

# Welcome to the (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP) Training Course

# Course Agenda

**Domain 1: Security and Risk Management**

**Domain 2: Asset Security**

**Domain 3: Security Architecture and Engineering**

**Domain 4: Communication and Network Security**

**Domain 5: Identity and Access Management (IAM)**

**Domain 6: Security Assessment and Testing**

# Course Agenda (continued)

**Domain 7: Security Operations**

**Domain 8: Software Development Security**

# Domain 2

---

## Asset Security

# Domain Objectives

1. Understand key asset terms such as assets, information, data, resources, etc.
2. Explain how security controls are dictated by the value of assets, including information.
3. Understand that information/data is only one example of valuable assets that organizations need to protect based on the value of those assets to the organization.
4. Explain how asset classification drives the protection of assets based on value.
5. Describe the asset lifecycle.

## Domain Objectives (continued)

6. Understand how data classification and categorization applies to the asset lifecycle.
7. Understand the importance of establishing accountability and responsibilities for information ownership and custodianship.
8. Explain accountabilities and responsibilities for protection of assets by owner, custodians, stewards, controllers, and processors.
9. Explain key terms associated with asset protection.
10. Understand how privacy of personal information is affected by today's technologies.

# Domain Objectives (continued)

11. Explain the expectations of subjects according to privacy laws and regulations.
12. Explain the importance of the Organization for Economic Cooperation and Development (OECD) guidelines on Privacy Protection.
13. Express the eight principles for privacy protection according to the OECD guidelines.
14. Understand the concept of collection limitation as it applies to privacy.
15. Understand asset retention and how retention policies are driven by organizational requirements.

## Domain Objectives (continued)

16. Explain the reasons that drive data and records retention, including compliance or organizational requirements.
17. Understand the issues associated with long-term storage of assets.
18. Define baseline protection.
19. Explain how baselines can help an organization achieve minimum levels of security associated with valuable assets.
20. Understand how baselines include security controls and how to implement them.
21. Describe baseline protection and scoping and tailoring in reference to asset protection.



## Domain Objectives (continued)

- 22. Understand the different data states and explain how to secure each.
- 23. Explain the difference between end-to-end and link encryption as it relates to data in motion.
- 24. Understand how media requires controls to protect its content.
- 25. Understand labeling and marking requirements of assets that have been classified.
- 26. Understand how the handling of media and assets that have been classified should be allowed only to those that are authorized.

## Domain Objectives (continued)

- 27. Understand how storing, retention, and destruction of assets is dictated by classification.
- 28. Understand data remanence and its impact to the value of assets.
- 29. Explain the various options in addressing data remanence, including clearing, purging, and destruction.
- 30. Explain methods used to clear, purge, and destroy data.

# Domain Agenda

---

Information and Assets

---

Asset Lifecycle

---

Information and Asset Ownership

---

Protect Privacy

---

Asset Retention

---

# Domain Agenda (continued)

---

Data Security Controls

---

Information and Asset Handling Requirements

---

Data Remanence

---

Domain Review

---

# Module 1

---

## Information and Assets

# Module Objectives

1. Understand key asset terms such as assets, information, data, resources, etc.
2. Explain how security controls are dictated by the value of assets, including information.
3. Understand that information/data is only one example of valuable assets that organizations need to protect based on the value of those assets to the organization.
4. Explain how asset classification drives the protection of assets based on value.

# Assets Security Concepts

Asset security is a broad subject, and it deals with a vast array of knowledge and terminology, some more technical than others. The term *asset* describes computing devices, IT systems, software (both an installed instance and a physical instance), virtual computing platforms (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, and keyboards). This matches definitions common to industry and regulatory entities, such as the National Institute of Standards and Technology (NIST). Data is also an asset to an organization. The terms are not interchangeable, as data is a subset of valuable assets to an organization. It is important for the security professional to have a grounding in some key concepts that relate to securing assets.

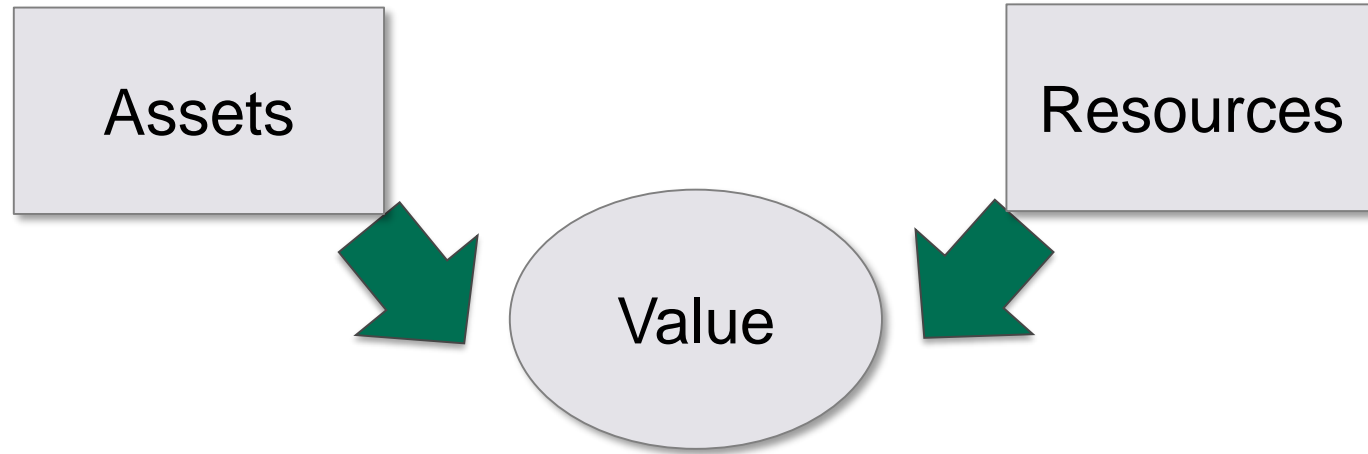
## **DATA POLICY**

Data management has to be guided by a set of principles and procedures that apply broadly to the organization. Each department in the organization may choose to customize the policy to fulfill unique requirements, but must remain in alignment with the authority of the top-level policy. A sound data policy should guide the organization to collect only the required information, keep it safe, and securely destroy any information once the asset is no longer needed.

A sound data policy helps an organization address important considerations that impact the practice of data protection. Because the nature of asset security is dynamic as threats change, the data policy will need to be flexible and able to accommodate change. However, the data policy must be aligned with prevailing law and regulatory requirements in all cases.

Establishing a data policy is important in an organization for more than just compliance or due diligence. Data policy also plays a significant role in data governance. A well-defined data policy provides direction for the management to set practices and standards related to quality, format, access, and retention of data.

# Assets, Information, and Resources



Let us take for example a plot of land. A company, let's call that X buys that plot of land in exchange of money to be used in production activities.

In this case, land is a *resource* as in, the land is the source from which benefit is produced. The benefit here is the land being used for productive purposes.


The land becomes an asset for the company. An asset is a resource that is controlled by the person/company from which one can expect to receive future benefits. By future benefit, I mean the revenue that is generated by the operation of the business in the land.

The capital is the money that is used to buy the plot of land. In other terms, the capital can also be explained as the amount that is invested to run the business. In simple terms, asset creation requires capital.

To sum it up, *resource* is the source of profit. When controlled, resource becomes an *asset*; and the money used to purchase the asset is the *capital*.




# Assets, Information, and Other Valuable Resources



## Value of an Asset

- Quantitative
- Qualitative



## Protection of Valuable Assets

- Should be based on the value

# Examples of Valuable Assets

People	Corporate Reputation/Brand	Products
Information/Data	Architectures	Processes
Hardware	Software	Intellectual Property/Ideas

# **DATA GOVERNANCE**

A data governance office oversees data policy and outlines roles and responsibilities for the cross-functional stakeholders. An organization should determine how it wants to manage the creation, transformation, and usage of data valued by the organization. This function describes data governance. The concept of data governance includes the people, processes, and IT organizations used to handle data properly and consistently, both internally and externally. There are several guiding principles that an organization should use to establish their data governance model:

- Establish responsibilities
- Plan to best support the organization
- Acquire validly
- Ensure performance when required
- Ensure conformance with rules
- Ensure respect for human factors

A data governance model establishes authority and management and decision-making parameters related to the data produced or managed by the enterprise.

# Identification/Discovery and Classification of Assets Based on Value

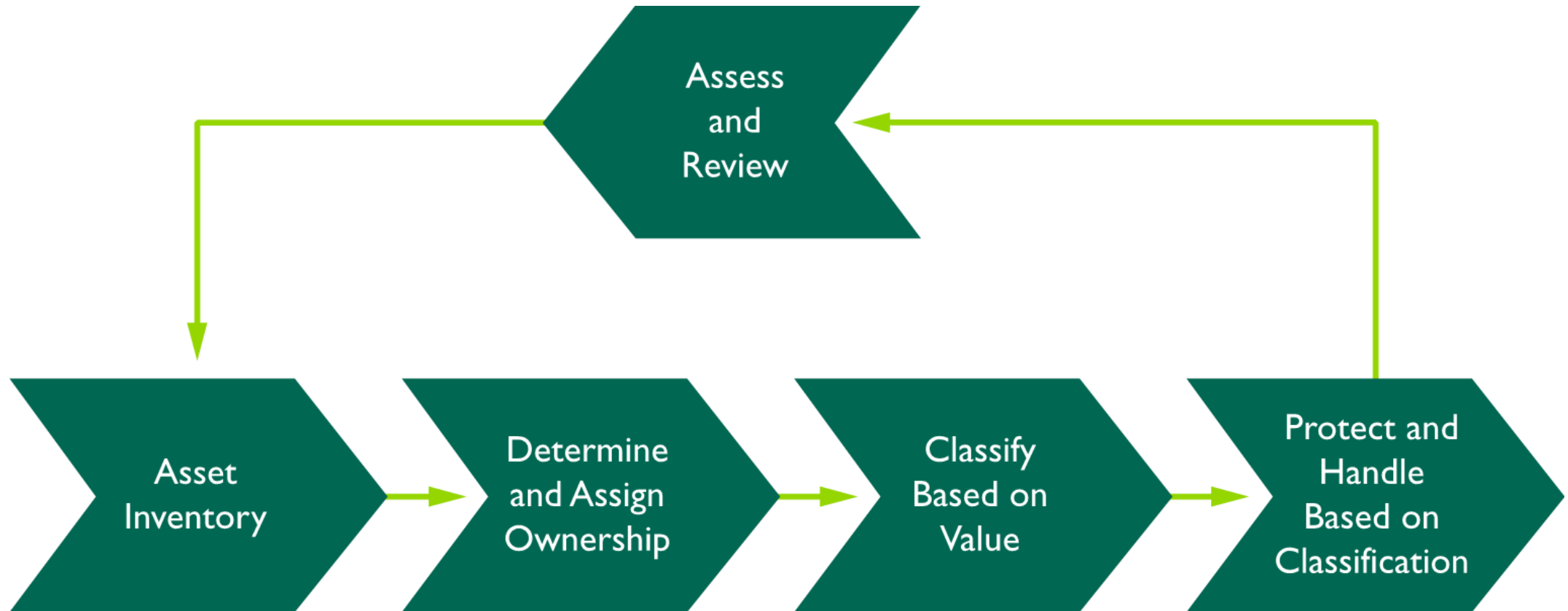
## Identify/Discover Assets

- Inventory
- Needs to be formal process

## Asset Classification

- Requires management support, commitment, and conviction
- Accountability
- Policies
- Training/awareness/education

# Classification Process



# Process of Protection of Valuable Assets Based on Classification

Identify and Locate  
Assets Including  
Information

Asset discovery

Classify Based  
on Value

Requires ownership  
to establish  
accountability

Protect Based on  
Classification

Baselines for each  
classification level

# DATA QUALITY

Data quality involves the integrity and reliability of data. To maintain its data quality, it is important to verify and validate data throughout useful life. In fact, the quality of the data is related to the fitness for use or potential use of the information. Factors such as accuracy, currency, and relevance top the list of items to check for when measuring data quality.

- ***Quality assurance (QA):*** Use of prescribed standards to assess and to discover inconsistencies and other anomalies in the data and apply data cleansing to deliver a final product. QA addresses the question, “Is the data fit for the purpose?”
- ***Quality control (QC):*** An assessment of data quality based on internal standards, processes, and procedures to control and monitor quality as informed by QA. QC addresses the question, “Is the data fit for use?”

The purpose of performing QA and QC in data quality procedures is to reduce errors in the data sets to acceptable levels.

The following are the general types of errors that good data quality practices aim to reduce:

***Errors of commission:*** Data entry mistakes or inaccurate transcription that should be reduced by having a sufficient QA process in data acquisition.

***Errors of omission:*** Harder to detect, these are missing data that can lead to inaccurate values or interpretation of data sets or calculations made on the data.

# DATA DOCUMENTATION

The practice of documentation and organization of data assets is useful in organizations to manage the increasingly large sets of data critical to business processes. Proper data documentation helps to ensure that data users will understand and use data efficiently. It also helps organizations ensure that data will be usable far into the future. The general components of data documentation are how the data was created, what the context is for the data, the structure of the data and its contents, and any manipulations that have been done to the data. The objectives of data documentation are as follows:

- Longevity and reuse of data.
- Data users should understand content, context, and limits of data.
- Easier discovery of data within the organization.
- Data interoperability and exchange of data.

**Metadata:** Metadata management is an inextricable part of records management, serving a variety of functions and purposes. It is descriptive information about the data set. It is data describing the context, content, and structure of records and their management through time.

