Information Security

Dr./ Ahmed Mohamed Rabie

Chapter 5

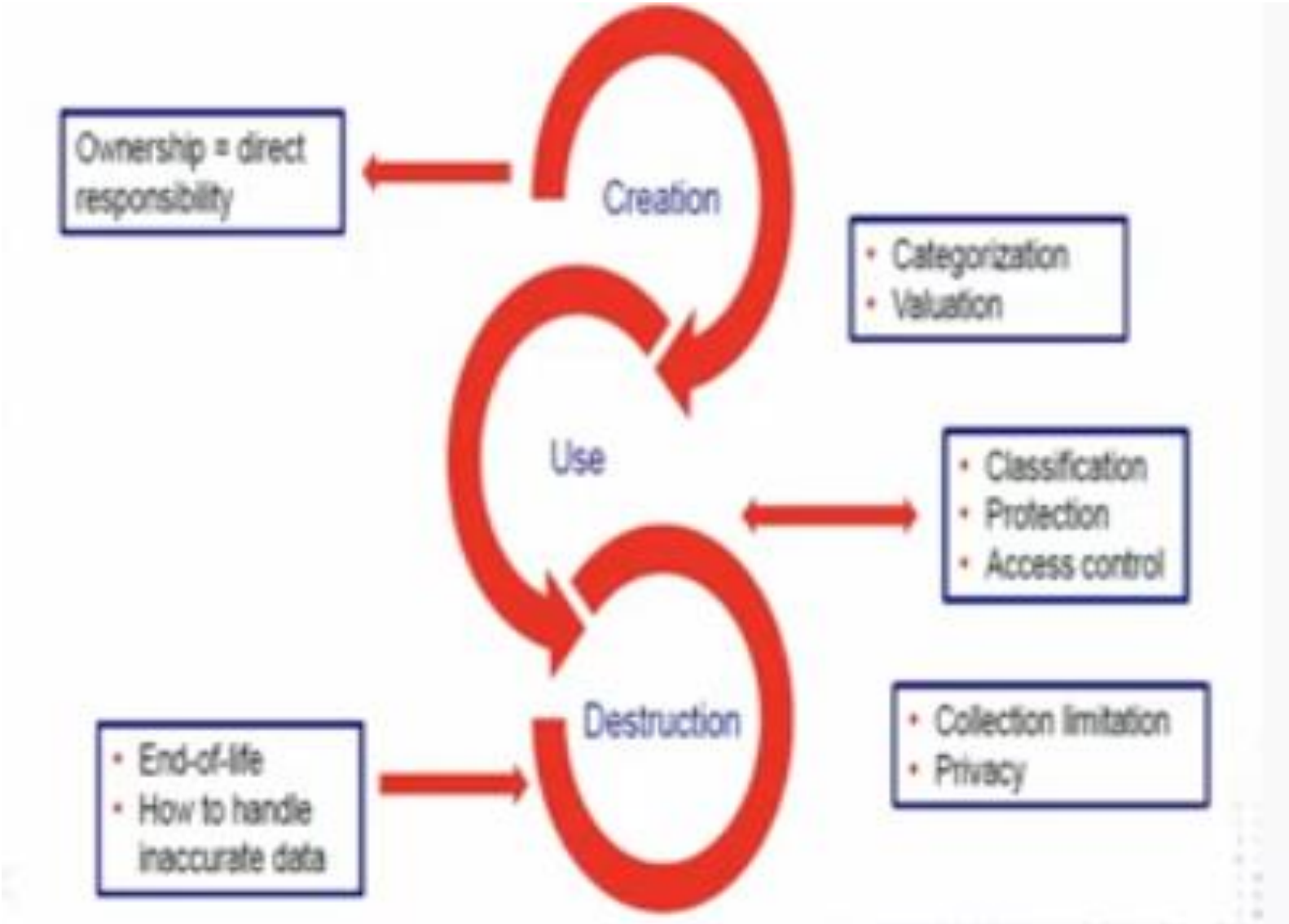
Assets Security

The **Asset Security** domain focuses on collecting, handling, and protecting information throughout its life cycle. A primary step in this domain is classifying information based on its value to the organization. All follow-on actions vary depending on the classification. For example, highly classified data requires stringent security controls. In contrast, unclassified data uses fewer security controls.

