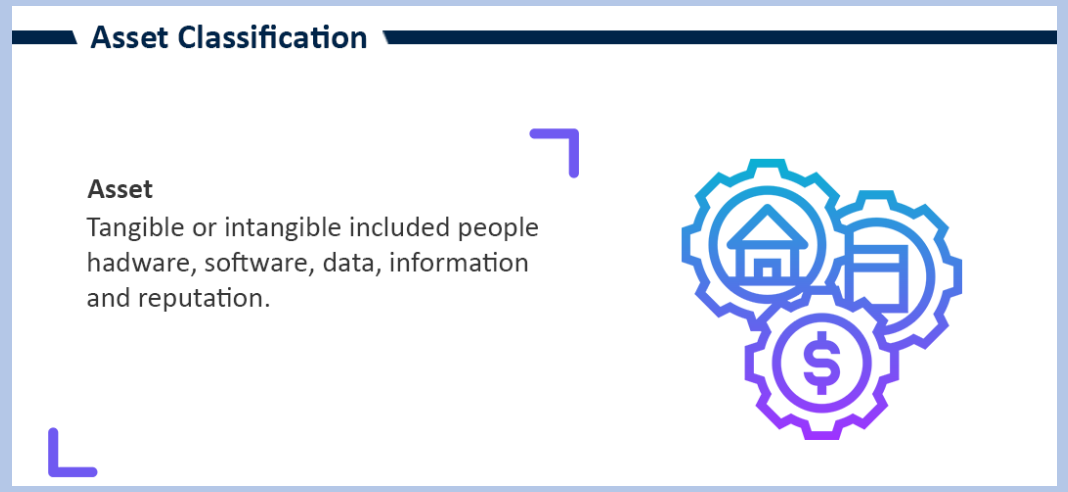
DOMAIN 02: ASSET SECURITY

What is Asset

Anything that has worth for organization

- People
- Partners
- Equipment
- Facilities
- Reputation



Types of Assets

- **Tangible:** Physical presence – can see and touch

  Car, machinery, computer, routers cash

- **Intangible:** No physical presence – cant touch but still have value

  Copyright, brand, software, Data

Asset Classification

Organizations apply appropriate Security Controls based on their importance, value, sensitivity

Critical Assets:

Software, servers, Data

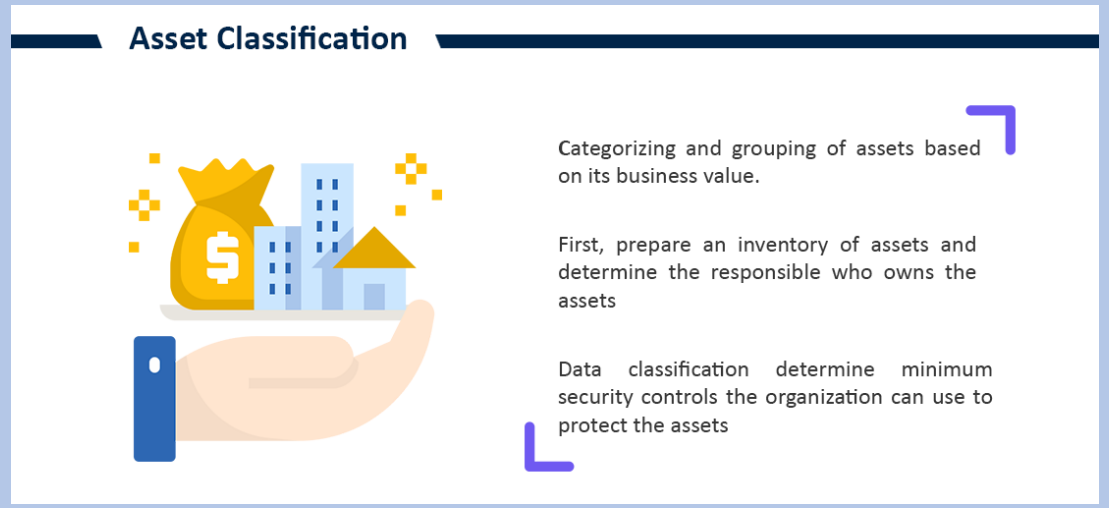
Sensitive Assets:

Licenses, firewalls, IDS/IPS

Public Assets:

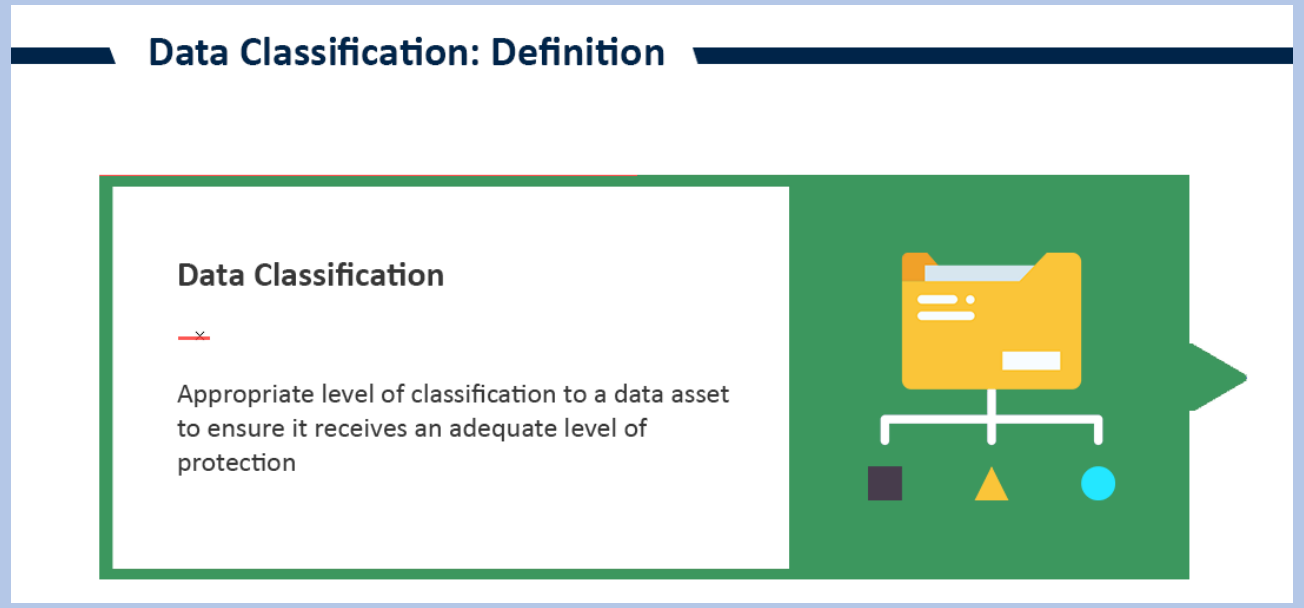
Websites, marketing materials, IoT devices

