical record number, full-face photographs, and biometric records (fingerprints)

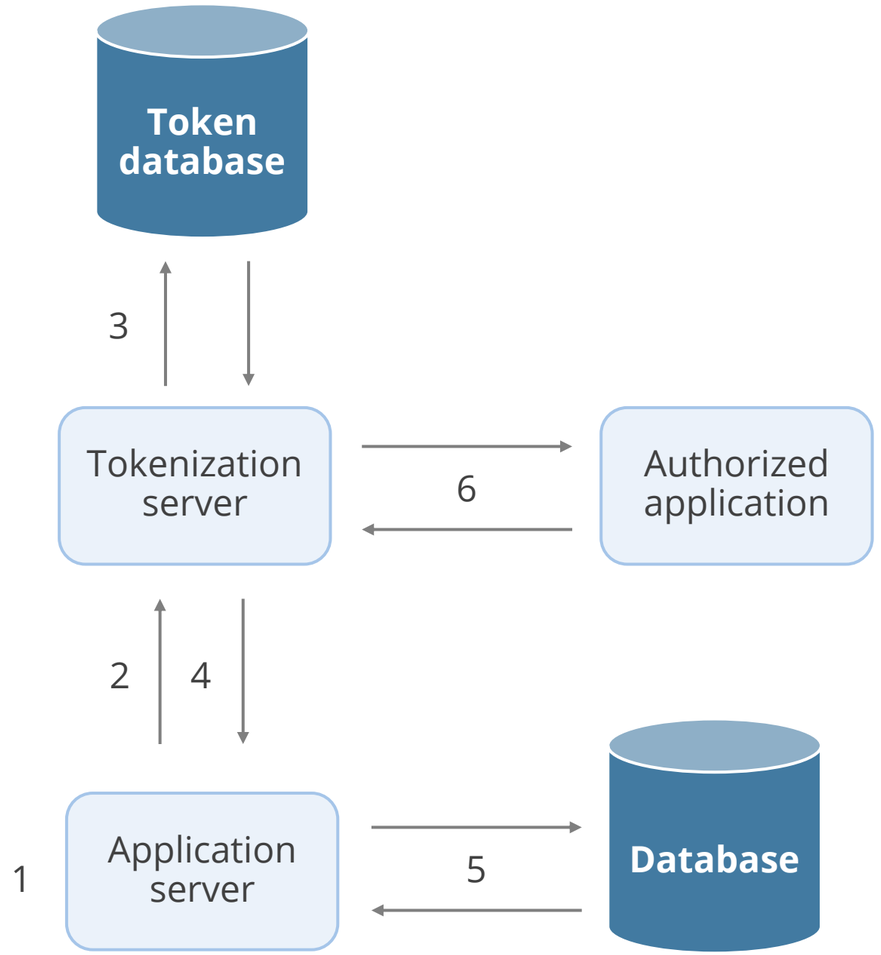
Indirect identifier

- It includes information that can be combined with other information to identify specific individuals.
- **Example:** Gender, date of birth, geographic indicators, and other descriptors