Information life cycle

Information Life Cycle is a process that helps organization to manage the flow of data throughout its lifecycle from initial creation through to destruction. While there are many interpretations as to the various phases of a typical data lifecycle, they can be summarized as follows:

- Creation
- Use
- Destruction


Ownership = direct responsibility
Creation
• Categorization
• Valuation
Use
• Classification
• Protection
• Access control
Destruction
• End-of-life
• How to handle inaccurate data
• Collection limitation
• Privacy

Data creation: Organizations generate vast amounts of data every second of every day. This data can include anything from transactional sales data to website clicks to PDFs. organizations are especially vulnerable to "dirty data" - the collection of inaccurate, incomplete, inconsistent, or duplicate data. "Dirty Data" is often the result of manual error but can be caused by more malicious factors such as data poisoning.

Data usage: What is the value of your data? How are you synthesizing the results of data analytics? This is the phase where you align value with action. How is your data used and moved around your enterprise? Maybe you incorporate feedback from end-users into product enhancement opportunities? Roles need to be defined around who has access to sensitive data. This involves ensuring that data flows seamlessly between various systems, dashboards and analytics tools. Encryption and other data obfuscation methods are often leveraged to ensure data confidentiality.

Destruction is the final stage in the life cycle of media and is the most secure method of sanitizing media. When destroying media it's important to ensure that the media cannot be reused or repaired and that data cannot be extracted from the destroyed media. Methods of destruction include incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals. Some organizations remove the platters in highly classified disk drives and destroy them separately.

Classifying and Labeling Assets

One of the first steps in asset security is **classifying and labeling assets**. Organizations often include classification definitions within a security policy. Personnel then label assets appropriately based on the security policy requirements. In this context, assets include sensitive data, the hardware used to process it, and the media used to hold it.

Sensitive data is any information that isn't public or unclassified. It can include confidential, proprietary, protected, or any other type of data that an organization needs to protect due to its value to the organization, or to comply with existing laws and regulations.

1- Personally Identifiable Information (PII) is any information that can identify an individual. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 provides a more formal definition:

Any information about an individual maintained by an agency, including:

- any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

- any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

The key is that organizations have a responsibility to protect PII. This includes PII related to employees and customers. Many laws require organizations to notify individuals if a data breach results in a compromise of PII.

2- **Protected health information (PHI)** is any health-related information that can be related to a specific person. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of PHI. HIPAA provides a more formal definition of PHI: Health information means any information, whether oral or recorded in any form or medium, that :-