- People
- Supporting Assets (Power, HVAC)
- Location – Office

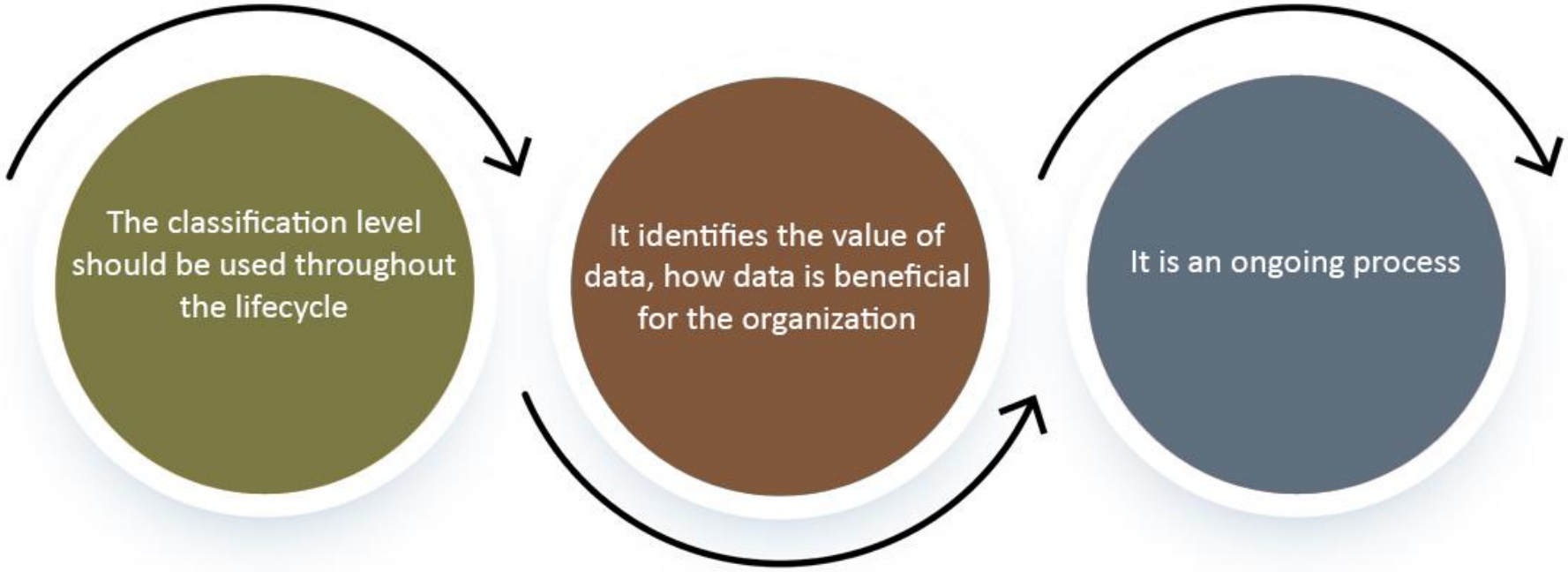


Data

- Piece of digital information
    - Personal Info:
    - Financial Data:
    - Confidential Business Data:
    - Public Data:

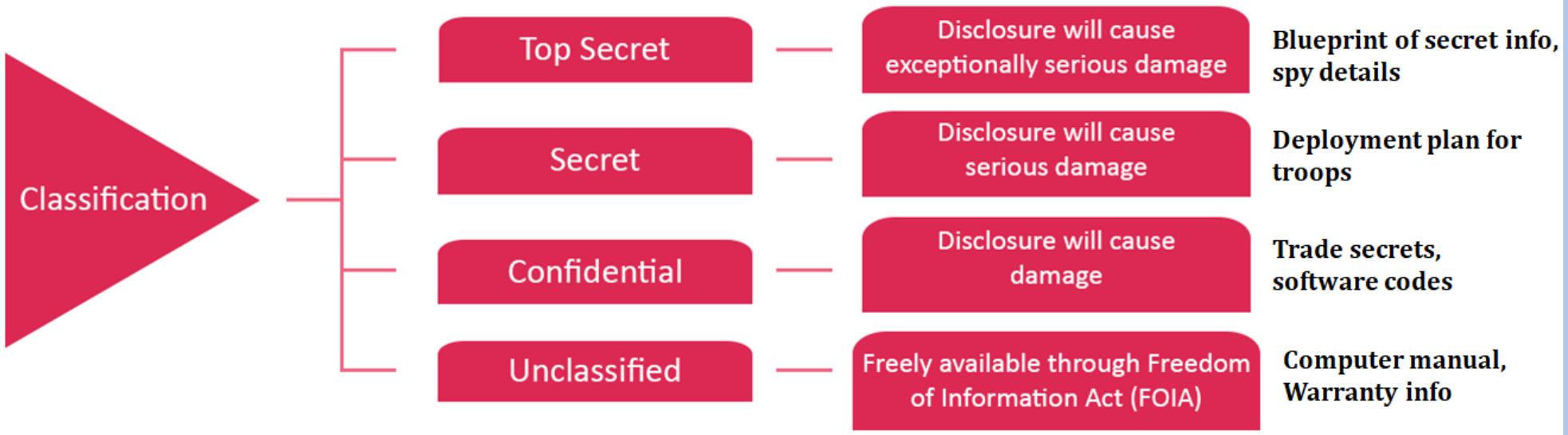


Data Classification



Data Classification Parameters

Information Classification: Government Sector



Commercial or Private Sector Classification

Four level of Classification.

Commercial or private sector classification:

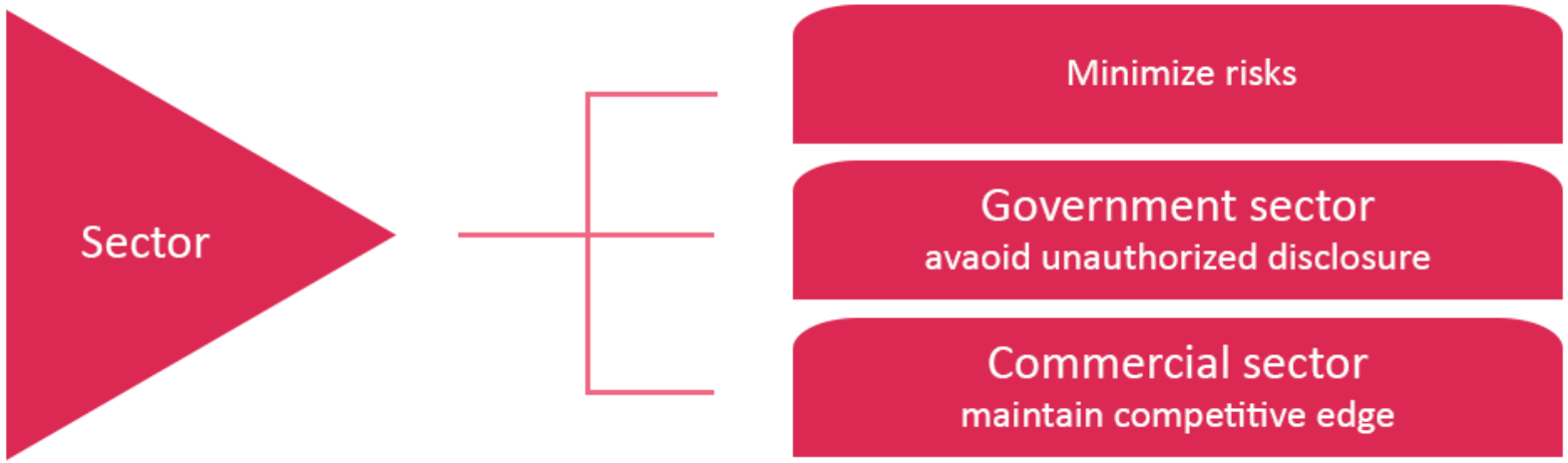
A	Sensitive or Restricted	**Financial info, Projects details**
B	Confidential	**Trade secrets, Software codes**
C	Public	**Resource on specific project**
D	Private	**HR info, Medial record**