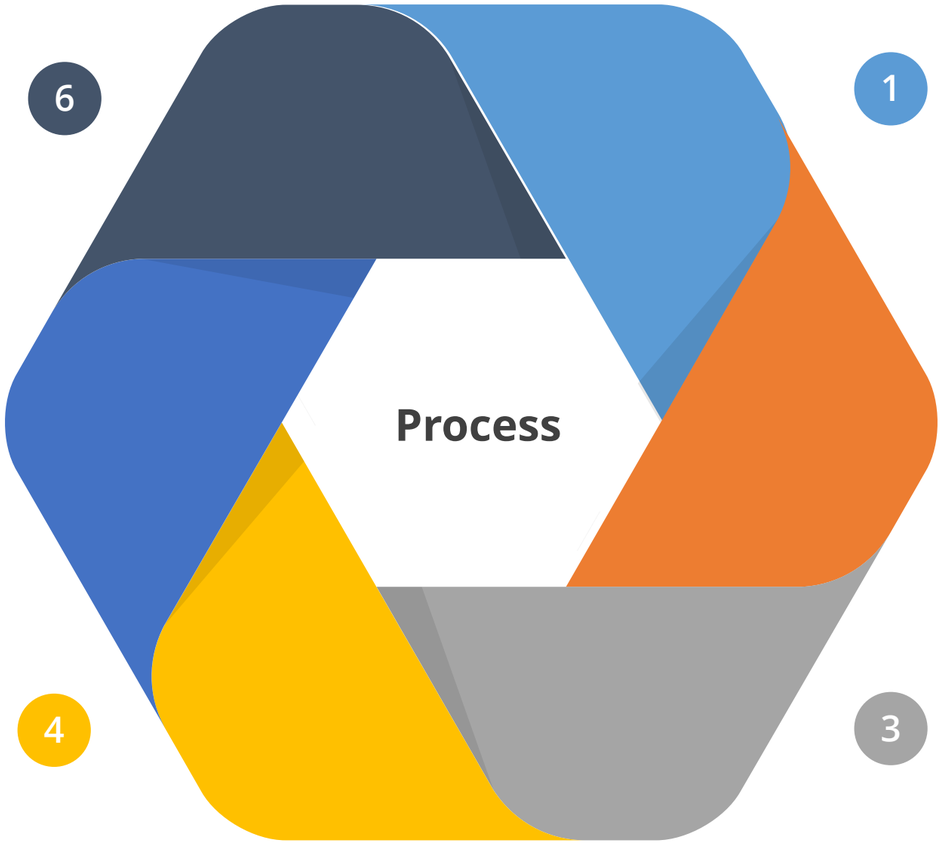
Tokenization

It is the process of substituting a sensitive data element with a non-sensitive equivalent known as a token.

- It replaces the original data with non-sensitive placeholders.
- It safeguards sensitive data in a secure, protected, and regulated environment.



Tokenization



1. Collect or generate sensitive data through an application
2. Send the data to a tokenization server without storing it locally
3. Generate a token on the tokenization server and store both the sensitive data and the token in a token database
4. Return the token to the application
5. Store the token, instead of the original data, in the application
6. Request the sensitive data from the tokenization server when needed by an authorized application or user

Tokenization: Example

- Netflix collects credit card information from customers.
- Netflix uses tokenization to secure credit card information.
- The credit card details are sent to a tokenization database and replaced with a token.
- Netflix stores the token instead of the actual credit card information.
- When needed, Netflix uses the token to retrieve the credit card information from the tokenization database.

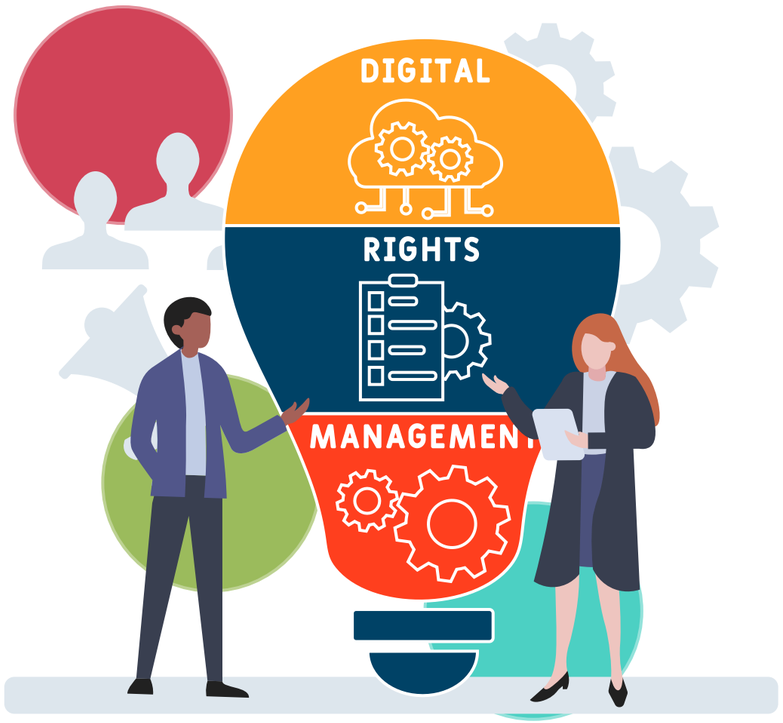
Recent Attack on Privacy

Dell Supply Chain Breach

- **Date:** May 2024
- **Impact:** About 49 million Dell customers
- **Details:** A massive cyberattack in May 2024 compromised the data of about 49 million Dell customers. The threat actor, known as Menelik, created fake partner accounts and used brute-force attacks to gain access to customer information.