The metadata requirements are established by the organization, but some types of metadata used are as follows:

Information describing the record

Business rules, policies, and mandates

Agents (or people) related to the record

Business activities and processes

Information about records management processes

Metadata about the metadata record



# DATA DOCUMENTATION

**Readme file:** This is a type of data documentation used primarily for application or programming files. The use of a Readme file in .txt or .pdf format helps explain the data set beyond the metadata description.

**File contents:** There is no mandatory formatting or requirements for file organization, but in general, files should be named something unique, consistent, informative, and easily sortable. Using project names or author names is encouraged while the use of special characters is not, except for dashes, underscores, and numbers.

## DATA ORGANIZATION

The process organizations use to arrange and control data is called *data organization*.

A *data structure* is described as a collection of data values, the relationships among them, and the functions or operations that can be applied to the data.

**Unstructured data** is data that lacks a formal data model. An example of this kind of data is a simple text document, where names, dates, and other pieces of information are scattered throughout random paragraphs.

**Structured data** is acquired, maintained, and analyzed within the context of a formal data model.

### **Data Schema**

A *data schema* is a concept that would be covered in great depth if this were a data science book. Limited to the topic of asset security, it is important to note that the data schema is an element of data organization.

# Module 2

---

## Asset Lifecycle

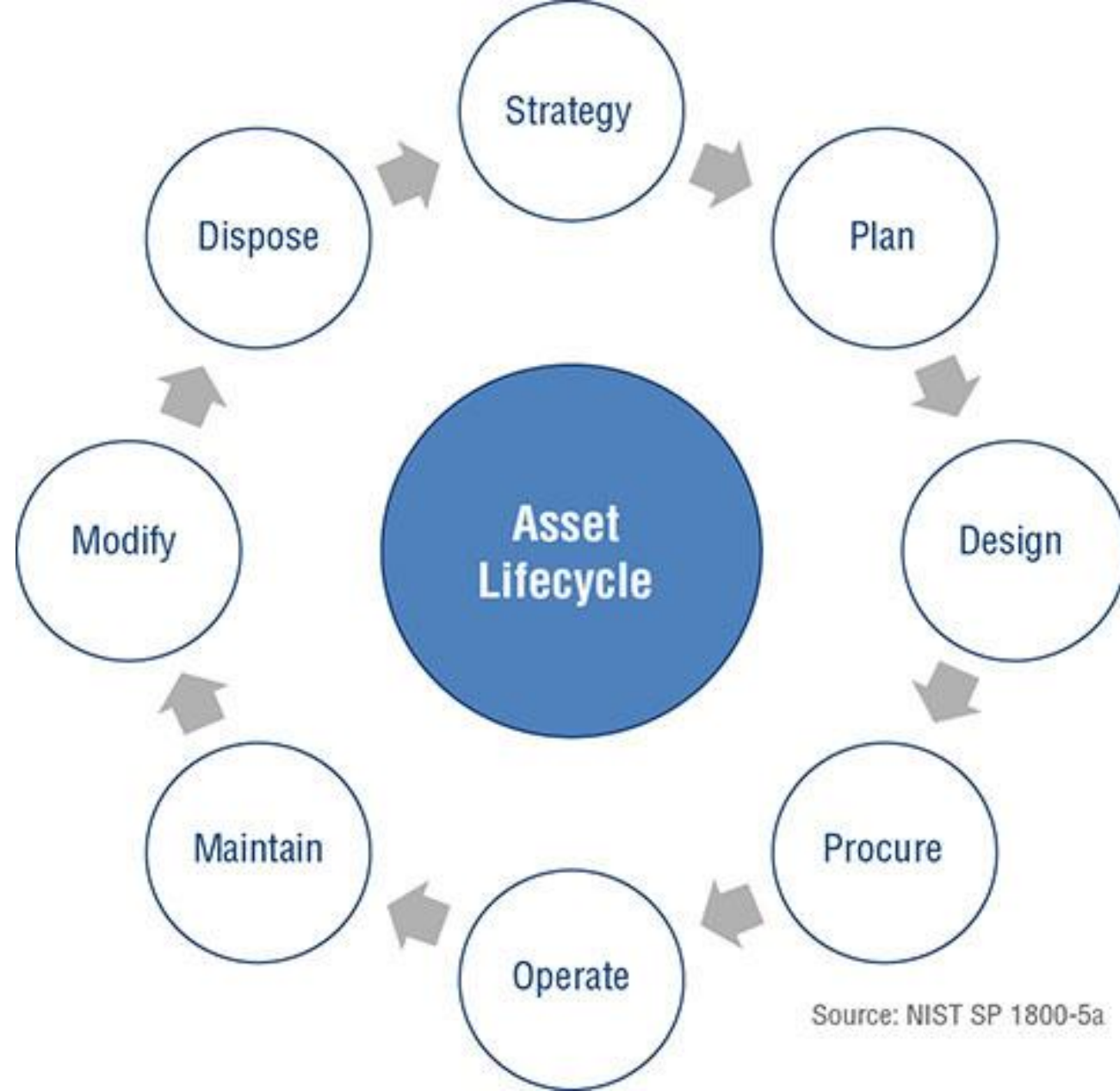
# Module Objectives

1. Describe the asset lifecycle.
2. Understand how data classification and categorization applies to the asset lifecycle.

# Module Objectives

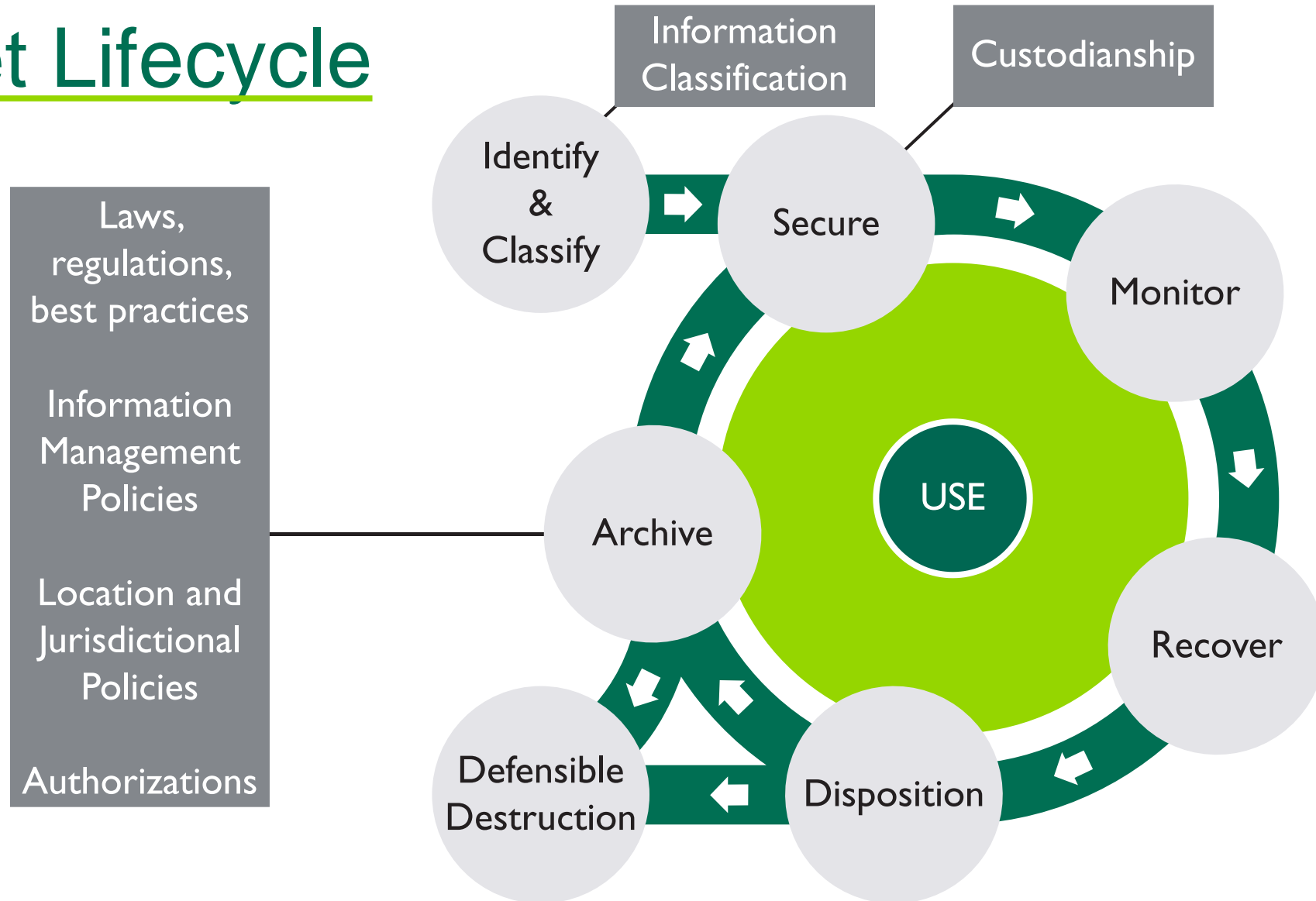
1. Describe the asset lifecycle.
2. Understand how data classification and categorization applies to the asset lifecycle.

# Asset Lifecycle



Source: NIST SP 1800-5a

# Asset Lifecycle



# Differences between Classification and Categorization



## Classification

- The act of forming into a class or classes
- A distribution into groups, as classes according to common attributes

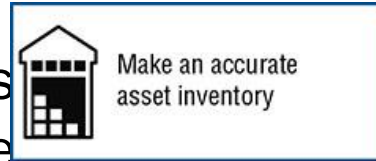
## Categorization

- The process of sorting or arranging things into classes

# Classification

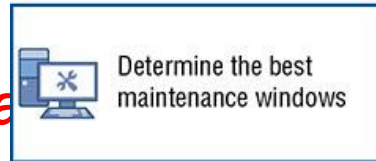
Ensures assets are marked and protected (based on value) in such a way that only those with an appropriate level of clearance can have access to the information.

**Asset classification** begins with identifying the responsible persons, or owners, for the

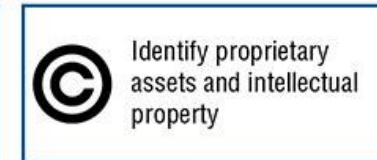
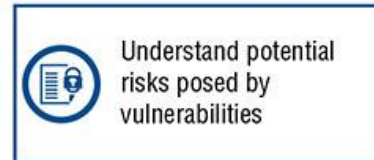


determining the responsible on-handling capabilities.

**Classifying the assets means** of classification dictate a information. Keep in mind regulatory requirements. organization establishes ( provide sufficient protection



level of sensitivity. The levels on will use to protect the n that exceeds legal and nism through which an an develop controls that





# Benefits of Classification



Make an accurate  
asset inventory



Gain insight into the  
environment



Optimize change,  
vulnerability, and patch  
management programs



Determine the best  
maintenance windows



Improve security  
controls and  
segmentation



Tailor protection of  
sensitive data



Identify rogue assets



Understand potential  
risks posed by  
vulnerabilities



Identify proprietary  
assets and intellectual  
property



Forecast costs of  
protection



Compliance /  
Regulatory controls

# Qualitative vs. Quantitative Asset Value Analysis

- Annual Loss Expectancy (ALE) = Single Loss Expectancy (SLE)  $\times$  Annual Rate of Occurrence (ARO)
- Single Loss Expectancy = Asset Value  $\times$  Exposure Factor
- Safeguard Value = (ALE Before – ALE After) – Annual Cost of Countermeasure

To compute the ALE, the first step is to determine the value of the asset (AV). As an example, assume the AV equals \$100,000. This helps determine the SLE because SLE equals AV multiplied by exposure factor (EF). EF is the probability the asset loss will occur. EF is expressed as a percentage in this example; if the EF is 30 percent, the SLE is \$30,000, as  $\$100,000 \times 0.30 = \$30,000$ .

Annualized rate of occurrence (ARO) is the estimated frequency of the threat occurring in one year. To calculate ALE, ARO is multiplied by SLE. So, continuing the example, if SLE is \$30,000 and the organization estimates ARO as 50 percent probability, the ALE is \$15,000 or  $(\$30,000 \times (0.5))$ .

# Qualitative vs. Quantitative Asset Value Analysis

CATEGORIES	ASPECTS	EXAMPLES
Tier 0	<p>Essential to several business units.</p> <p>May handle data that is extremely sensitive.</p> <p>Compromise could have a critical impact on the business's ability to function.</p> <p>Required to be available 100 percent of the time.</p>	<p>Domain controllers</p> <p>Databases</p> <p>Email servers</p> <p>File shares</p> <p>Client web servers</p> <p>Gateway network devices (firewalls, routers, and network-critical infrastructure)</p> <p>Anything else that shuts down business for a day if it breaks or turns off</p>
Tier 1	<p>Important but not necessarily critical to the organization.</p> <p>Essential to specific departments but not to the entire business.</p> <p>Compromise of any of these assets would have a moderate impact on the business's ability to function.</p>	<p>Development environments with critical data</p> <p>Redundant backup systems with critical data</p> <p>Department file shares</p> <p>Local network devices (switches, routers, firewalls, and segmentation devices)</p>
Tier 2	<p>Neither essential nor critical to daily operations.</p> <p>These systems are typically only used by a few people or a single individual.</p> <p>The compromise of any of these assets may inconvenience a few people but would not be a major disruption to business processes.</p>	<p>Workstations</p> <p>Laptops</p> <p>Mobile phones and tablets</p> <p>Printers</p> <p>Desk phones</p>
Significant Systems	<p>Any assets that handle or store data subject to compliance standards.</p> <p>Significant systems may fall into more than one category or may stand alone for categorization, because loss of the system would not disrupt operations, even if it is damaging to the business.</p>	<p>Cardholder data (CHD)—any system that stores, processes, or transmits CHD must align to PCI DSS.</p> <p>Protected health information (PHI)— medical data must be protected per the standards outlined in the Health Insurance Portability and Accountability Act (HIPAA)</p> <p>Financial data—this data may fall under certain privacy requirements outlined in the Financial Industry Regulatory Authority (FINRA)</p> <p>Classified government data (FISMA/FIPS)—for U.S. military and government</p>

# Categorization

## *Formal Assignment of Ownership*

Within an organization, the chief executive officer or authorized delegates have formal ownership responsibility. This responsibility includes the authority to represent the organization for the protection and security of the information asset.