Need for Data Classification

- Valuable data use to take strategic decisions
- Implemenatation of controls depending on the sensitivity of information
- Data loss may become huge problem to the organization
- Standardizes type of information and protection requirements
- Information classification improve the confidentiality, integrity and availability.
- Increases cost benefit ratio

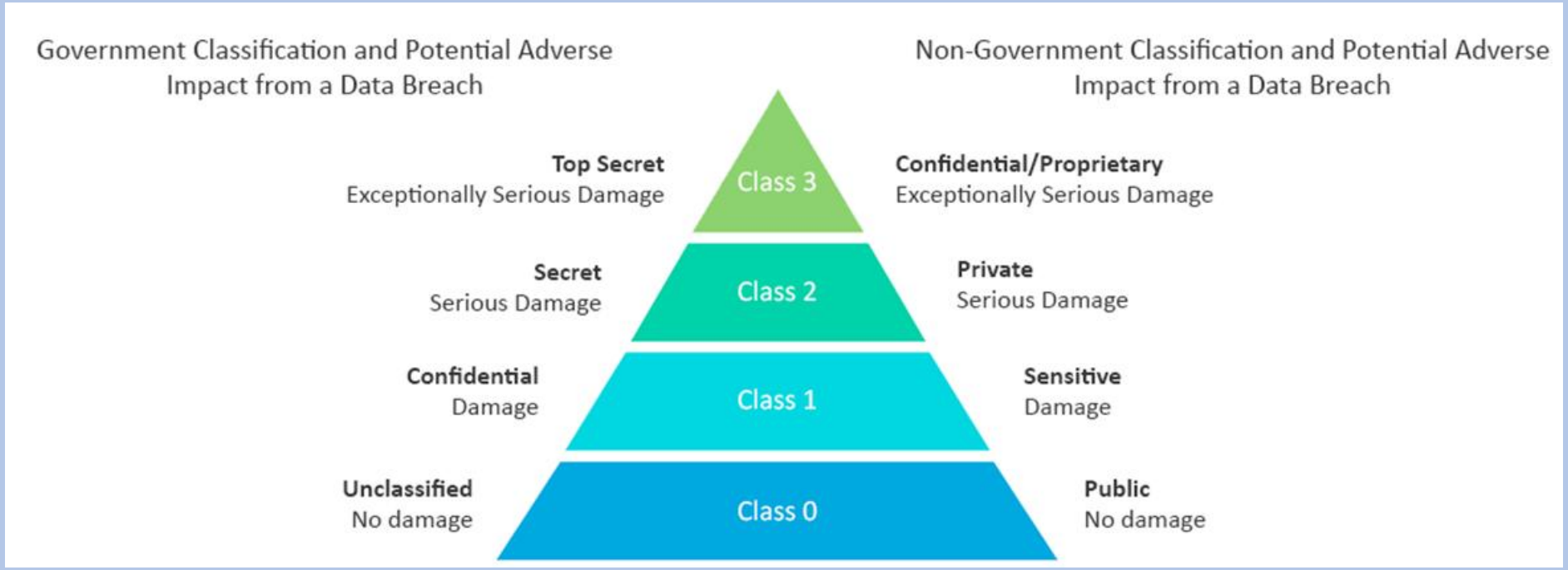
Information Classification Objectives

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



Data Classification

Government Sector vs. Non-Government Sector



Data Classification Procedure

01 Identify the data and create inventory

02 Define classification levels

03 Criteria of classification

04 Data owner responsible for classification

05 Data custodians responsible for maintaining data

06 Security controls on each classification level

07 Classification awareness

08 Methods to transfer data ownership

09 Procedure to review classification and ownership

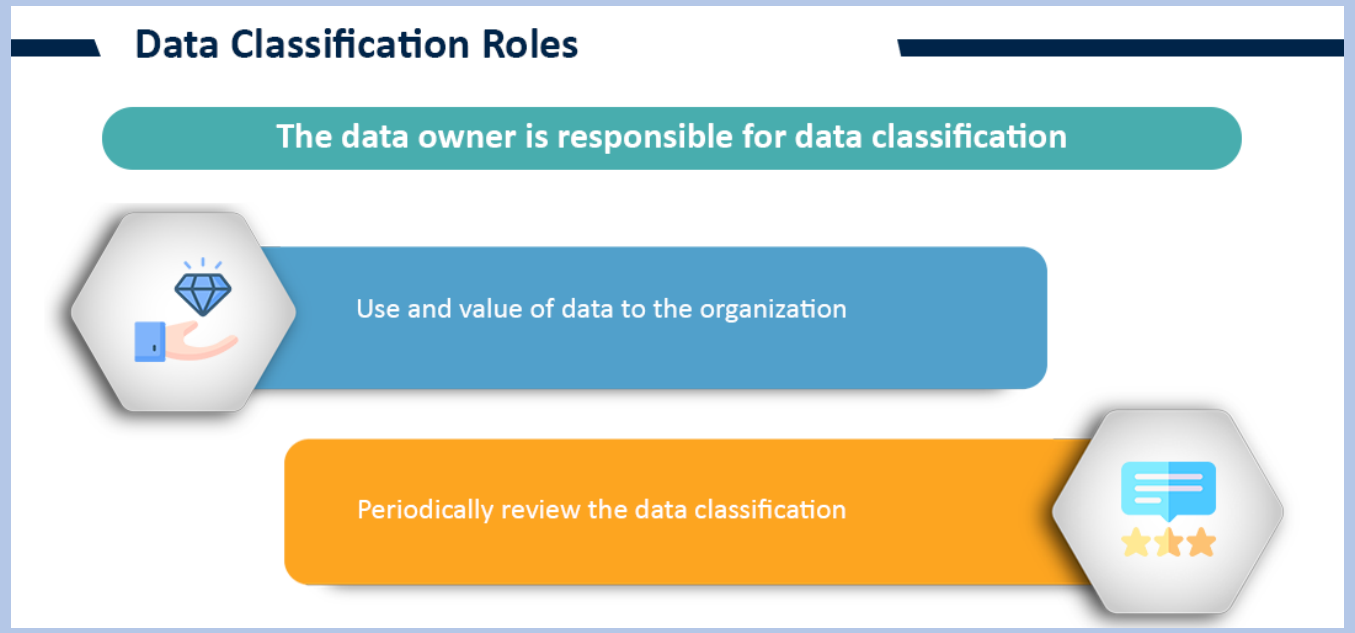
10 Declassification procedures

11 Training of the employees

Data Security Roles

Data Roles

- Data Owner – Head of IT
- Data Custodian – manage Day to Day Data issues
- Data Users – Employees
- Data Controller – Organization
- Data Processor – Contractor
- Data Subject – Customers



Data Owner

Once Controls implemented, to ensure if risk come down to acceptable

Determine sensitivity level

Senior management work as Data custodian

Maintain the confidentiality, integrity and availability of Data

Responsible for labeling

Data Classification and Categorization: Responsible for classifying Data based on its sensitivity, criticality, and importance

Access Control and Authorization: What level of authorization

Data Protection and Security: Ensure encryption, authentication, other Security Controls are in place

Data Lifecycle Management: From creation and usage to storage and disposal. They determine retention periods, archival processes, and Data deletion policies.