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

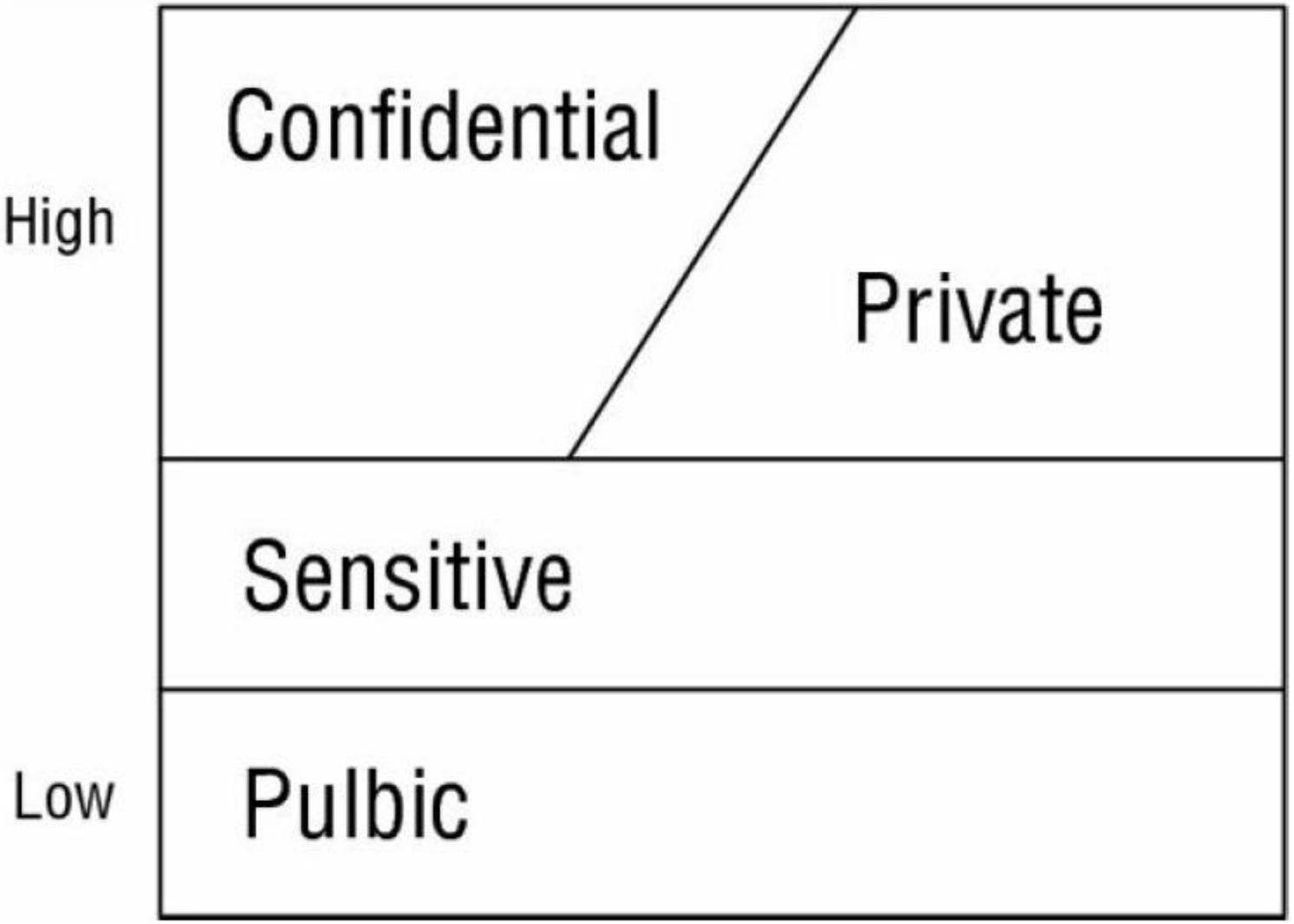
Some people think that only medical care providers such as doctors and hospitals need to protect PHI. However, HIPAA defines PHI much more broadly. Any employer that provides, or supplements, health-care policies collects and handles PHI. It's very common for organizations to provide or supplement health-care policies, so HIPAA applies to a large percentage of organizations in the US.

Organizations typically include data classifications in their security policy, or in a separate data policy. A **data classification** identifies the value of the data to the organization and is critical to protect data confidentiality and integrity. The policy identifies classification labels used within the organization. It also identifies how data owners can determine the proper classification, and personnel should protect data based on its classification.

- **Government data classifications** include top secret, secret, confidential, and unclassified. Anything above unclassified is sensitive data, but clearly, these have different values. The US government provides clear definitions for these classifications. As you read them, note that the wording of each definition is close except for a few key words. Top secret uses the phrase "exceptionally grave damage," secret uses the phrase "serious damage," and confidential uses the term "damage."