Additional responsibilities of asset owners may include the following:

- Keeping the information asset inventory up to date
- Identifying the classification level of the information asset
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset
- Assessing and monitoring safeguards to ensure compliance and reporting situations of noncompliance
- Authorizing access for those who have a business need for the information
- Ensuring that access is removed from those who no longer have a business need for the information

# Categorization

## Information Technology Asset Management

- Change Management
- Configuration Management
- Software Library
- Monitoring and Reporting

## Software asset management (SAM)

- A sufficient SAM program consists of the following:
- Inventory of applications
- Current list of known vulnerabilities
- Prioritization of each vulnerability by risk level
- Each application patch level
- Actions to patch or apply alternative or compensating controls

- ***Software Licensing***

- Licensing Models
- End-user license agreement (EULA)
- A site license is a method to obtain multiple end-user licenses at one cost.
- A subscription software license is a multiple-user or organizational-level license option that generally includes software maintenance, product upgrades, and access to technical and developer support for a negotiated period of time.
- A perpetual license is like a subscription in that one fee is paid and a negotiated number of users can use the software. There will likely be a term of service that will include upgrades, updates, support, and maintenance from the developer or a representative.
- A consumptive license is a negotiated arrangement for an up-front payment for a specified period of time, too. The difference is that the arrangement also includes a pay-as-you-go cost for each use.

# Categorization

The process of determining the impact of the loss of confidentiality, integrity, or availability of the information to an organization.

# Data Classification Policy

Who will have access  
to the data

How the data  
is secured

How long the data is  
to be retained

What method(s)  
should be used to  
dispose of the data

Whether the data  
needs to be  
encrypted

The appropriate use  
of the data



# Activity: Applying Policy Considerations in Your Organization

## **INSTRUCTIONS**

Working with a partner, discuss how you would apply each of the policy considerations in your organization.

Who has access  
to the data

How the data  
is secured

How long the data  
is to be retained

What method(s) should  
be used to dispose of  
the data

Whether the  
data needs to  
be encrypted

The appropriate  
use of the data



# Examples of Classification Levels

- Government organizations might use following classification scheme:
  - Examples
    - Top Secret
    - Secret
    - Confidential
    - Sensitive But Unclassified (SBU)
    - Unclassified
- Commercial organizations might use following classification scheme:
  - Examples
    - **Confidential**
    - **Sensitive**
    - **Private**
    - **Proprietary**
    - **Public**

# Examples of Classification Levels

Classification	Description
Sensitive	A classification label applied to data which is treated as classified in comparison to the public data. Negative consequences may ensue if such kind of data is disclosed.
Confidential	It is the highest level in this classification scheme. This category is reserved for extremely sensitive data and internal data. A "Confidential" level necessitates the utmost care, as this data is extremely sensitive and is intended for use by a limited group of people, such as a department or a workgroup, having a legitimate need-to-know. A considerable amount of damage may occur for an organization given this confidential data is divulged. Proprietary data, among other types of data, falls into this category.
Private	Data for internal use only whose significance is great and its disclosure may lead to a significant negative impact on an organization. All data and information which is being processed inside an organization is to be handled by employees only and should not fall into the hands of outsiders.
Proprietary	Proprietary data is data that is disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as the technical specifications of a new product.
Public	The lowest level of classification whose disclosure will not cause serious negative consequences to the organization.

Classification	Description
Top Secret	It is the highest level in this classification scheme. The unauthorized disclosure of such information can be expected to cause exceptionally grievous damage to the national security.
Secret	Very restricted information. The unauthorized disclosure of such data can be expected to cause significant damage to the national security.
Confidential	A category that encompasses sensitive, private, proprietary and highly valuable data. The unauthorized disclosure of such data can be expected to cause serious, noticeable damage to the national security.
Sensitive But Unclassified (SBU)	SBU data is data that is not considered vital to national security, but its disclosure would do some harm. Many agencies classify data they collect from citizens as SBU. In Canada, the SBU classification is referred to as protected (A, B, C).
Unclassified	It is the lowest level in this classification scheme. Furthermore, this data is neither sensitive nor classified, and hence it is available to anyone through procedures identified in the Freedom of Information Act (FOIA).

# Classification – Done by Owners

- The individual who owns the data should decide the classification
- Owners should review the classification on a regular basis and adjust based on value at that particular time
  - Classification system should allow the increase or decrease in classification
  - Change needs to be documented to allow system to adjust based on new classification

# Purpose of Asset Classification

---

Ensure that information assets receive an appropriate level of protection

---

Provide security classifications that will indicate the need and priorities for security protection

---

Minimize risks of unauthorized information alteration

---

Avoid unauthorized disclosure

---

# Purpose of Asset Classification (continued)

---

Maintain competitive edge

---

Protect legal tactics

---

Comply with privacy laws, regulations, and industry standards

---

# Classification Benefits

Benefits of having classifications are

- Awareness among employees and customers of the organization's commitment to protect information
- Identification of critical information
- Identification of vulnerability to modification
  - Enable focus on integrity controls
- Sensitivity to the need to protect valuable information
  - Understanding the value of information
  - Meeting legal requirements

# Issues Related to Classification

Information is classified by the Information Owner or designate

- Human error
- Proper classification is dependent on ability and knowledge of the classifier
- Requires awareness of regulations and customer and business expectations
- Requires consistent classification method—often the decisions can be somewhat arbitrary
- Needs clear labeling of all classified items
- Must include support for declassification and destruction of assets

- *European Union*
- *Safe Harbor Transition to Privacy Shield*
- *Asia-Pacific Economic Cooperation Cross-Border Privacy Rules*
- *U.S. Data Privacy Laws and Guidelines*
- *The Privacy Act of 1974 (U.S.)*
- *Fair Information Practice Principles*
  - Consent
  - Access
  - Integrity
  - Enforcement
- ***Personal Information Protection and Electronic Documents Act (Canada)***
  - Accountability
  - Identifying Purposes
  - Consent
  - Limiting Collection
  - Limiting Use, Disclosure, and Retention
  - Accuracy
  - Safeguards
  - Openness
  - Individual Access
  - Challenging Compliance



# Module 3

---

## Information and Asset Ownership

# Module Objectives

1. Understand the importance of establishing accountability and responsibility for asset and information ownership and custodianship.
2. Explain accountabilities and responsibilities for protection of assets by owners, custodians, stewards, controllers, and processors.
3. Explain key terms associated with asset protection.

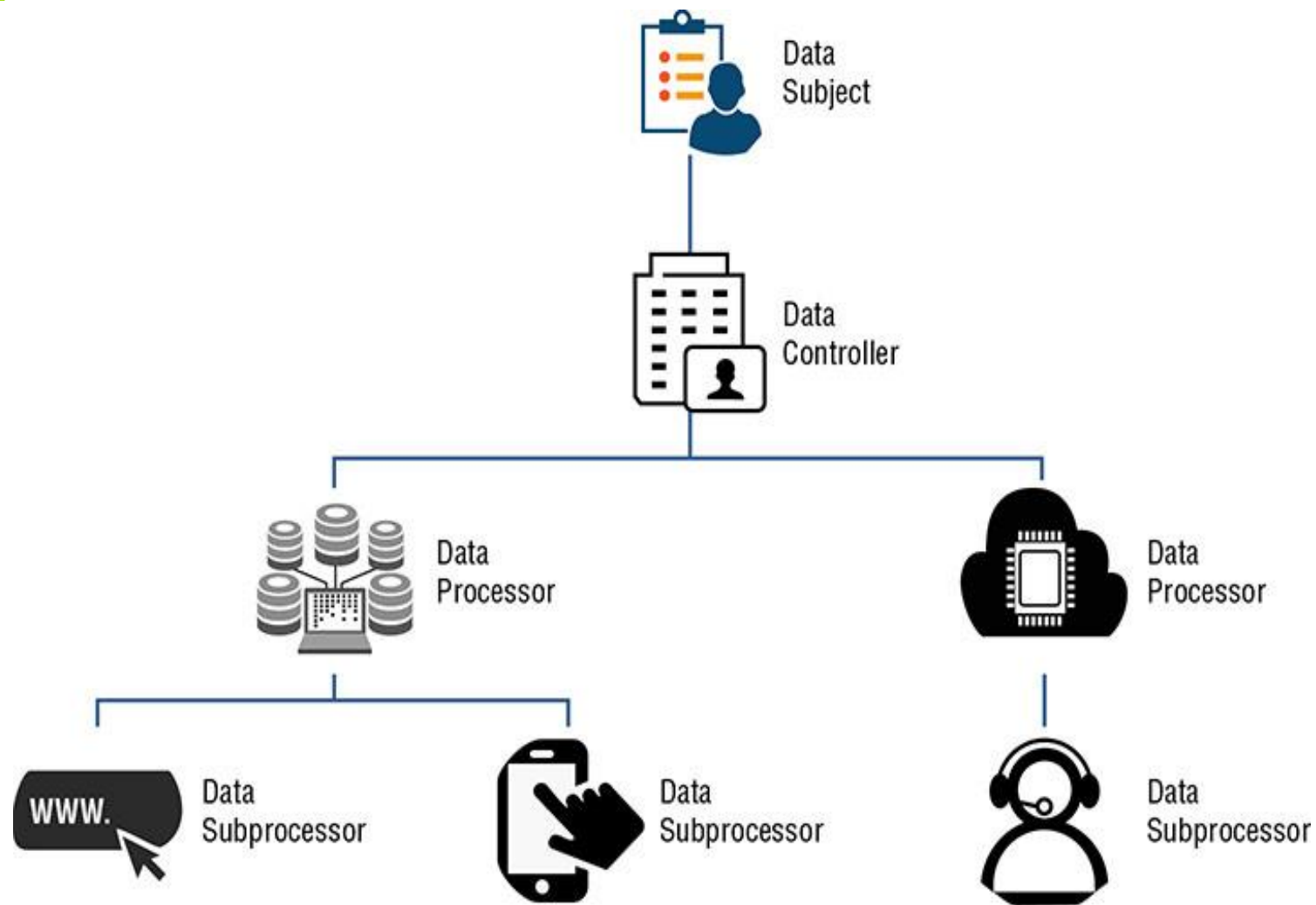
# Asset Protection and Classification

## Terminology

The following are key terms associated with asset management:

- Data subject
- Data owner
- Data custodian
- Data steward
- Personal data
- Processing
- Data controller
- Data processor

# DATA OWNERS



- *Data controller determines the need and how the data will be processed.*
- *Data processor is a separate legal entity processing data for the controller.*
  - *Cloud providers are generally considered data processors, as are market research firms, payroll companies, accountants.*

# Data Ownership

Accountable for important information security activities surrounding the lifecycle of information to:

- Protect it
- Ensure it is available to only those who require access
- Destroy it when it is no longer needed

# Information Owner

The data owner typically has the following example accountabilities:

- Determine the impact the information has on the mission of the organization.
- Understand the replacement cost of the information (if it can be replaced).
- Know when the information is inaccurate or no longer needed and should be destroyed.
- Determine who has a need for the information and under what circumstances the information should be released.

# Data Custodianship

Typical responsibilities include the following:

- Adherence to appropriate and relevant data policies, standards, procedures, baselines and guidelines
- Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
- Fundamental data maintenance, including but not limited to data storage and archiving
- Data documentation, including updates to documentation
- Assurance of quality and validation of any additions to data, including supporting periodic audits to ensure ongoing data integrity

# Difference Between Data Owner/Controller and Data Custodian/Processor

## Data Owner/Controller

The controller acts as the owner, therefore is accountable.

Accountable for the protection of data based on relevant national or community laws or regulations.

## Data Custodian/Processor

The processor processes data on behalf of the owners (example cloud provider).



# Difference Between Data Owner/Controller and Data Custodian/Processor (continued)

## Data Owner/Controller

The natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.

## Data Custodian/Processor

The processor processes data on behalf of the owners (example cloud provider). Therefore, is responsible for the adherence of policies, standards, procedures, baselines, and guidelines to ensure protection while in their custody.



# Activity: Understanding Accountability and Responsibility

## INSTRUCTIONS

Fill in each of the spaces with either the word “accountable” or “responsible” as it relates to protection of data and each of the roles:

Data Steward

Data Owner

Data Custodian

Data Processor

Data Controller

Data Subject



# Activity: Understanding Accountability and Responsibility – Answers

## INSTRUCTIONS

Fill in each of the spaces with either the word “accountable” or “responsible” as it relates to protection of data and each of the roles:

Data Steward  
(responsible)

Data Owner  
(accountable)

Data Custodian  
(responsible)

Data Processor  
(responsible)

Data Controller  
(accountable)

Data Subject  
(control)

# Module 4

---

## Protect Privacy

# Module Objectives

1. Understand how privacy of personal information is affected by today's technology.
2. Explain the expectations of subjects according to privacy laws and regulations.
3. Explain the importance of the OECD Guidelines on Privacy Protection.
4. Express the eight principles for privacy protection according to the OECD guidelines.
5. Understand the concept of collection limitation as it applies to privacy.