Policy and Compliance: Compliance with relevant regulations, industry standards and organizational policies

- **Data Custodian**
  - Maintain the Data, implement the Controls, make backups

Implement patches
Follow Data owner instructions

- **Data Security Implementation:** Responsible for implementing the Security Controls

- **Access Control Management:**
- **Data Backup and Recovery:**
- **Data Encryption:**
- **Data Retention and Disposal:**

Data Controller

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

Data controller responsibilities:

Data Processor

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

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

Data Subject

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

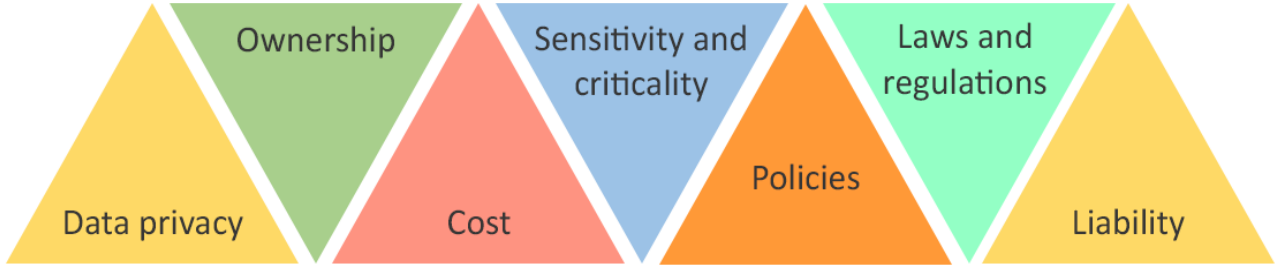
Data Policy

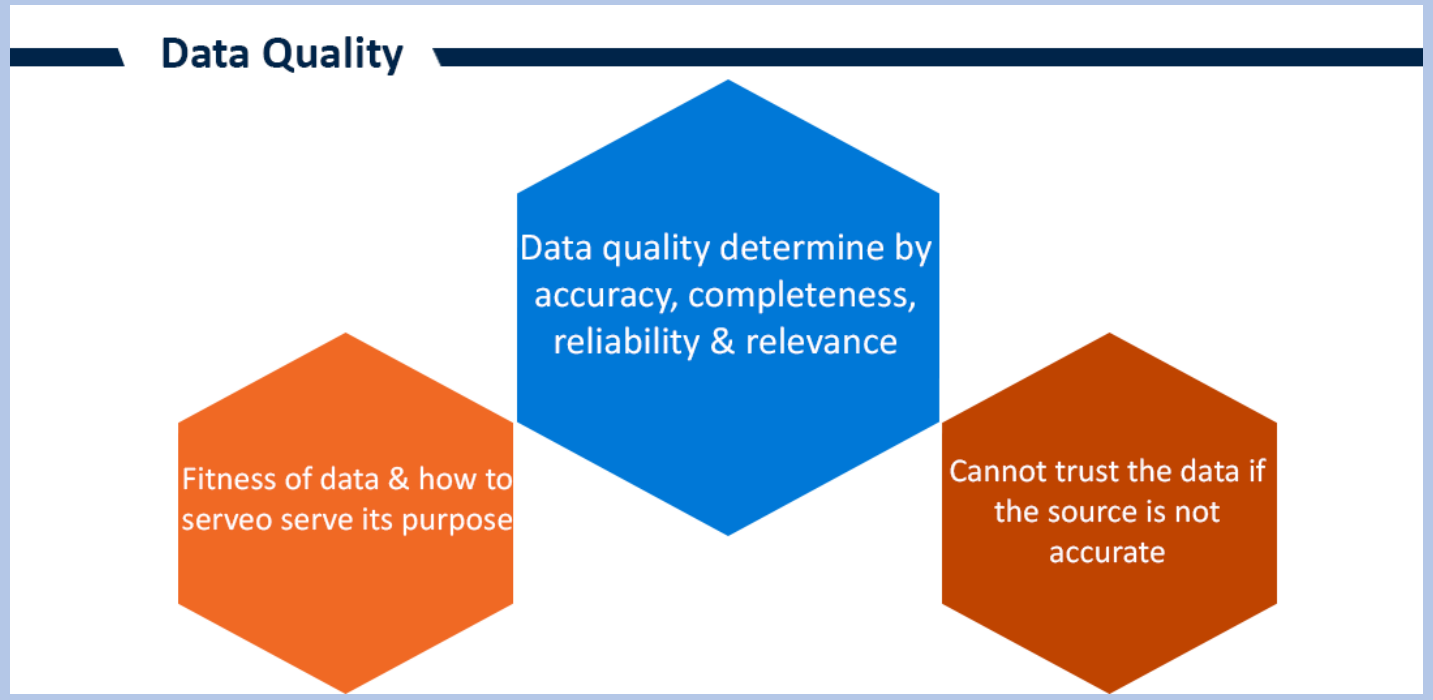
- A high-level document created by senior management that defines long-term goals for data management

- Framework for data management related to data access, lcustodian, data acquisition, data handling, legal and other issues.

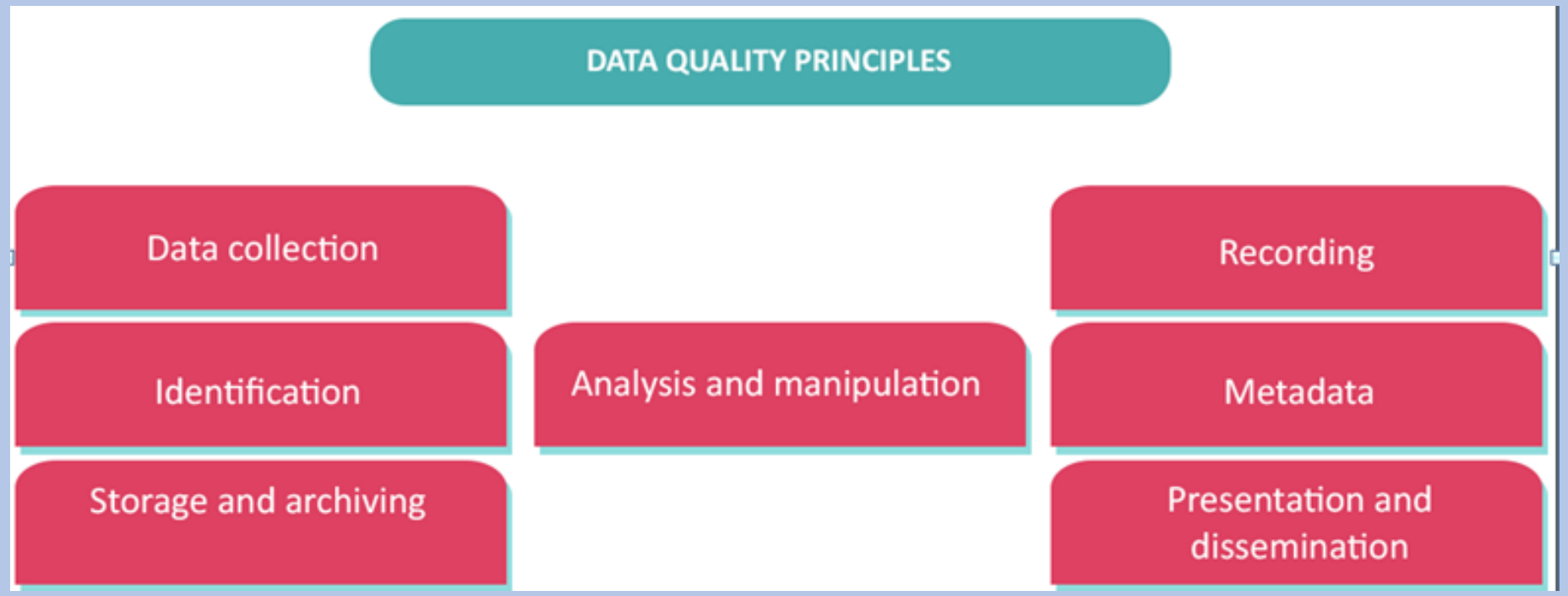
Data Policy

DATA POLICY ELEMENTS





- Accuracy, reliability, completeness and consistency of Data
- High quality Data is essential for effective Cyber Security operations, threat detection, Incident response and decision-making
- Poor quality Data can lead to inaccuracies, misinterpretations, and inadequate Security measures