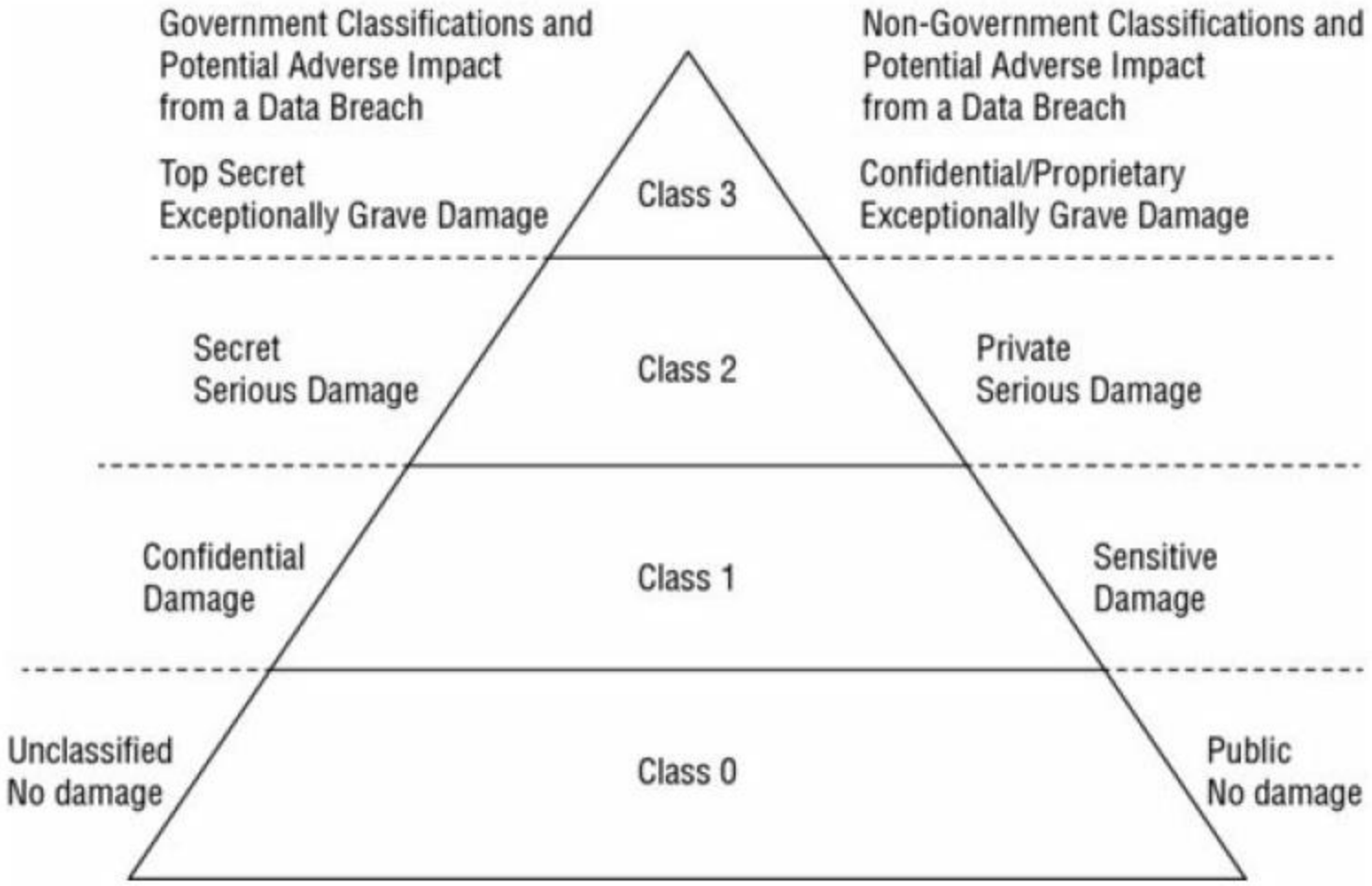

Top Secret
Secret
Confidential
Unclassified

- **Nongovernment (civilian) organizations** rarely need to classify their data based on potential damage to the national security. However, management is concerned about potential damage to the organization. For example, if attackers accessed the organization's data, what is the potential adverse impact? In other words, an organization doesn't just consider the sensitivity of the data but also the criticality of the data. They could use the same phrases of "exceptionally grave damage," "serious damage," and "damage" that the US government uses when describing top secret, secret, and confidential data.