# Privacy – Introduction

- Individuals should have control over their personal information
- According to many data protection laws, personal information must be
  - Obtained fairly and lawfully
  - Used only for the original specified purpose
  - Adequate, relevant, and not excessive to purpose
  - Accurate and up to date
  - Not kept longer than necessary
  - Accessible to the subject
  - Kept secure
  - Not transmitted to a country without adequate level of protection

# OECD Privacy Guidelines

The OECD guideline principles are as follows:

Collection Limitation  
Principle

Data Quality Principle

Purpose Specification  
Principle

Use Limitation  
Principle

Security Safeguards  
Principle

Openness  
Principle

Individual  
Participation Principle

Accountability  
Principle

# Example – Collection Limitation Principle

There should be limits  
to the collection of data

Should be obtained by  
lawful and fair means

With the knowledge and  
consent of the subject



# Module 5

---

## Asset Retention

# Module Objectives

1. Understand asset retention and how retention policies are driven by organizational requirements.
2. Explain the reasons that drive data and records retention, including compliance or organizational requirements.
3. Understand the issues associated with long-term storage of assets.

# Establishing Information Governance and Retention Policies

Understand where the data exists

Classify and define data

Archive and manage data

# Building Effective Archiving and Data Retention Policies

Involve all stakeholders in the process

Establish common objectives for supporting archiving and data retention best practices within the organization

Monitor, review, and update documented data retention policies and archiving procedures

# Creating a Sound Record Retention Policy

---

Evaluate statutory requirements, litigation obligations, and business needs

---

Classify types of records

---

Determine retention periods and destruction practices

---

Draft and justify record retention policy

---

# Creating a Sound Record Retention Policy (continued)

---

Train staff

---

Audit retention and destruction practices

---

Periodically review policy

---

Document policy, implementation, training, and audits

---



## Activity: Review an Organization's Sample Policy

### **INSTRUCTIONS**

- Working with a partner, review the following sample policy
- For your assigned section, note your ideas about why each aspect of the policy is in place or the risks to the organization if the policy is not implemented
- Be prepared to share your thoughts with the group

# Important Considerations

- Who needs access to archived data and why?  
How fast do they need it?
- Do access requirements change as the archives age?
- How long do we need to keep the archived data? When should it be disposed of or deleted?



# Best Practices

---

Promote cross-functional ownership

---

Promote cross-functional ownership for archiving, retention, and disposal policies

---

Plan and practice data retention and orderly disposal

---

Key areas of focus: media, hardware, and personnel

---

# Examples of Data Retention Policies

---

European Document Retention Guide 2013

---

State of Florida Electronic Records and Records Management Practices,  
November 2010

---

The Employment Practices Code, Information Commissioner's Office,  
UK, November 2011

---

Wesleyan University, Information Technology Services Policy Regarding  
Data Retention for ITS-Owned Systems, September 2013

---

# Examples of Data Retention Policies (continued)

---

Visteon Corporation, International Data Protection Policy,  
April 2013

---

Texas State Records Retention Schedule (Revised 4th edition), effective  
July 4, 2012

---

# Retention Policies

Data protection requires that sensitive data, when processed for any purpose, should not be preserved for a longer time. Unfortunately, there is no universal agreement on how long the organization should retain data. However, the regulatory and legal requirements vary among business communities and countries. Every organization must follow data retention policies to thwart disaster, particularly when coping with the ongoing or pending litigations.

## *Examples of retention policies include:*

- The State of Florida Electronic Records and Records Management Practices, 2010
- The European Documents Retention Guide, 2012

## **How to Develop a Retention Policy?**

There are three fundamental questions that every retention policy must answer:

**1. How to Retain Data:**The data should be kept in a manner so that it is accessible whenever required. To make this accessibility certain, the organization should consider some issues, including:

- **The Taxonomy** is the scheme for data classification. This classification involves various categories, including the functional (human resource, product developments), the organizational (executive, union employee), or any combination of these.
- **The Normalization** develops tagging schemes that ensure that the data is searchable. In fact, non-normalized data is kept in various formats such as audio, video, PDF files, etc.

# Retention Policies

**2.How Long to Retain Data:** The classical data retention longevity approaches were: “thekeep everything” camp and “the keep nothing” camp. But in modern times, these approaches are dysfunctional in many circumstances, particularly when an organization encounters a lawsuit.

As aforementioned, there is no universal pact on data retention policies. Nevertheless, the rules of thumb or general guidelines for data retention longevity are described in Table 1.

**Table 1**

Types of Data	General Period of Retention
Business documents (e.g., meeting minutes)	7 years
Invoices	5 years
Accounts payable and receivable	7 years
Human resource files	7 years (for employee who leave ) or 3 years (for candidates who were not hired)
Tax records	4 years after taxes were paid
Legal correspondence	Permanently

**3. What Data to Retain:** The data related to business management, third party dealings, or partnership is valuable for any organization. Moreover, the counsel opinion has paramount importance, because he suggests what data is useful in the event of litigation.

# Module 6

---

## Data Security Controls

# Module Objectives

1. Define baseline protection.
2. Explain how baselines can help an organization achieve minimum levels of security associated with valuable assets.
3. Understand how baselines include security controls and how to implement them.
4. Describe baseline protection and scoping and tailoring in reference to asset protection.
5. Understand the different data states and explain how to secure each.
6. Explain the difference between end-to-end and link encryption as it relates to data in motion.

# Baselines

Minimum levels of security  
and protection  
requirements

Used as reference points  
to ensure minimum levels  
for assets



# Example Baselines and How They Can Be Used to Enforce Security Controls

Classification	Access	Encryption	Labeling	Monitoring
High	<ul style="list-style-type: none"><li>– Strong passwords</li><li>– Asset owner approves request, review, and termination</li><li>– NDA</li></ul>	<ul style="list-style-type: none"><li>– 128 bit symmetric encryption for creation, data-in-motion, data-at-rest</li></ul>	<ul style="list-style-type: none"><li>– Electronic watermark</li><li>– Physical watermark</li></ul>	<ul style="list-style-type: none"><li>– Real time using SIEM</li></ul>
Medium	<ul style="list-style-type: none"><li>– Passwords</li><li>– Asset owner approves request, review, and termination</li></ul>	<ul style="list-style-type: none"><li>– 128 bit encryption for data-in-motion</li></ul>	<ul style="list-style-type: none"><li>– None</li></ul>	<ul style="list-style-type: none"><li>– Timely</li></ul>
Low	<ul style="list-style-type: none"><li>– Asset owner approves request, review, termination</li></ul>	<ul style="list-style-type: none"><li>– None</li></ul>	<ul style="list-style-type: none"><li>– None</li></ul>	<ul style="list-style-type: none"><li>– None</li></ul>

# Baselines – Summary

- Consistent reference point
- Define minimum levels of protection to protect valuable assets
- Can be configurations for specific architectures and systems

# Considerations

Which parts of the enterprise or systems can be protected by the same baseline?

Should the same baseline be applied throughout the whole enterprise?

At what security level should the baseline aim?

How will the controls forming the baselines be determined?

# Objective of Baseline Protection

- Establish a minimum set of safeguards to protect assets that have value.

# Baseline Catalogs

Catalogs of baseline safeguards can provide comprehensive guidance on baseline creation. Could be obtained from

- International and national standards organizations
- Industry sector standards or recommendations
- Some other company, preferably with similar business objectives and of comparable size

# Generally Accepted Principles

---

Information System Security Objectives

---

Prevent, Detect, Respond, and Recover

---

Protection of Information While Being Processed, in Transit,  
and in Storage

---

External Systems Are Assumed to Be Insecure

---

# Generally Accepted Principles (continued)

---

Resilience for Critical Information Systems

---

Auditability and Accountability

---

# Scoping and Tailoring

**Scoping**—limiting general baseline recommendations by removing those that do not apply

**Tailoring**—altering baselines recommendations to apply more specifically





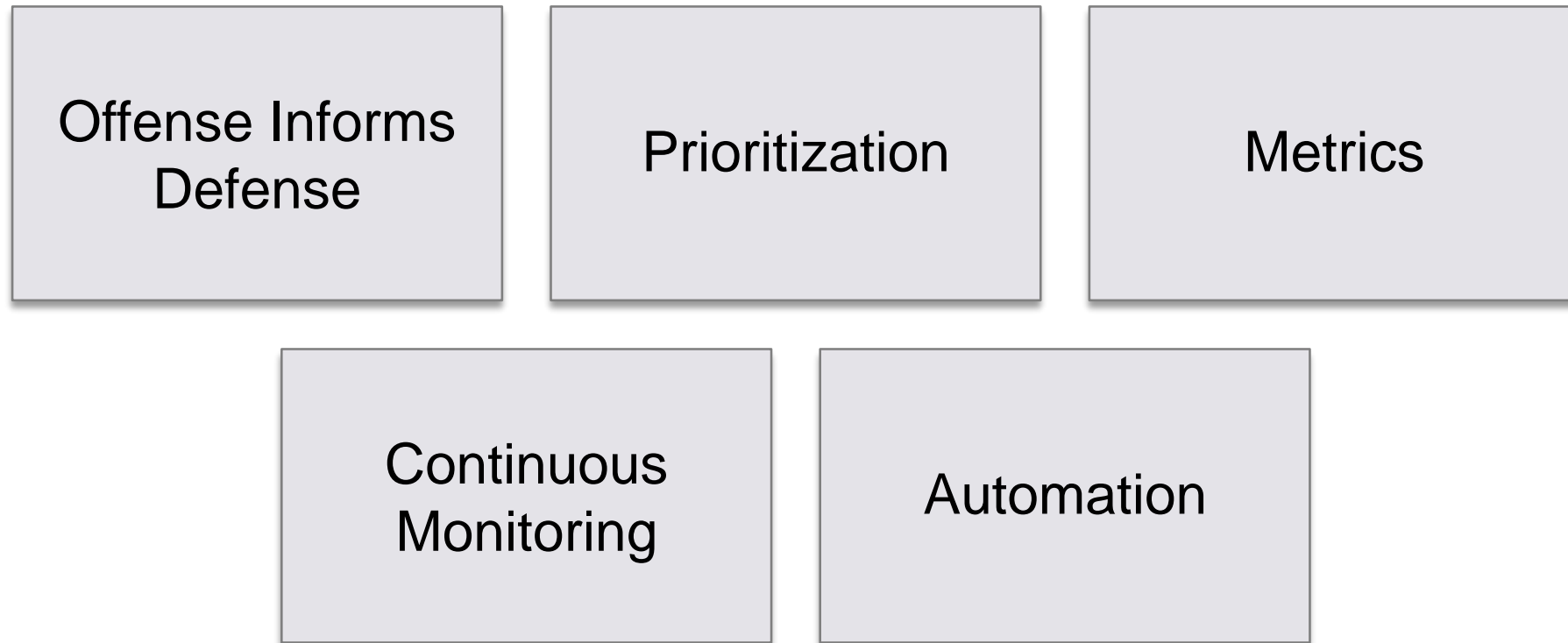
# Case: Standards Selection Review

## **INSTRUCTIONS**

Working on your own, review your assigned standards and prepare to introduce them to the rest of the class

# CSIS 20 Critical Security Controls Initiative

The five “critical tenets”:



# Current List of Critical Security Controls – Version

## 5.1

A list of critical security controls developed by the Council on CyberSecurity.

For more information see their white paper here:

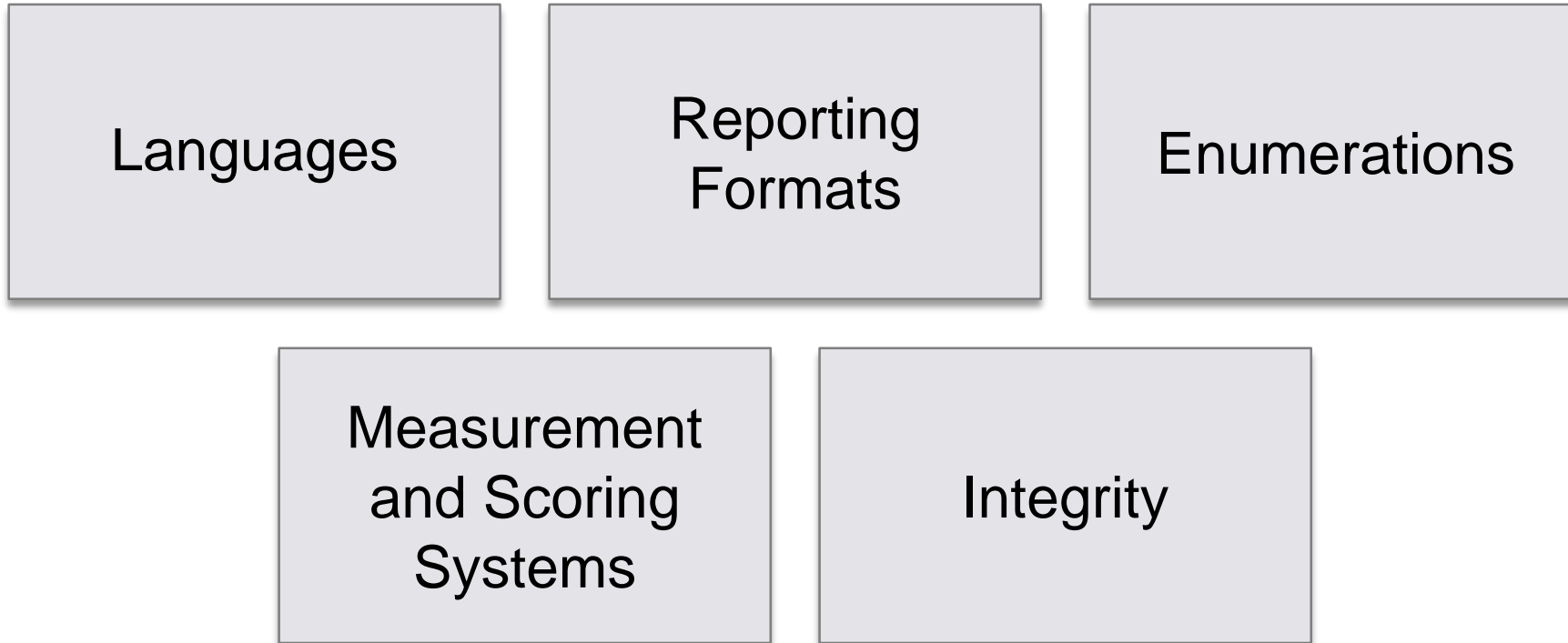
<https://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf>

# NIST Security Content Automation Protocol (SCAP)

Suite of specifications

Multi-purpose framework  
of specifications

# SCAP Version 1.2 Categories



# Framework for Improving Critical Infrastructure Cybersecurity

Common taxonomy for organizations to

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

# Framework Components

Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

# Framework Components (continued)

Framework  
Implementation  
Tiers

Framework Profile



# Data States



The diagram consists of three light gray circles arranged horizontally. Each circle contains text representing a different data state. The first circle on the left is labeled 'Data at Rest', the middle circle is labeled 'Data in Motion', and the third circle on the right is labeled 'Data in Use'.