DATA QUALITY PRINCIPLES
Data collection
Identification
Storage and archiving
Analysis and manipulation
Recording
Metadata
Presentation and dissemination

Techniques to Protect Privacy

Pseudonymization

Data protection technique to enhance Security by replacing or encrypting identifying information

- Replace actual name to false name
- Removes privacy Data so that a Dataset can be shared
- However, the original Data remains available in a separate Dataset

- ACTUAL details replace with FALSE details
- Reversible process

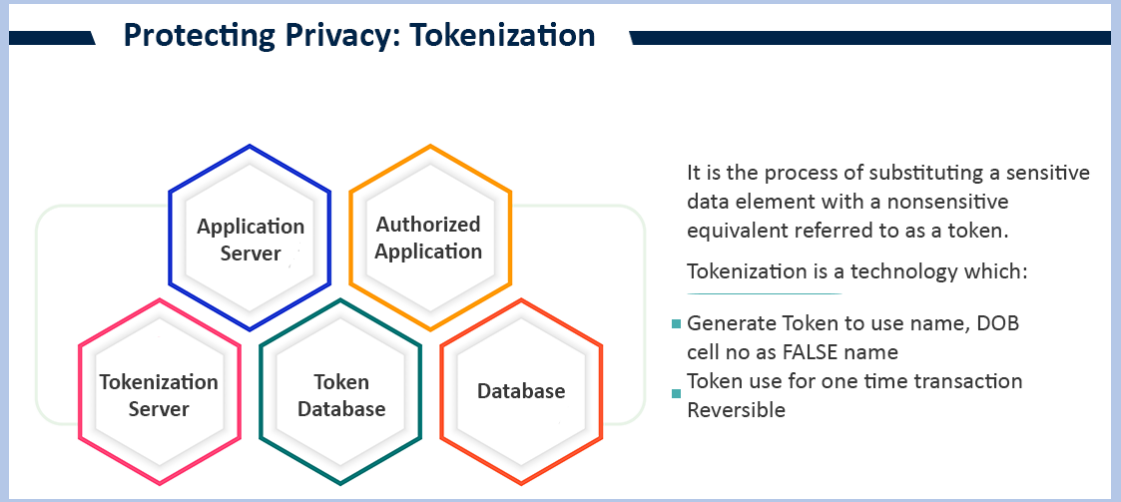
Example:
- Consider a medical record held by a doctor's office
- Replace patient's name, address, and phone number, as Patient A248
- Doctor's office link orignal record with A248

User Authentication: Instead of storing password in plan text, it converts into different format

Tokenization

Data protection technique to replace sensitive Data with a unique token

- Used in payment processing for Data protection
- Reversible



Example:
Credit Card Transactions:

- When a customer makes a credit card transaction, actual card number replaced with a token
- Reduce risk of exposing actual credit card details

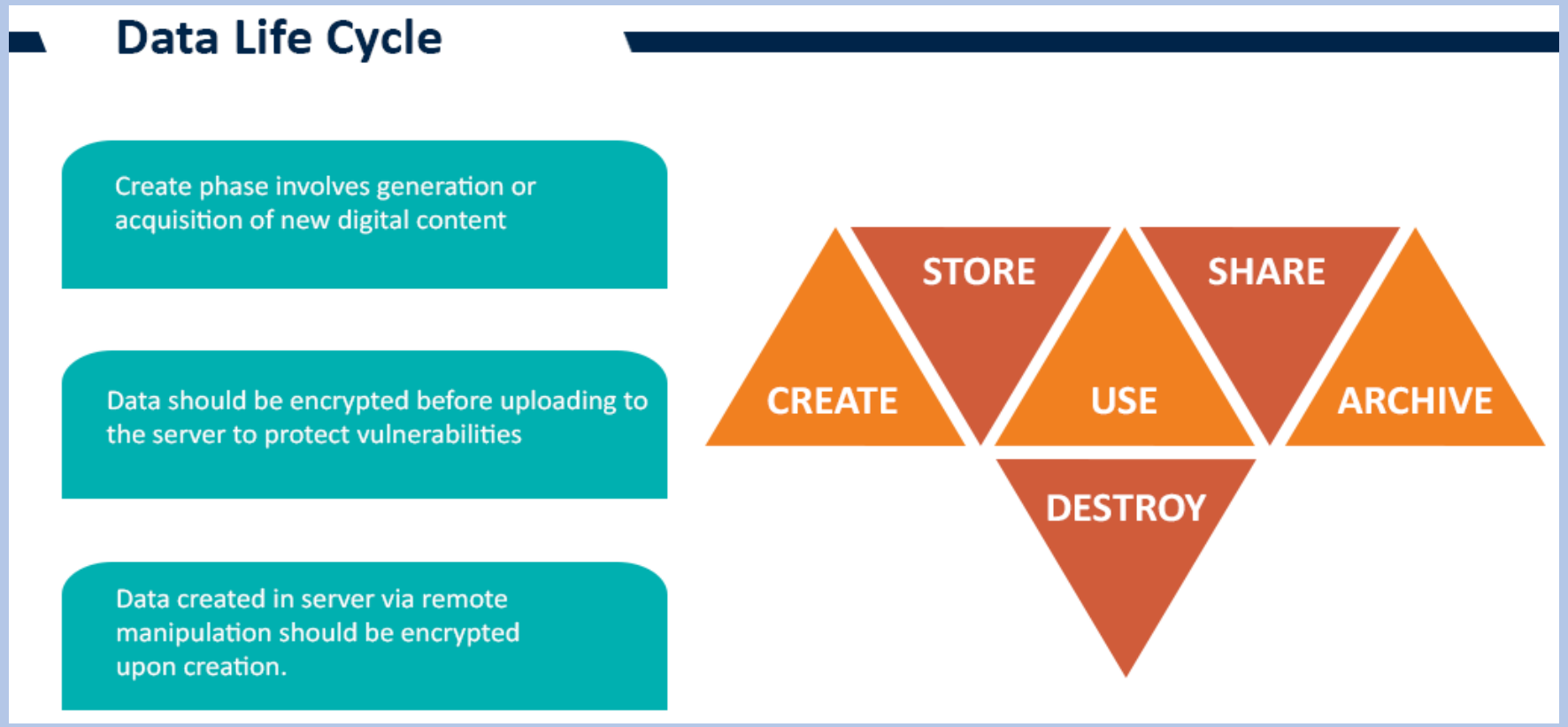
Anonymization

Remove all relevant Data so impossible to identify original person or object

- Credit card bills – only last 4 digits visible & other are masking
- HIDE the actual info
- Non-Reversible