Digital Rights Management (DRM)

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



It puts restrictions 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.

Digital Rights Management (DRM)

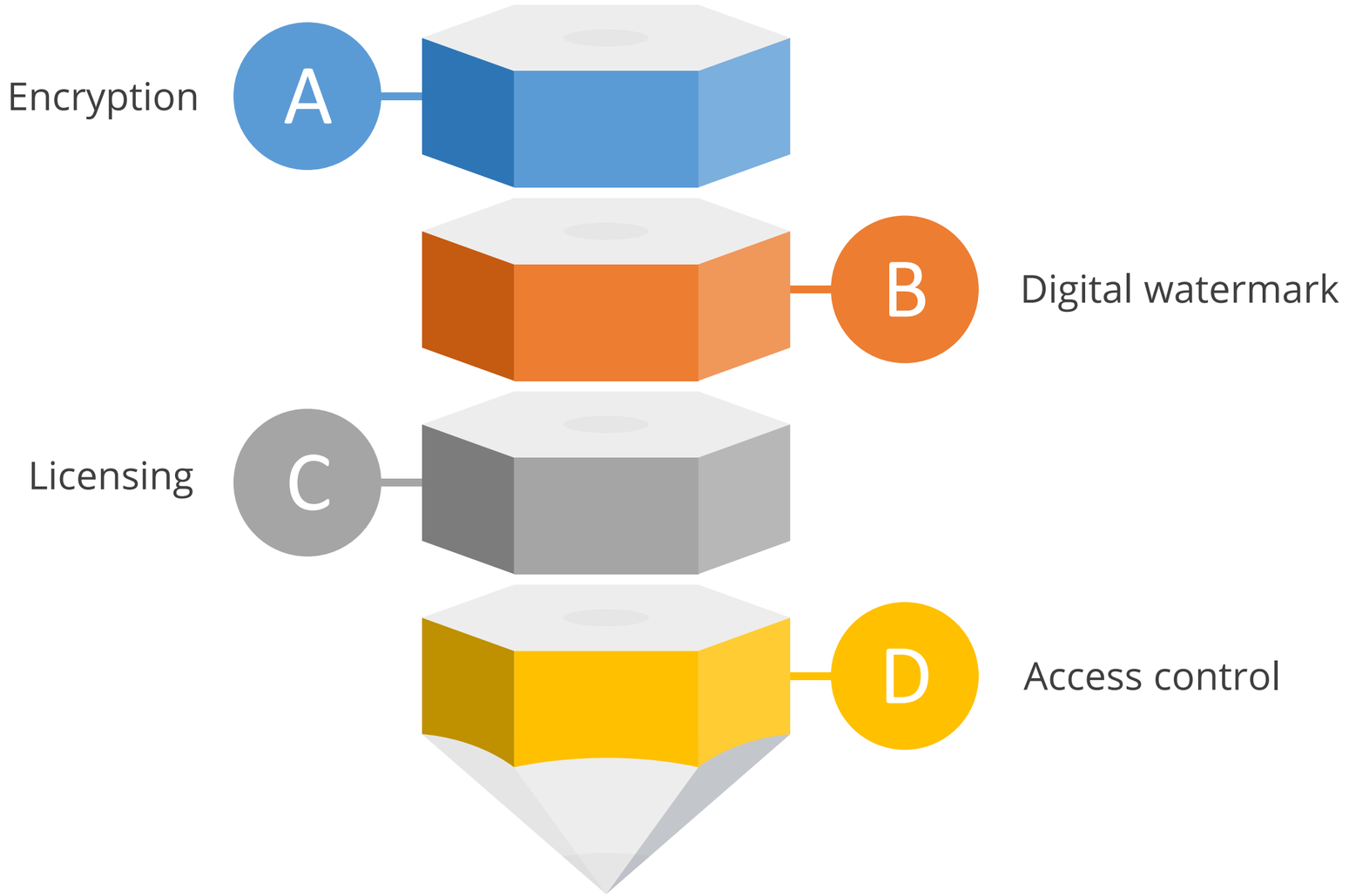
Features

- Protects the intellectual property of a vendor’s digital product that is electronically sold into a wide market
- Allows licensors to electronically specify how their digital products can be used and distributed

Example

DRM can be used to restrict the sharing or copying of music files and limit the viewing time of videos.