Data  
at  
Rest

Data  
in  
Motion

Data  
in  
Use

# Protection of Data

- Data protection involves both data at rest, in motion, or in use
- But always based on classification

# Data at Rest

---

The protection of stored data is often a key requirement for an organization's sensitive information

---

Backup data, off-site storage, password files, and many other types of sensitive information need to be protected

---

This is typically done through the use of cryptographic algorithms

---

# Data at Rest – Description of Risk

Malicious actors may

- Affect confidentiality, integrity, and availability
- Examples:
  - Gain unauthorized physical or logical access to assets
  - Transfer information from the device to an attacker's system
  - Perform other actions that jeopardize the confidentiality of the information on a device

# Data at Rest – Recommendations

---

Implement controls such as encryption, access controls, and redundancy  
Develop and test an appropriate Data Recovery Plan

---

Use compliant encryption algorithm and tools

---

Whenever possible, use AES for the encryption algorithm because of its strength and speed

---

Follow strong password requirements

---

Do not use the same password from other systems

---

# Data at Rest – Recommendations (continued)

---

Use a secure password management tool to store sensitive information such as passwords and recovery keys

---

Where passwords need to be shared with other users, ensure that passwords are sent separately from the encrypted file

---

Do not write down the password and store it at the same location as the storage media

---

# Data at Rest – Recommendations (continued)

- After the valuable data is copied to a removable media:
  - Verify that the removable media works by following instructions to read the encrypted valuable data
  - If applicable, securely delete unencrypted valuable data following secure deletion guidelines
- Removable media should be labeled with:
  - Title
  - Data owner
  - Encryption date

# Data in Transit

Prevent the contents of the message from being revealed even if the message itself was:

- intercepted
- in transit



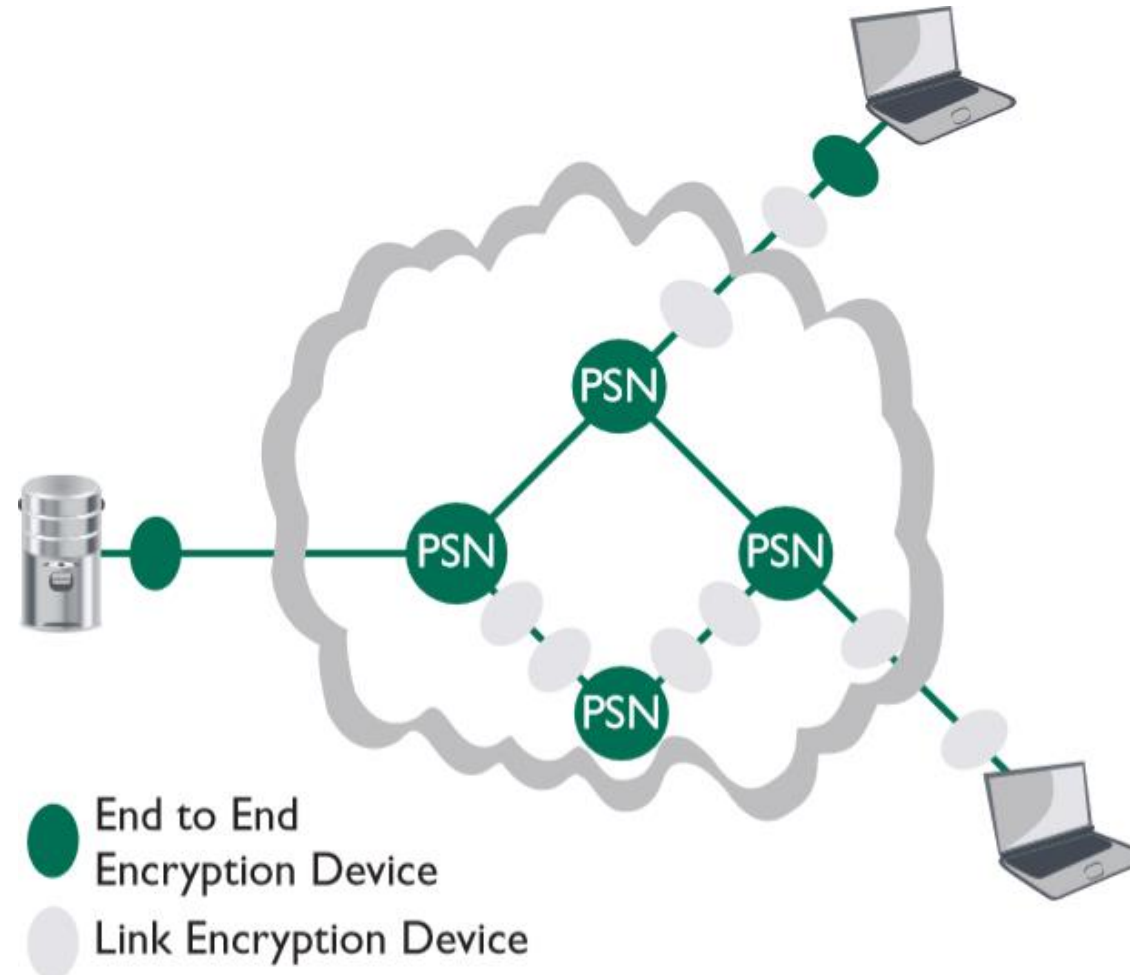
# Link Encryption

- Link encryption encrypts all of the data along a communications path
- Performed by service providers

# End-to-End Encryption

- Data is encrypted at the start of the transmission and remains encrypted until decrypted at the remote end
- Although data remains encrypted throughout the network, routing information needs to be visible

# Comparison of End-to-End and Link Encryption



# Data in Transit – Description of Risk

Malicious actors may intercept or monitor plaintext data transmitting across network and gain unauthorized access that jeopardizes confidentiality, integrity, or availability.

# Data in Transit – Recommendations

- Valuable data must be encrypted when transmitted across any network
- Email is not considered secure and must not be used to transmit valuable data

## Data in Transit – Recommendations (continued)

---

Where a device is reachable via web interface, web traffic must be transmitted over secure network protocols, using only strong security such as SSLv3, and TLS v1.1 or v1.2

---

Valuable data transmitted over email must be secured using cryptographically strong email encryption tools such as PGP or S/MIME

---

# Data in Transit – Recommendations (continued)

---

Non-web valuable data traffic should be encrypted via application-level encryption

---

Where an application database resides outside the application server, all connections between the database and application should be encrypted using FIPS-compliant cryptographic algorithms

---

## Data in Transit – Recommendations (continued)

---

Where application-level encryption is not available for non-web valuable data traffic, implement network-level encryption such as IPSec or SSH tunneling

---

Encryption should be applied when transmitting valuable data between devices in protected subnets with strong firewall controls

---

Good access controls to limit access should also be used

---

Redundancy controls need to be applied

---



# Data in Use

---

Can be particularly challenging to protect as data in use typically is in clear text

---

Data being processed on a architecture may be at risk, depending on the vulnerabilities on the architecture

---

If the application processing the data or the architecture is insecure, so is the data

---

# Data in Use – Recommendations

---

Concept of “enclave” protection is recommended

---

Secure dedicated portions of memory where the processing actually happens

---

Enclaves are isolated from other components of the architectures

---



# Activity: Data at Rest/Data in Transit Comparison

## INSTRUCTIONS

Working with a partner, complete the following table.

	Data at Rest	Data in Transit
Definition		
Risk Profile		
Recommendations (list at least two)		

# Examples of Insecure Network Protocols and Their Secure Alternatives

Action	Instead of this ...	Use these ...
Web Access	HTTP	HTTPS
File Transfer	FTP, RCP	FTPS, SFTP, SCP
Remote Shell	telnet	SSH v3
Remote Desktop	VNC	radmin, RDP

# Picking Encryption Algorithms

- Always choose the encryption algorithms that support longer key lengths as they generally provide stronger protection
- Since passwords are often used to control the keys within the cryptosystem, long complex passphrases are stronger than shorter passphrase

# Wireless Connections

When connecting to wireless networks to access a system handling valuable data, only connect to wireless networks employing cryptographically strong wireless encryption standards such as WPA2.

# Module 7

---

## Information and Asset Handling Requirements

# Module Objectives

1. Understand how media requires controls to protect its content
2. Understand labeling and marking requirements of assets that have been classified
3. Understand how the handling of media and assets that have been classified should be allowed only to those that are authorized
4. Understand how storage, retention, and destruction of assets is dictated by classification



# Media

---

Media storing sensitive information requires physical and logical controls

---

Media lacks the means for digital accountability when the data is not encrypted

---

For this reason, extensive care must be taken when handling sensitive media

---

# Marking

---

Storage media should have a physical label, identifying the sensitivity of the information contained

---

The label should clearly indicate if the media is encrypted

---

The label may also contain information regarding a point of contact and a retention period

---

When media is found or discovered without a label, it should be labeled at the highest level of sensitivity until the analysis reveals otherwise

---

# Handling

---

Only designated personnel should have access to sensitive media

---

Policies and procedures describing the proper handling of sensitive media should be communicated

---

Individuals responsible for managing sensitive media should be trained on the policies and procedures

---

# Storing

- Sensitive media should not be left lying about where a passerby could access it.
- Whenever possible, backup media should be encrypted and stored in a security container.

# Destruction

Media that is no longer needed or is defective should be defensibly destroyed rather than simply disposed of.

# Record Retention

- Information and data should be kept only as long as it is required
- Ensure that:
  - The organization understands the retention requirements for different types of data throughout the organization
  - The organization documents in a record's schedule the retention requirements for each type of information
  - The systems, processes, and individuals of the organization retain information in accordance with the schedule but not longer

# Module 8

---

## Data Remanence

# Module Objectives

1. Understand data remanence and its impact to the value of assets.
2. Explain the various options in addressing data remanence, including clearing, purging, and destruction.
3. Explain methods used to clear, purge, and destroy data.



# Data Remanence

- The residual physical representation of data that has been in some way erased
- After storage media is erased, there may be some physical characteristics that allow data to be reconstructed

# Data Remanence (continued)

- On a hard disk drive (HDD), the data is magnetically written onto the drive by altering the magnetic field of the hard drive platter
- Solid-state drives (SSDs) use flash memory to store data
- Three commonly accepted countermeasures employed to address data remanence in HDDs:
  - Clearing
  - Purging
  - Destruction

# Clearing

- The removal of sensitive data from storage devices so there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities
- The data may still be recoverable but not without special laboratory techniques

# Purging

The removal of sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique.

# Destruction

---

The storage media is made unusable for conventional equipment

---

Effectiveness of destroying the media varies

---

Destruction using appropriate techniques is the most secure method of preventing retrieval and referred to as “defensible destruction”

---

# Data Destruction Methods

Overwriting

Degaussing

Encryption

Shredding of  
smaller  
diskettes

Physically  
Destruction

Optical storage  
devices  
Sanitization

Sanitization  
for solid-state  
storage devices

Zeroing

Requirements of  
BSEN 15713

# MEMORY

***Cache Memory*** Cache memory is the fastest memory on the system, required to keep up with the CPU as it fetches and executes instructions. The data most frequently used by the CPU is stored in cache memory. The fastest portion of the CPU cache is the register file, which contains multiple registers. Registers are small storage locations used by the CPU to store instructions and data. The next fastest form of cache memory is Level 1 cache, located on the CPU itself. Finally, Level 2 cache is connected to (but outside) the CPU. SRAM (Static Random Access Memory) is used for cache memory.

## ***RAM and ROM***

RAM is volatile memory used to hold instructions and data of currently running programs. It loses integrity after loss of power. RAM memory modules are installed into slots on the computer motherboard. RAM is also becoming increasingly embedded in computer motherboards, making upgrading difficult, if not impossible.

ROM (Read Only Memory) is nonvolatile: data stored in ROM maintains integrity after loss of power. A computer Basic Input Output System (BIOS) Firmware is stored in ROM. While ROM is “read only,” some types of ROM may be written to via flashing, as we will see shortly in the “Flash Memory” section.

## ***DRAM and SRAM***

Static Random Access Memory (SRAM) is fast, expensive memory that uses small latches called “flip-flops” to store bits. Dynamic Random Access Memory (DRAM) stores bits in small capacitors (like small batteries), and is slower and cheaper than SRAM. The capacitors used by DRAM leak charge, and must be continually refreshed to maintain integrity, typically every few to a few hundred milliseconds, depending on the type of DRAM. Refreshing reads and writes the bits back to memory. SRAM does not require refreshing, and maintains integrity as long as power is supplied.