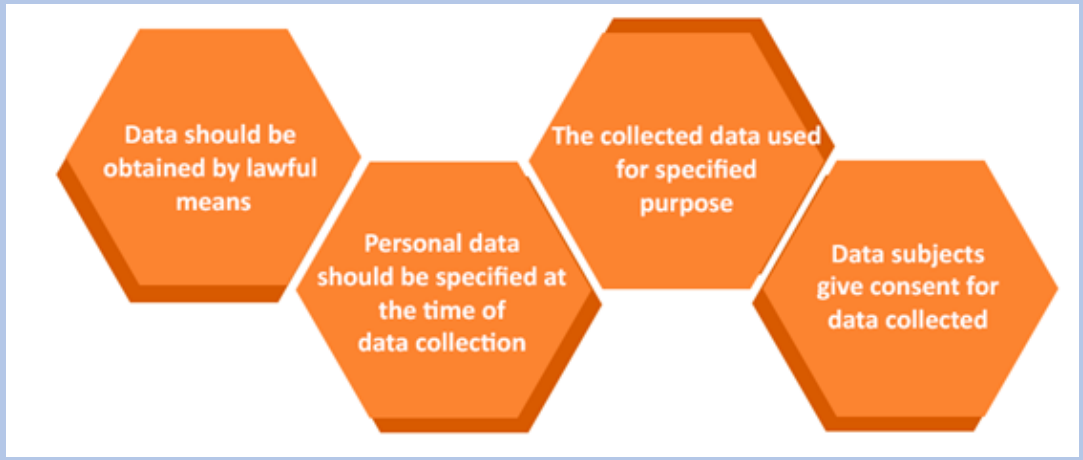
Example:

- **Data Masking:** Replacing name with "User 1“
- **Data Truncation:** Remove some fields from Dataset
- **Data Sharing:** Organizations share anonymized Data with third parties to investigate Security breaches without exposing sensitive Data



Stages of Data from creation, acquisition, deletion, remove and archive

- **Data Life Cycle – Data Create**
    - Collect and compile Data from different sources
    - If personnel info collected, it should follow PII rules
    - Security aspects always important



Examples:

- **Network Data:** Routers, IDS/PDS generate logs about network traffic
- **E-commerce Data:** Online Purchase Data
- **Healthcare Data:** Patient Data created during their visit
- **Social Media Data:** Post and Tweets

- **Data Life Cycle – Data Store**

Store in efficient way for future access

Physical storage devices to modern cloud-based solutions

Example:

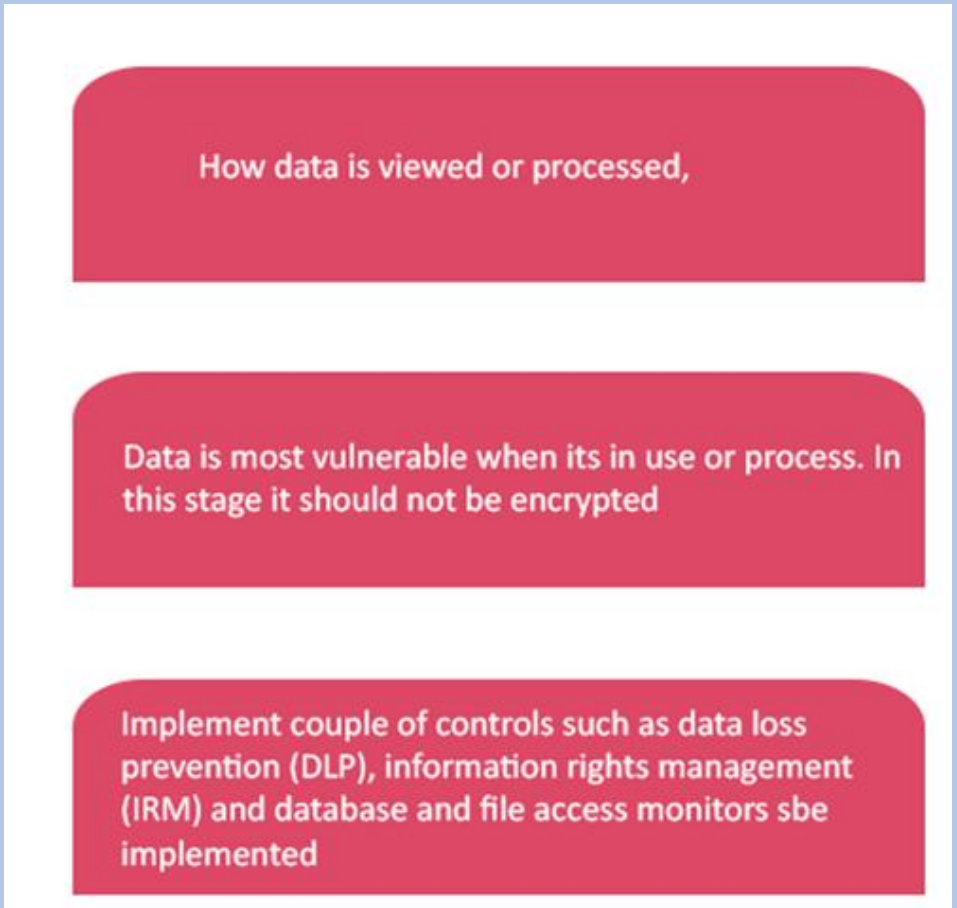
- **Primary Storage:** Online Storage for fast access - RAM, SSDs
- **Secondary Storage:** Offline Storage – hard drive, external drives
- **Cloud Storage:** Provide accessibility and disaster recovery capabilities

Key Consideration:

- **Scalability:** Storage without performance degradation
- **Performance:** High-performance storage is suitable for low latency
- **Data Security:** Protected from unauthorized access
- **Data Backup:** Ensure Data availability

- **Data Life Cycle – Data In_Use**
  - When Data processed or manipulated by applications
  - Data temporarily resides in primary storage: RAM, registers, cache

Example:
- **Real-Time transactions:** When user submitting forms online
- **Editing Documents**
- **Search Queries**
- **Video Conferencing**



- **Data Life Cycle – Data Share**

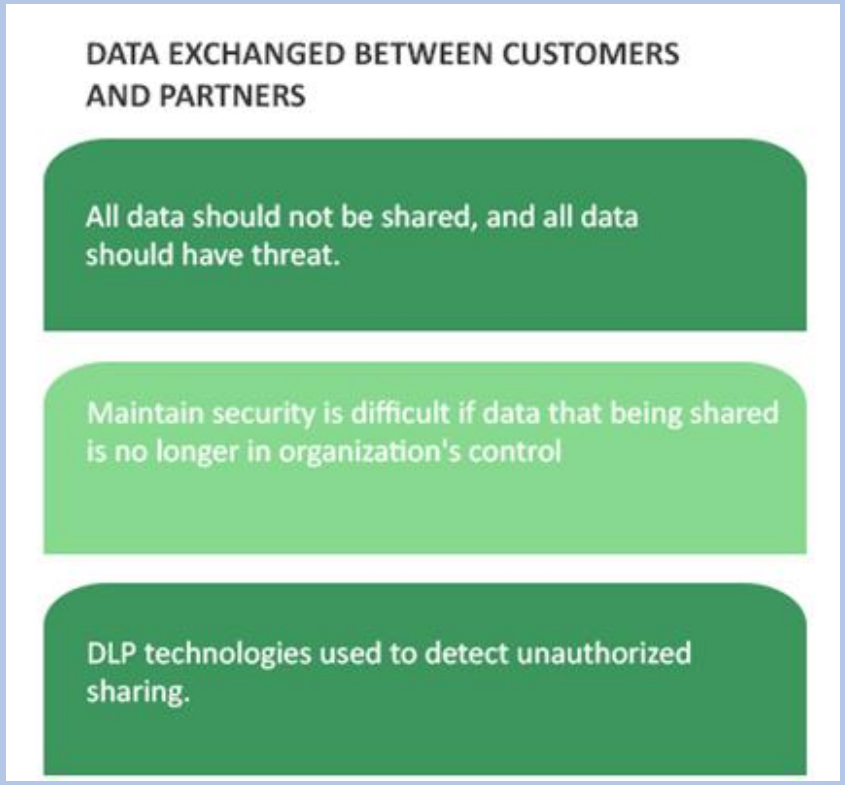
  Transmitting Data from one individual or location to another location