Implementing DRM



DRM Functions

Persistent protection

Tracks and protects content regardless of location, duplication, or usage

Automatic expiration

Recognizes and manages content that is not protected indefinitely due to legal restrictions

Continuous auditing

Monitors and reviews the content's use and access history comprehensively

Replication restrictions

Restricts all forms of copying, including screen-scraping, printing, and electronic duplication

Remote rights revocation

Enables revocation of intellectual property rights at any time, especially for litigation or infringement

Dynamic policy control

Adjusts ACLs and permissions for protected data as needed by content creators and data owners

Information Rights Management (IRM)

It focuses on protecting organizational information and privacy.

Features

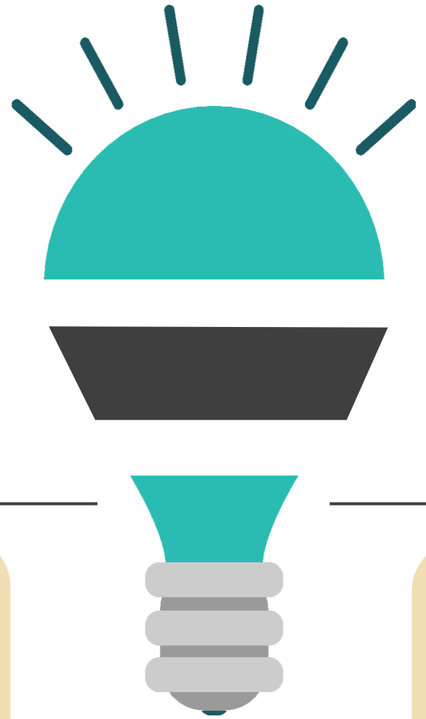
- Sets policies on who can access documents and specifies actions they can take, such as printing, copying, and saving
- Embeds access control lists (ACLs) into the original file, making IRM agnostic to the file's location compared to other preventive controls
- Ensures that protection travels with the file, keeping information secure across both protected and unprotected networks
- Protects sensitive organizational content, including financial documents, emails, web pages, database columns, and other data objects
- Establishes a baseline for default information protection policies using IRM

Example

IRM can be used to control who can read, write, delete, or forward official email.

Data Loss Prevention (DLP)

Implements a set of controls and practices to ensure data is accessible only to authorized users and systems



Aims to manage and minimize risk, maintain regulatory compliance, and demonstrate due diligence by application and data owners

Focuses on protecting against external threats

Acts as an integral part of the overall risk management approach

DLP Approach

Data 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

DLP Architecture

Data in motion (Network-based or gateway DLP)	• Deploys a monitoring engine near the organizational gateway • Monitors outgoing protocols such as HTTP, HTTPS, SMTP, and FTP
Data at rest (Storage-based data)	• Installs DLP engine where the data is at rest, such as storage subsystems or file or application servers • Supports data discovery and tracking usage, potentially requiring integration with network or endpoint DLP for policy enforcement
Data in use (Client or endpoint-based)	• Installs DLP application on user's workstations and endpoint devices • Offers insights into user interactions with data and provides protection beyond what network DLP offers

Software Licensing

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

The following are the considerations:

- 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

Quick Check

A software development team applies data masking to production data, allowing it to be used for testing without exposing sensitive information. How is data masking best described in this scenario?

A. A method for creating similar but unauthentic datasets used for software testing and user training

B. A method for creating similar and authentic datasets used for software testing and user training

C. A method for testing similar but unauthentic datasets used for software development and user training

D. None of the above

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.
- Privacy impact analysis assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, and business relationships.

Thank You