# MEMORY

## *Firmware*

Firmware stores small programs that do not change frequently, such as a computer's BIOS (discussed below), or a router's operating system and saved configuration. Various types of ROM chips may store firmware, including PROM, EPROM, and EEPROM.

PROM (Programmable Read Only Memory) can be written to once, typically at the factory. EPROMs (Erasable Programmable Read Only Memory) and EEPROMs (Electrically Erasable Programmable Read Only Memory) may be “flashed,” or erased and written to multiple times. The term “flashing” derives from the use of EPROMs: flashing ultraviolet light on a small window on the chip erased the EPROM. The window was usually covered with foil to avoid accidental erasure due to exposure to light. EEPROMs are the modern type of ROM, electrically erasable via the use of flashing programs. A Programmable Logic Device (PLD) is a field-programmable device, which means it is programmed after it leaves the factory. EPROMs, EEPROMS, and Flash Memory are examples of PLDs.

## *Flash Memory*

Flash memory (such as USB thumb drives) is a specific type of EEPROM, used for small portable disk drives. The difference is any byte of an EEPROM may be written, while flash drives are written by (larger) sectors. This makes flash memory faster than EEPROMs, but still slower than magnetic disks.



# MEMORY

## *Solid State Drives (SSDs)*

A Solid State Drive (SSD) is a combination of flash memory (EEPROM) and DRAM. Degaussing has no effect on SSDs. Also: while physical disks have physical blocks (“block 1” is on a specific physical location on a magnetic disk), blocks on SSDs are logical, and are mapped to physical blocks. Also: SSDs do not overwrite blocks that contain data: the device will instead write data to an unused block, and mark the previous block unallocated. A process called garbage collection later takes care of these old blocks: “Unused and unerased blocks are moved out of the way and erased in the background. This is called the ‘garbage collection’ process. Working in the background, garbage collection systematically identifies which memory cells contain unneeded data and clears the blocks of unneeded data during off-peak times to maintain optimal write speeds during normal operations.” [4] The TRIM command improves garbage collection. “TRIM is an attribute of the ATA Data Set Management Command. The TRIM function improves compatibility, endurance, and performance by allowing the drive to do garbage collection in the background. This collection eliminates blocks of data, such as deleted files.” [5] While the TRIM command improves performance: it does not reliably destroy data.

A ‘sector by sector overwrite’ behaves very differently on an SSD vs. a magnetic drive, and does not reliably destroy all data. Also, electronically shredding a file (overwriting the file’s data before deleting it, which we will discuss shortly) is not effective.

Tests performed by the Department of Computer Science and Engineering, University of California, San Diego found: “Overall, the results for overwriting are poor: while overwriting appears to be effective in some cases across a wide range of drives, it is clearly not universally reliable. It seems unlikely that an individual or organization expending the effort to sanitize a device would be satisfied with this level of performance.”

# MEMORY

Data on SSD drives that are not physically damaged may be securely removed via ATA Secure Erase. SanDisk provides the following details: “When the relevant secure erase command is executed on the SanDisk SSD, all blocks in the physical address space, regardless of whether they are currently or were previously allocated to the logical space, are completely erased (the “logical to physical mapping table” is also erased). Additionally, a new encryption key is generated and the old key is discarded. This erase operation does not overwrite the blocks like an HDD write or format command would. Data is written to flash on a page-level and a page must be completely erased before it can be written to again. Unlike HDDs, which may leave remnants of data in regions between tracks, an erased flash cell is restored to the same content it contained at the time it was manufactured. As in the case with an HDD, physical blocks that have been marked “bad” may still contain remnant user data. There is no way to access these blocks to overwrite them, and secure erase makes no attempt to do so. Because the secure erase operation also regenerates the internal encryption key, it is not possible to decrypt the data, even if it were accessible.” [7] The two valid options for destroying data on SSD drives are ATA secure erase and destruction. Destruction is the best method for SSD drives that are physically damaged.

# Media Destruction – Defensible Destruction

- Physically breaking the media apart
- Chemically altering the media into a non-readable, non-reverse-constructible state
- Phase transition
- For magnetic media, raising its temperature above the Curie Temperature

# Solid-State Drives (SSDs)

- SSDs use flash memory for data storage and retrieval
- Flash memory differs from magnetic memory in one key way: flash memory cannot be overwritten

# Solid-State Drive (SSD) Data Destruction

---

Unlike HDDs, overwriting is not effective for SSDs

---

SSD manufacturers include built-in sanitization commands that are designed to internally erase the data on the drive

---

Cryptographic erasure, or crypto-erase, takes advantage of the SSD's built-in data encryption

---

The best data destruction method is a combination of crypto-erase, sanitization, and targeted overwrite passes

---

# Cloud-Based Data Remanence

- Little to no visibility into the management and security of the data in many cases
- PaaS-based architectures can actually provide a solution for the issues raised by data remanence in the cloud
- Crypto-Erase / Crypto Shredding

# Data Security Controls

## Data Security Controls

Determining data security controls is a Herculean task. However, the standards, scoping, and tailoring are employed to choose the controls. Also, control's determination is affected by the situation either the data is in motion, at rest, or in use. Figure 1 shows the states of data.

**Scoping and Tailoring:** Scoping is a process to determine which standard will be used by the organization. The tailoring helps in customizing the standard for organizations.

Data in motion is data that is being transmitted across the network, while data at rest is stored on the hard drive. Either type needs unique controls for protection.

**Drive Encryption** is the control for the protection of data at rest. This control is recommended for all media and cellular devices that contain confidential information.

**Media Transportation and Storage** provides data protection through backup and facilitates data storage off site through physically movement or via networks.

**Protecting data in motion** requires the secure transit of data via networks. Table 2 shows the examples of insecure network protocols and their reliable solutions:

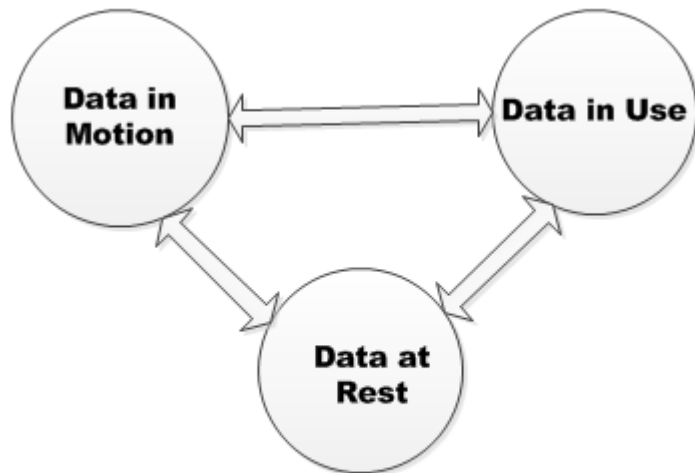


Figure 1 - The states of data

Table 2

Action	Not appropriate	Appropriate
Web Access	HTTP	HTTPS
File Transfer	FTP, RCP	FTPS, SFTP, SCP
Remote Desktop	VNC	RDP, radmin
Remote Shell	telnet	SSH3

# **DATA ISSUES WITH EMERGING TECHNOLOGIES**

- **Volumes of data**
- **Quality of data**
- **Sharing of data**
- **Data accuracy**

## **ENSURE APPROPRIATE ASSET RETENTION**

- Document the purpose of the policy.
- Identify who is affected by the policy.
- Identify the types of data and electronic systems covered by the policy.
- Define key terms, especially legal and technical terminology.
- Describe the requirements in detail from the legal, business, and personal perspectives.
- Outline the procedures for ensuring data is properly retained.
- Outline the procedures for ensuring data is properly destroyed.
- Clearly document the litigation exception process and how to respond to discovery requests.
- List the responsibilities of those involved in data retention activities.
- Build a table showing the information type and its corresponding retention period.
- Document the specific duties of a central or corporate data retention team if one exists.
- Appendix for additional reference information



# SECURITY CONTROL

- ISO 27001
- ISO 27005
- Control Objectives for Information and Related Technology (COBIT)
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense
- The Security Content Automation Protocol
- Cybersecurity Framework

## ***The Center for Internet Security Critical Security Controls***

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses

10. Limitation and Control of Network Ports
11. Data Recovery Capability
12. Secure Configurations for Network Devices
13. Boundary Defense
14. Data Protection
15. Controlled Access Based on the Need to Know
16. Wireless Access Control
17. Account Monitoring and Control
18. Security Skills Assessment and Appropriate Training to Fill Gaps
19. Application Software Security
20. Incident Response and Management
21. Penetration Tests and Red Team Exercises

# DATA PROTECTION METHODS

- **Data Backups**

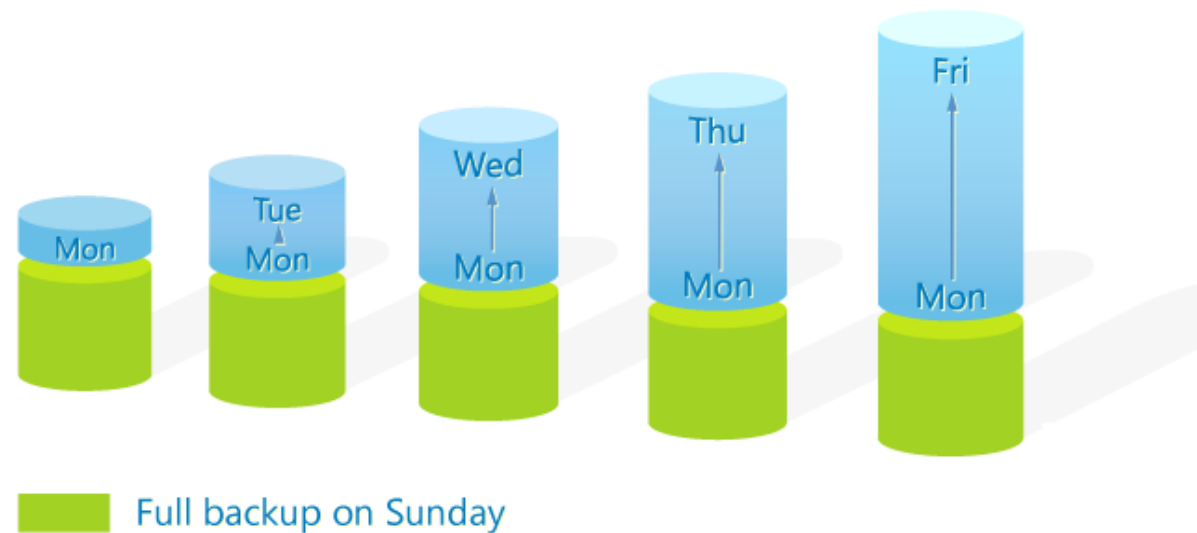
- The Traditional Backup Cycle
  - Full Backups
  - Differential Backups
  - Incremental Backups
  - Journaling

- **Other Backup Approaches**

- Database Mirroring
- Snapshots
- Availability Zones
- Vaulting
- Physical Media Backup
- LAN-Free and Server-Free Backup to Disk

- **Data Deduplication**

## DIFFERENTIAL BACKUP



### Pros:

- The process is much quicker than a full backup since it only takes a copy of what was changed.
- The backup copy itself takes far less storage space than when a full copy is created each day.

### Cons:

- The size of the data differences part grows with each cycle. If the cycle is long (e.g. the full backup is performed once a month and the differential is taken every day), at the end of it the size of the archive might be quite big and the process itself pretty lengthy.

# DATA PROTECTION METHODS

## Pros:

- The backup process is even faster than the differential job, not to mention the full backup. It is, in fact, so fast that it can be performed every hour or even minute.
- Each iteration of the backup job copies just the data that was changed. Therefore, only a small amount of storage is required each time.

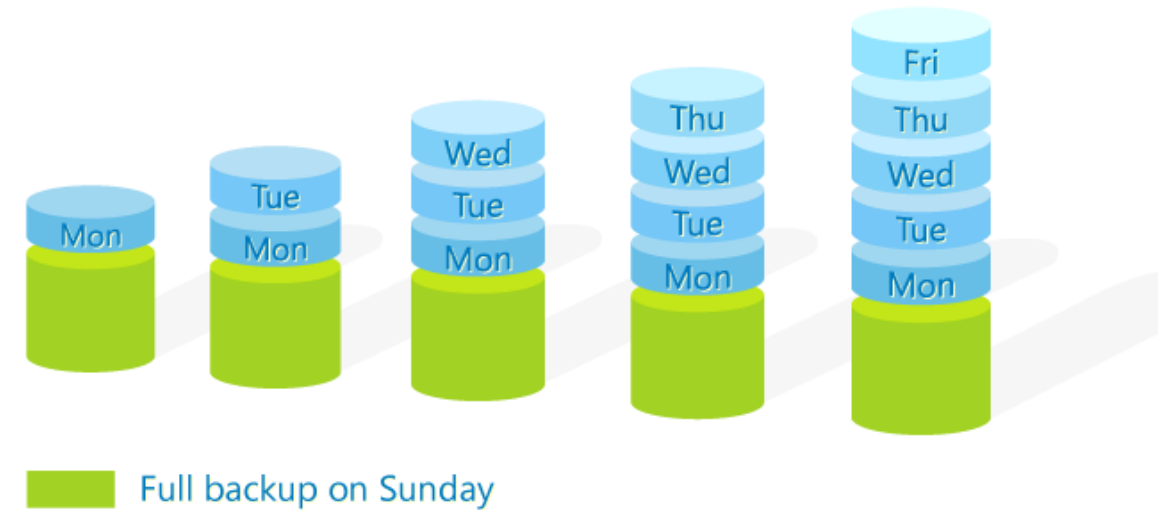
## Cons:

- The main disadvantage is that if a restore is attempted from the incremental backup, the time to restore can be lengthy, as each incremental volume has to be processed.
- In some cases, the backup software requires all iterations of the incremental backup for data restoration. If one of the pieces is missing – the restore is impossible.
- The restore process might take some time as the software needs to rebuild data from separate incremental pieces and also the last full backup piece too.