Examples:

Internal Data Sharing: Within organization
External Data Sharing: partners, customers, suppliers
Personal Data Sharing: Social networking

Key Consideration:

Privacy: Sensitive information protected
Security: Encryption, access Controls, authentication mechanisms
Consent: Proper consent from individuals before sharing
Data Quality: Ensure Data is accurate, up-to-date
Compliance: Sharing practices align with relevant industry regulations



Data Life Cycle – Data Archieve

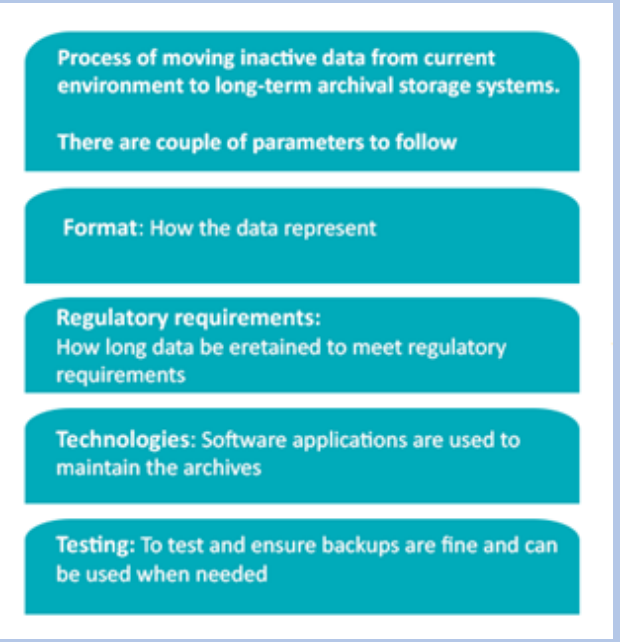
Transfer Data that is no longer actively used
Moving to separate storage location for long-term retention

Examples:

- **Financial Services:** Transaction Records for regulatory compliance and auditing.
- **Healthcare:** Patient records, medical images, treatment history
- **Legal: C**ontracts, legal correspondence

Key Considerations:

- **Retention:** For extended periods for legal, regulatory, business requirements
- **Access:** Accessible when needed
- **Cost Savings:** Less frequently Data helps save costs compare to high-performance
- **Long-Term Preservation:** Design to ensure Data integrity for long term



Data Life Cycle – Data Destroy

- Process of permanently remove Data
- Critical aspect when Data is sensitive or have confidential information

Data Sanitization Method - Erasing

- Simply performing delete operation
- In most cases, the deletion or removal process removes only the directory. The actual Data remains on the drive
- This is Data overwriting

- Least likely to prevent Data remanence
- Perform OS to delete, which simply marks storage space as unavailable not clearing the Data
- If the storage space is not overwritten by another file, Tools can be used to read those storage areas that are marked as unavailable

- Erasing is a simple deletion process.
- Remove only the reference not files.
- This is not the best practice to destroy data because anyone can retrieve later

Tools:

DBAN (Darik's Boot and Nuke): Open-source

Blancco: Commercial Data

Data Sanitization Method - Clearing

Also known as overwriting
Writes Data two or three times over the medium

Used when recycling SSDs
Over writing couple of times

- Prepare media for reuse
- Unclassified data written on addressable locations on the media.
- Data recovery requires special techniques.
- Reuse at the same classification level.

Data Sanitization Method - Purging

Data overwritten many times and more intense than clearing
Repeat clearing process many times
Data cant be recovered

- More intense form of clearing, in this method repeat the clearing process on multiple times.
- Data cannot be recovered
- Combine with degaussing for complete data removal
- Use when prepare media for reuse at lower classification level.

Data Sanitization Method - Degaussing

- By using strong magnetic field to erase Data
- Hard disks and magnetic tapes.
- Not good for SSDs, CDs and DVDs

- Deguassing generates heavy magnetic fields to destroy Only use on hard drives
- **AC erasure:** Medium is degaussed by applying alternating field
- **DC erasure:** Medium is saturated by applying a unidirectional field.

Destroy magnetic media by exposing strong magnetic field

Data Sanitization Method - Destruction

Physical destroying the storage media when no longer needed

- Shredding
- Dismantling
- Chemical Destruction

- In Sanitization process, data cannot be recovered by any means.
- Process includes ensuring non-volatile memory is erased

States of Data

Data at Rest

Data stored on media, Exp: hard drives, USB, SAN, tapes etc,

Data in Transit or Motion

Data transmitted over a network.

Exp: data transmitted over an internal or external metwork, internet etc.

Data in Use

Data resides in temporary storage, buffers when application is using

States of Data – Data at-REST

Data stored on a physical or digital medium, such as hard drives, SSDs, Databases, or backup tapes (not actively processed or transmitted)

Examples:
When files stored on hard drive, Database server

- Encryption
- Physically protected
- Strong Password
- Labeling
- Masking

States of Data - Data In-TRANSIT

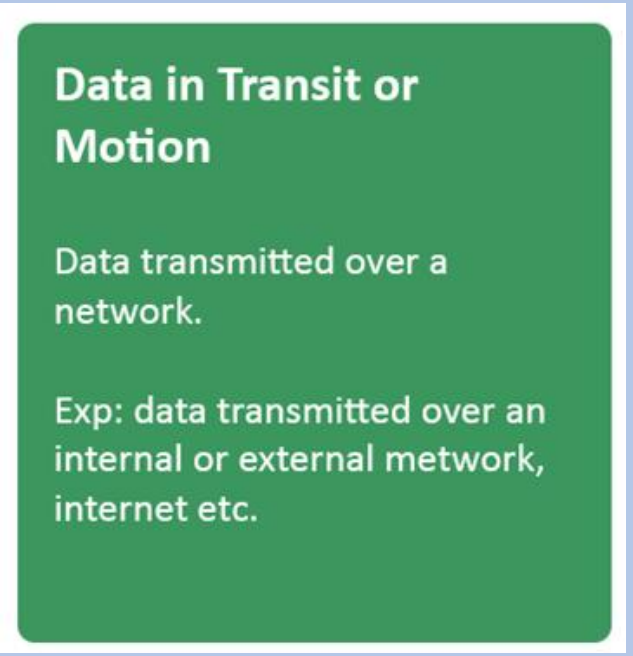
Data travel from one system or network from to other or one network from other networks

Examples:

- Sending email, upload a file, or online purchase
  Data sent across the network