### *Database Mirroring*

Using database mirroring, a copy of the information is kept on two different servers, the principal and the mirror. The mirrored copy is a secondary copy and is not active until required. The mirrored copy is consistently synchronized with the principal database. The process assures maximum data availability and improves data recovery in the event there is corruption or loss of data in the primary database.

## INCREMENTAL BACKUP



### *Journaling*

Journal files are created for each update. They record metadata about the transaction and are created during the backup process. It is important to store the journal files separately from the data backups. Both are needed to complete a full restoration from a backup free of data corruption.

# DATA PROTECTION METHODS

## *Snapshots*

This technology is a process of making a virtual copy of a set of files, directories, or volumes as they appeared in a particular point in time. Snapshots are not backups. They are point-in-time copies. They lack the metadata that is included when using traditional backup applications. Using snapshots for backups helps storage systems because they do not degrade application performance during the backup process. They are useful for efficiently backing up large amounts of data.

## *Availability Zones*

In cloud computing technology, these designations are isolated locations within geographic regions of the cloud service provider's data center. The choice of locations for availability zones is based on business requirements, which might include regulatory compliance and *proximity to customers. The storage of backups replicated in multiple availability zones can decrease latency or protect resources.*

## *Vaulting*

An organization can send data off-site to be protected from hardware failures, theft, and other threats. The service can compress and encrypt the data for storage in the remote vault. Data is usually transported off-site using removable storage media such as magnetic tape or optical storage. Data can also be sent electronically via a remote backup service. The locations of data vaults vary. They can be underground in converted mines or decommissioned military sites. They can also be located in free-standing dedicated facilities or in a properly secured location within a building with other tenants.

## *Physical Media Backup*

A couple of common media used for backups are magnetic tape and computer disk. Because the physical media are able to store the data without a connection to network resources, the removable nature allows physical media to be used for transportation of stored data from one location to another.

# DATA PROTECTION METHODS

## *LAN-Free and Server-Free Backup to Disk*

*Different from local storage options like USB hard drives or connected devices, local area network-free (LAN-free) and server-free options like storage area networks (SANs) are faster and more efficient solutions for large amounts of data.*

The LAN-free or server-free architecture still requires connection to the devices with databases or media files.

A SAN is a dedicated high-speed network or subnetwork that interconnects and presents shared pools of storage devices to multiple servers. It moves storage resources off the common user network and reorganizes them. This enables each server to access shared storage as if it were a drive directly attached to the server. SANs are primarily used to enhance storage devices, such as disk arrays and tape libraries, accessible to servers but not other devices on the LAN.

Not to be confused with SANs, network-attached storage (NAS) is file-level computer data storage servers connected to a computer network providing data access to a heterogeneous group of clients. The storage servers are specialized for serving files by their hardware, software, or configuration. They are networked appliances that contain one or more storage drives, often arranged into logical, redundant storage containers. NAS removes the responsibility of file serving from other servers on the network.

Generally speaking, a NAS system uses TCP/IP as the communication protocol. A SAN uses Fibre Channel. Fibre Channel is a high-speed data transfer rate technology, up to 4 Gbps. Fibre Channel is also very flexible. It connects devices over long distances, up to 6 miles when optical fiber is used as the physical medium. Optical fiber is not required for shorter distances, however, because Fibre Channel also works using coaxial cable and ordinary telephone twisted pair.

# DATA PROTECTION METHODS

## *Data Deduplication*

Protecting data includes not storing unneeded data. A type of excess data that organizations struggle with is duplicated data, or redundant data. To reduce the amount of duplicate data, security professionals can implement deduplication processes and use tools to remove duplicate information. This will help data owners and processors efficiently store, back up, or archive only the amount of data required. Duplicate data can be an entire database, a file folder, or subfile data elements, or can be implemented in the storage environment at the block level.

## *Disaster Recovery Planning*

### *Disk Mirroring and Storage Replication*

Disk mirroring is a technique in which data is written to two duplicate disks simultaneously to ensure continuous availability. A mirrored volume is a complete logical representation of separate volume copies. The same data is written to disk storage on separate areas, or partitions, on the same disk volume to establish fault tolerance. In the event of a disk drive failure, the system can instantly switch to the other disk without any loss of data or service. Disk mirroring is used commonly in online database systems where it's critical that the data be accessible at all times. Disk mirroring provides assurance of data resiliency when one copy of the data is lost or corrupted.

# DATA PROTECTION METHODS

- **Raid Level 0**
- **Raid Level 1**
- **Raid Level 2**
- **Raid Level 3**
- **Raid Level 4**
- **Raid Level 5**
- **Raid Level 6.**
- **Raid Level 10**

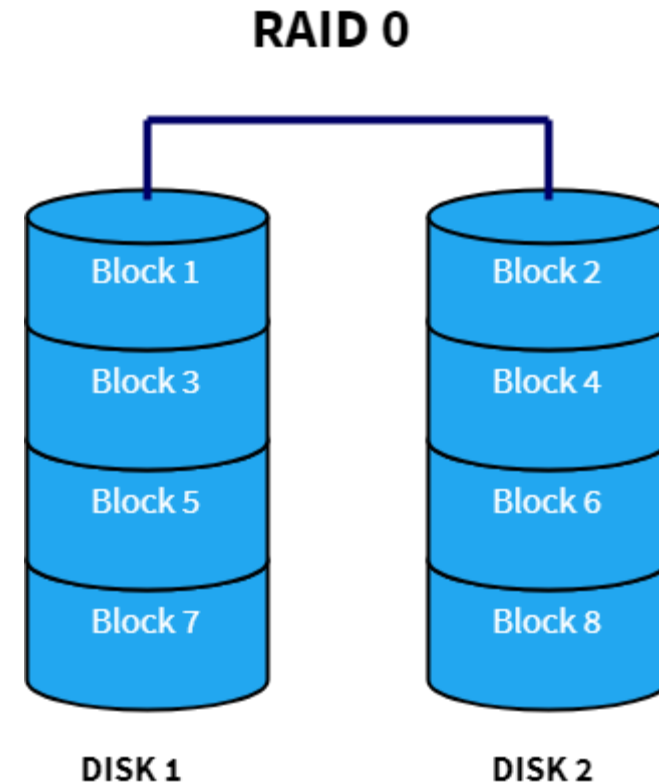
- **RAID 0** - Disk striping is used where speed is the primary objective.
- **RAID 1** - Disk mirroring is used for redundancy in case of single disk failure.
- **RAID 5** - Disk striping with parity is a good compromise for performance, redundancy and storage capacity.
- **RAID 10** - Disk mirroring with striping is used for redundancy in case of a single disk failure.

## **RAID 0**

- **Advantages**
  - RAID 0 offers great performance, both in read and write operations. There is no overhead caused by parity controls.
  - All storage capacity is used, there is no overhead.
  - The technology is easy to implement.
- **Disadvantages**
  - RAID 0 is not fault-tolerant. If one drive fails, all data in the RAID 0 array are lost. It should not be used for mission-critical systems.

## **Ideal use**

RAID 0 is ideal for non-critical storage of data that have to be read/written at a high speed, such as on an image retouching or video editing station. If you want to use RAID 0 purely to combine the storage capacity of two drives in a single volume, consider mounting one drive in the folder path of the other drive. This is supported in Linux, OS X as well as Windows and has the advantage that a single drive failure has no impact on the data of the second disk or SSD drive.



# DATA PROTECTION METHODS

## Advantages

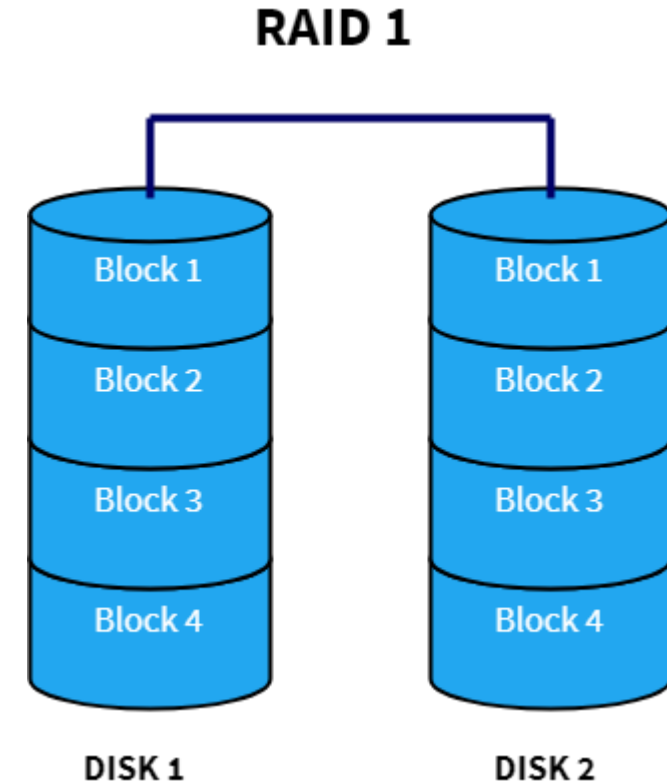
- RAID 1 offers excellent read speed and a write-speed that is comparable to that of a single drive.
- In case a drive fails, data do not have to be rebuild, they just have to be copied to the replacement drive.
- RAID 1 is a very simple technology.

## Disadvantages

- The main disadvantage is that the effective storage capacity is only half of the total drive capacity because all data get written twice.
- Software RAID 1 solutions do not always allow a hot swap of a failed drive. That means the failed drive can only be replaced after powering down the computer it is attached to. For servers that are used simultaneously by many people, this may not be acceptable. Such systems typically use hardware controllers that do support hot swapping.

## ***Ideal use***

RAID-1 is ideal for mission critical storage, for instance for accounting systems. It is also suitable for small servers in which only two data drives will be used.





# DATA PROTECTION METHODS

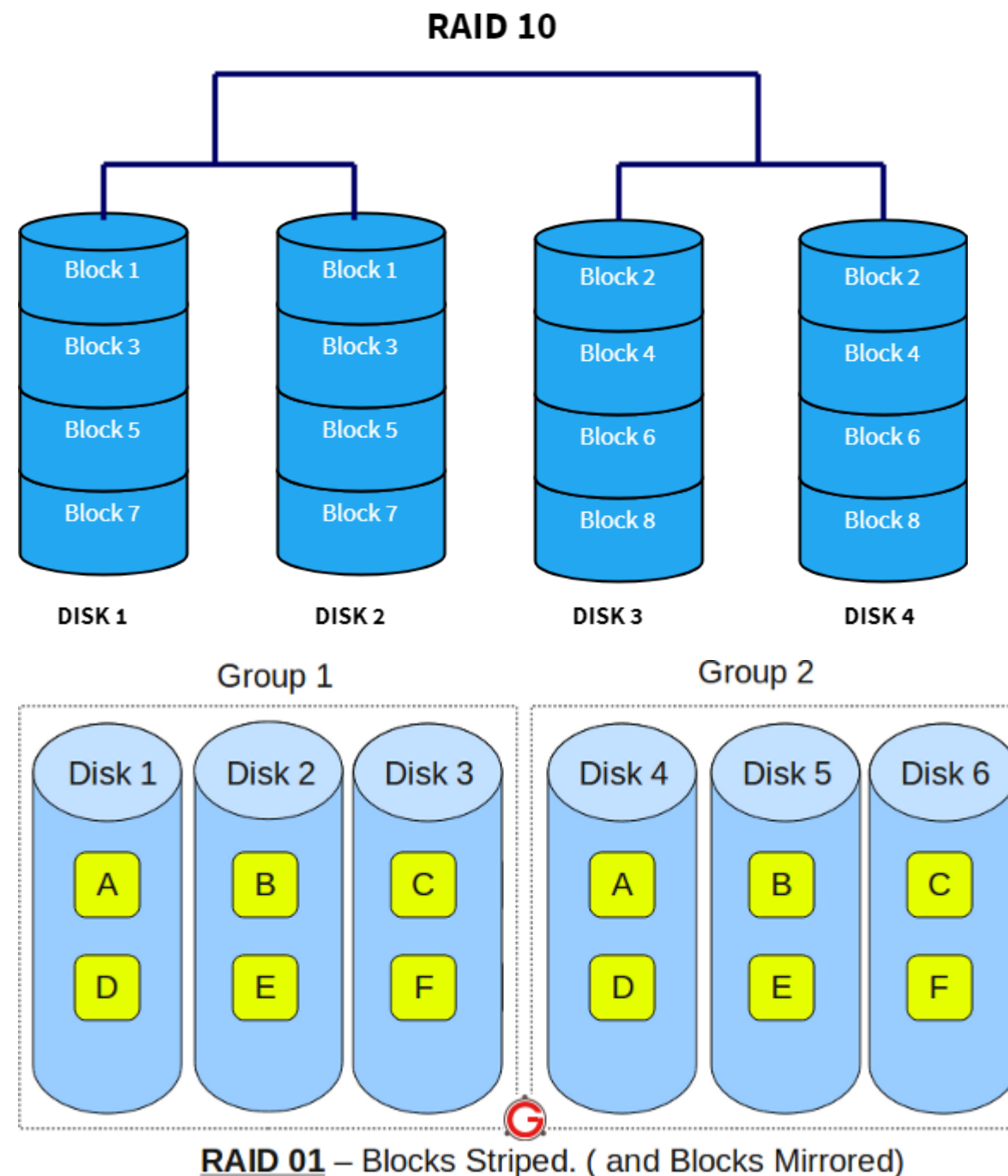
## RAID 10

### Advantages

- If something goes wrong with one of the disks in a RAID 10 configuration, the rebuild time is very fast since all that is needed is copying all the data from the surviving mirror to a new drive. This can take as little as 30 minutes for drives of **1 TB**.

### Disadvantages

- Half of the storage capacity goes to mirroring, so compared to large RAID 5 or RAID 6 arrays, this is an expensive way to have redundancy.
- RAID 01 is also called as RAID 0+1
- It is also called as “mirror of stripes”
- It requires minimum of 3 disks. But in most cases this will be implemented as minimum of 4 disks.
- To understand this better, create two groups. For example, if you have total of 6 disks, create two groups with 3 disks each as shown below. In the above example, Group 1 has 3 disks and Group 2 has 3 disks.
- Within the group, the data is striped. i.e In the Group 1 which contains three disks, the 1st block will be written to 1st disk, 2nd block to 2nd disk, and the 3rd block to 3rd disk. So, block A is written to Disk 1, block B to Disk 2, block C to Disk 3.
- Across the group, the data is mirrored. i.e The Group 1 and Group 2 will look exactly the same. i.e Disk 1 is mirrored to Disk 4, Disk 2 to Disk 5, Disk 3 to Disk 6.
- This is why it is called “mirror of stripes”. i.e the disks within the groups are striped. But, the groups are mirrored.



## ***Main difference between RAID 10 vs RAID 01***

- Performance on both RAID 10 and RAID 01 will be the same.
- The storage capacity on these will be the same.
- The main difference is the fault tolerance level. On most implementations of RAID controllers, RAID 01 fault tolerance is less. On RAID 01, since we have only two groups of RAID 0, if two drives (one in each group) fails, the entire RAID 01 will fail. In the above RAID 01 diagram, if Disk 1 and Disk 4 fails, both the groups will be down. So, the whole RAID 01 will fail.
- RAID 10 fault tolerance is more. On RAID 10, since there are many groups (as the individual group is only two disks), even if three disks fails (one in each group), the RAID 10 is still functional. In the above RAID 10 example, even if Disk 1, Disk 3, Disk 5 fails, the RAID 10 will still be functional.
- So, given a choice between RAID 10 and RAID 01, always choose RAID 10.

# DATA PROTECTION METHODS

## *Advantages*

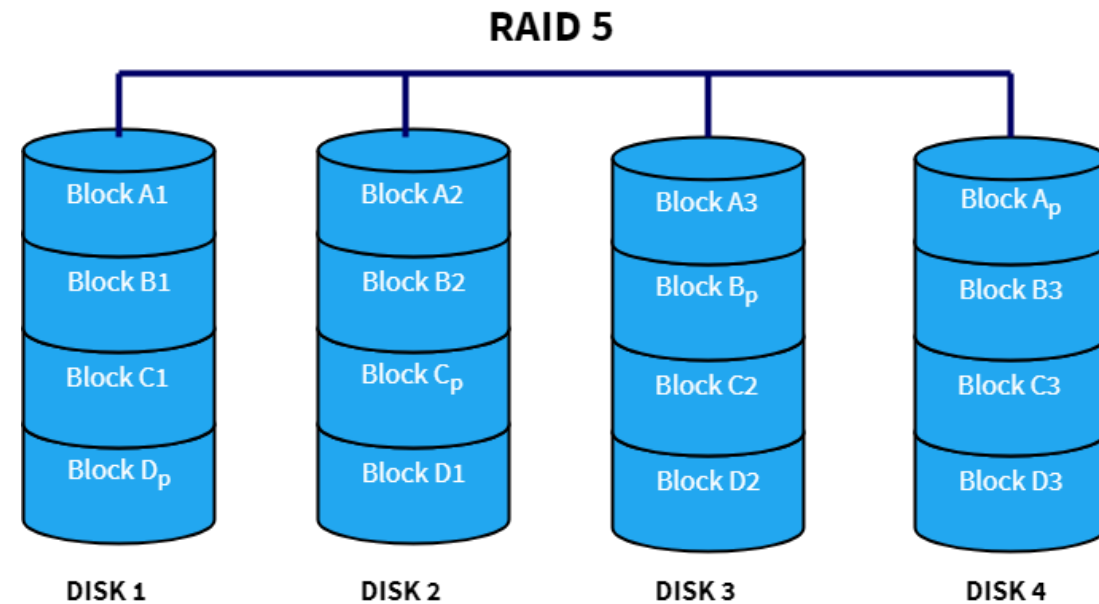
- Read data transactions are very fast while write data transactions are somewhat slower (due to the parity that has to be calculated).
- If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

## *Disadvantages*

- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. If one of the disks in an array using 4TB disks fails and is replaced, restoring the data (the rebuild time) may take a day or longer, depending on the load on the array and the speed of the controller. If another disk goes bad during that time, data are lost forever.

## *Ideal use*

RAID 5 is a good all-round system that combines efficient storage with excellent security and decent performance. It is ideal for file and application servers that have a limited number of data drives.



# DATA PROTECTION METHODS

## Advantages

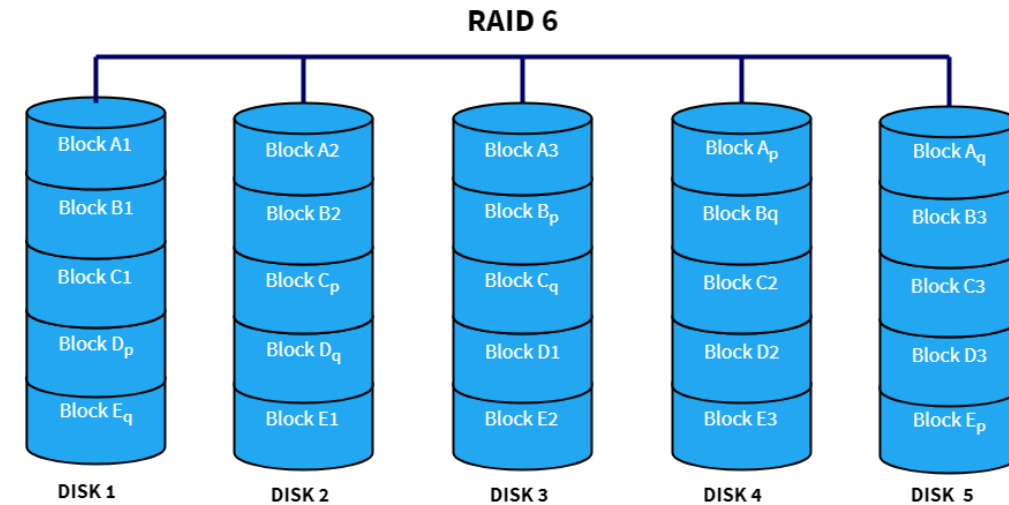
- *Like with RAID 5, read data transactions are very fast.*
- *If two drives fail, you still have access to all data, even while the failed drives are being replaced. So RAID 6 is more secure than RAID 5.*

## Disadvantages

- *Write data transactions are slower than RAID 5 due to the additional parity data that have to be calculated. In one report I read the write performance was 20% lower.*
- *Drive failures have an effect on throughput, although this is still acceptable.*
- *This is complex technology. Rebuilding an array in which one drive failed can take a long time.*

## Ideal use

*RAID 6 is a good all-round system that combines efficient storage with excellent security and decent performance. It is preferable over RAID 5 in file and application servers that use many large drives for data storage.*



# **ESTABLISH INFORMATION AND ASSET HANDLING REQUIREMENTS**

- MARKING AND LABELING
- HANDLING

## **DECLASSIFYING DATA**

- De-identification/Obfuscation/Anonymization
- Data Tokenization
- Destruction

# Module 9

---

## Domain Review

# Domain Summary

- Asset Security is all about the protection of valuable assets to an organization as those assets go through their lifecycle. Protection will always be done based on value.
- The value of the asset is expressed by its classification level that is initiated by the owner. The value must be monitored as the asset goes through its lifecycle.
- Classification, therefore, protects the asset based on its value. To protect the asset based on its classification, we need to implement baselines of minimum levels of security for each of the classification levels.

# Domain Summary (continued)

- To properly protect valuable assets, such as information, an organization requires the careful and proper implementation of ownership and classification processes that can ensure the assets receive the level of protection based on their value to the organization.



## Domain Summary (continued)

- The enormous increase in the collection of personal information by organizations has resulted in a corresponding increase in the importance of privacy considerations, and privacy protection constitutes an important part of the asset security domain. Individual privacy protection in the context of asset security includes the concepts of asset owners and custodians, processors, remanence, and limitations on collection and storage of valuable assets such as information. This also includes the important issue of retention as it relates to legal and regulatory requirements to the organization.

# Domain Summary (continued)

- Appropriate security controls must be chosen to protect the asset as it goes through its lifecycle, keeping in mind the requirements of each of the lifecycle phases and the handling requirements throughout.  
Therefore, understanding and applying proper baselines, scoping and tailoring, standards selection, and proper controls need to be understood by the security professional. This also requires the protection of data in different states, these states being data at rest, data in motion, and data in use. Encryption can be an effective tool in protecting all states.
- The asset lifecycle should end with the asset and data being destroyed securely, this is referred to as defensible destruction.

# Domain Review Questions

1. How can an asset classification program improve the organization's ability to achieve its goals and objectives?
  - A. By meeting the requirements imposed by the audit function
  - B. By controlling changes to production environments
  - C. By enhancing ownership principles
  - D. By specifying controls to protect valuable assets

# Answer

The correct answer is D.

Asset classification is implemented to allow the organization to protect assets based on the value of those assets, which is categorized by its classification level. Protection of assets, including information, is always done based on its value and, therefore, asset classification not only portrays its value, but also defines the protection requirements.

# Domain Review Questions

2. What is the correct order of the asset lifecycle phases?
- A. Create, use, share, store, archive, and destroy
  - B. Create, share, use, archive, store, and destroy
  - C. Create, store, use, share, archive, and destroy
  - D. Create, share, archive, use, store, and destroy

# Answer

The correct answer is C.

This is the correct order of the lifecycle phases of assets: create, store, use, share, archive, and destroy. This is according to the Securosis Blog. Asset classification, therefore, needs to be able to protect assets in whatever phase they are in.

# Domain Review Questions

3. Which of the following is the BEST definition of defensible destruction?
- A. The destruction of assets using defense approved methods
  - B. The destruction of assets using a controlled, legally defensible, and compliant way
  - C. The destruction of assets without the opportunity of the recovery of those assets
  - D. The destruction of assets using a method that may not allow attackers to recover data

# Answer

The correct answer is B.

The perfect definition of legally defensible destruction of assets, which should end the asset lifecycle, is eliminating data using a controlled, legally defensible, and regulatory compliant way.



# Domain Review Questions

4. In an environment where asset classification has been implemented to address the requirements of privacy protection, who in the following list is considered to be the “owner” and, therefore, has the accountability to ensure that the requirements for protection and compliance are addressed properly?
- A. Data processor
  - B. Data subject
  - C. Data controller
  - D. Data steward

# Answer

The correct answer is C.

In specific privacy legislation, the roles for accountability of protection of subject's personal privacy information is assigned to the data controller. They act as the "owner" and, therefore, have the accountability to protect based on legislative and legal requirements.

# Domain Review Questions

5. Which of the following is NOT a Organization for Economic Cooperation and Development (OECD) principle of privacy protection?
- A. Collection Limitation Principle
  - B. Right to be Forgotten Principle
  - C. Use Limitation Principle
  - D. Accountability Principle

# Answer

The correct answer is B.

The right to be forgotten principle is not a principle addressed in the OECD guidelines for privacy protection. It has been introduced and is part of privacy legislation in Europe and Argentina since 2006 and is part of the new General Data Protection Regulation (GDPR) to take effect in Europe.

# Domain Review Questions

6. Effective retention requirements for organizations requires all of the following EXCEPT for?
- A. Policy
  - B. Awareness, education, training
  - C. Understanding of requirements related to compliance
  - D. Data steward

# Answer

The correct answer is D.

A data steward may be required to address the proper protection of assets but is NOT a requirement to implement effective data retention methods in the organization. The other three answers are absolutely critical in addressing any important requirement, including retention.

# Domain Review Questions

7. Which of the following is not an objective of baseline security controls used in protecting assets?
- A. Specific steps that must be executed
  - B. Minimum level of security controls
  - C. May be associated with specific architectures and systems
  - D. A consistent reference point

# Answer

The correct answer is A.

Specific steps required to be executed are actually examples of procedures, not baselines. A baseline is a minimum level of security that must be achieved so that they can be consistently referenced and may be specific to certain architectures and systems.



# Domain Review Questions

8. Which of the following is the BEST definition of “scoping”?
- A. Altering baselines to apply more specifically
  - B. Modifying assumptions based on previous learned behavior
  - C. Limiting general baseline recommendations by removing those that do not apply
  - D. Responsible protection of assets based on goals and objectives

# Answer

The correct answer is C.

Limiting recommendations by removing those that do not apply is “scoping.” You are scoping to make sure things apply in the environments that you are trying to understand fully, from the perspective of protecting assets.

# Domain Review Questions

9. Which of the following is the BEST definition of an asset?
- A. A hardware system in a data center
  - B. People in specific valuable environments
  - C. Software running in a categorized environment
  - D. Any item perceived as having value

# Answer

The correct answer is D.

Even though A, B, and C may be considered to be assets, the question is asking for the best definition, not examples. An asset is anything that has value to the organization.

# Domain Review Questions

10. Which of the following is NOT an example of a data state?
- A. Data in motion
  - B. Data in use
  - C. Data in storage
  - D. Data at rest

# Answer

The correct answer is C.

Data in storage may be an example of data at rest, which is the correct terminology related to a data state. The three valid data states are data in motion, data at rest, and data in use. It is important to protect data in all three states and of course always based on value.