Network DLP

Monitor the Data while in transit



States of Data - Data In-USE

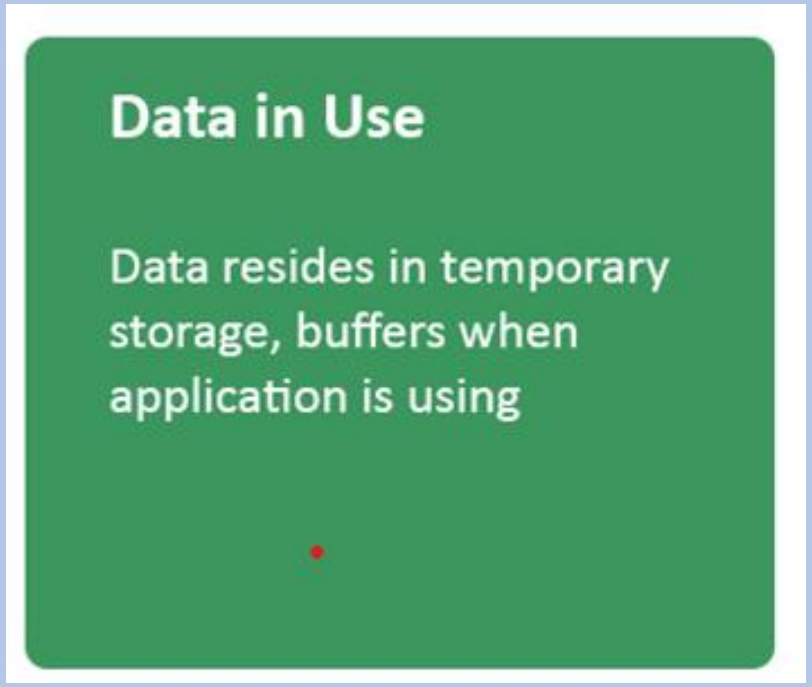
Actively processed or manipulated by user's or application

Editing document, viewing webpage, running application or performing calculations

Data is more Vulnerable when **IN-USE**

End Point DLP

Monitor the Data while In-use



Asset Retention Process

- **EOL – End of Life system**
  - Product discontinued but support still available till end date

Due to EOL/EOS system may have

- Degraded performance
- No support from vendor
- Vulnerabilities

EOS – End of Support

Support not available

Security issue remains there because support/patches are not available

- When software, hardware is no longer actively supported by its manufacturer, vendor, or developer.
- Product will no longer receive updates, patches, or technical support

Microsoft provides EOL dates for its OS, they will no longer releases patches

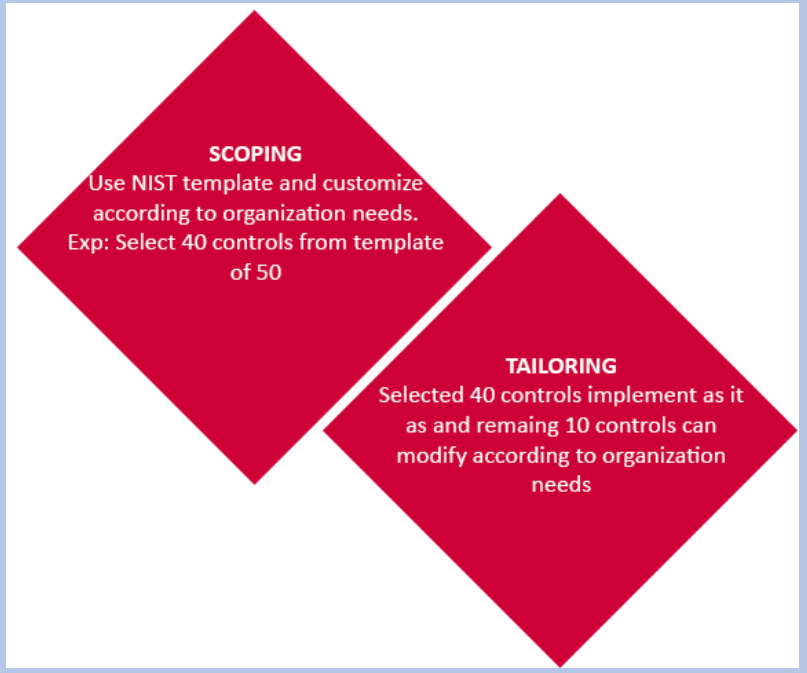
Scoping & Tailoring

- **Scoping**
  - Download Security baseline (all 114 Controls)
  - Apply only 80 Controls which are relevant

Which portion of standard apply in our organization

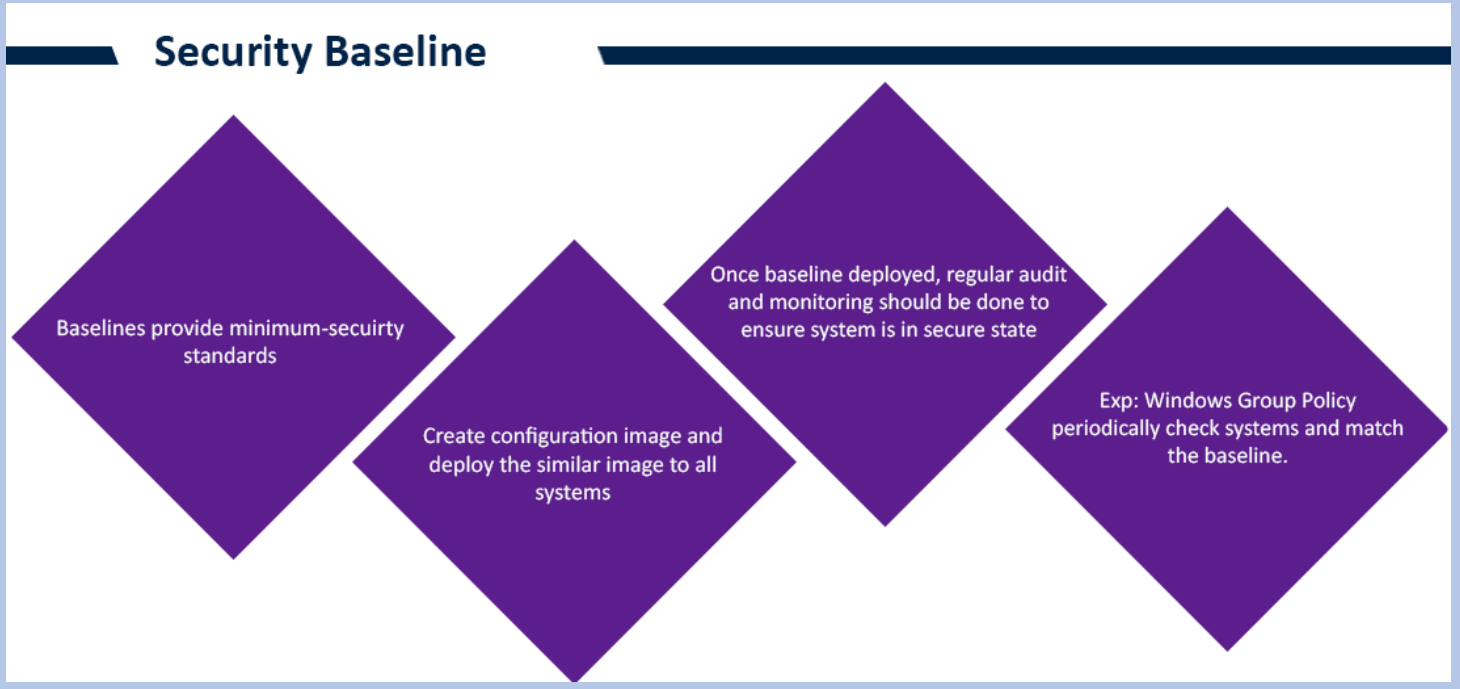
- **Tailoring**
  - Out of these 80 Controls
  - 76 Controls implemented As-it-Is and remaining Controls modified

Customize standards to fulfill organization requirements



- After scoping and Tailoring – Create Security Baseline

- Create image according to Security baseline and install on servers



Baseline

Minimum Security Controls apply