Commercial business/private sector classification levels

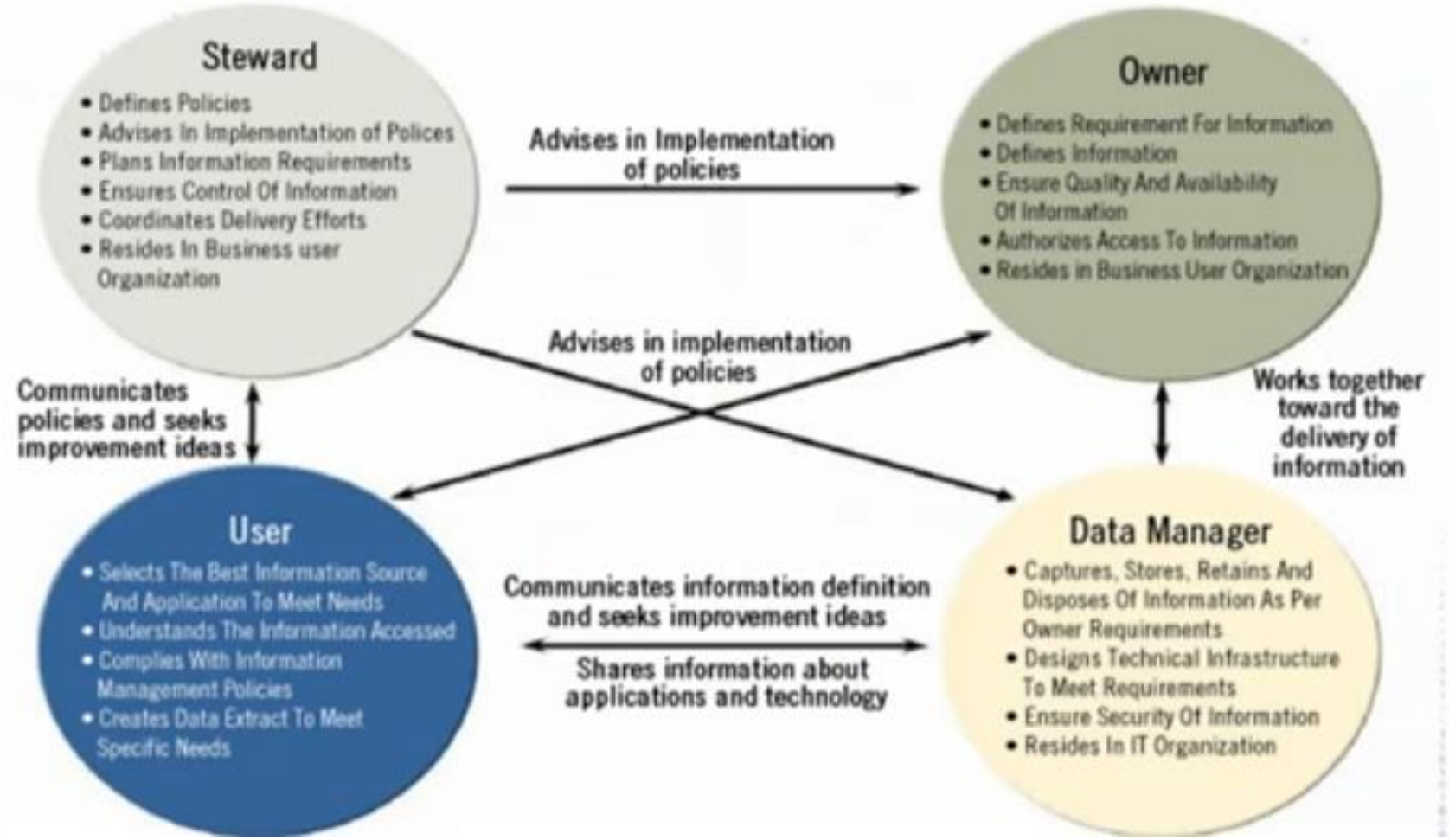
Both government and non government classifications identify the relative value of the data to the organization, with top secret representing the highest classification for governments and confidential representing the highest classification for organizations. However, it's important to remember that organizations can use any labels they desire. Sensitive information is any information that isn't unclassified (when using the government labels) or isn't public (when using the civilian classifications).



Data classifications

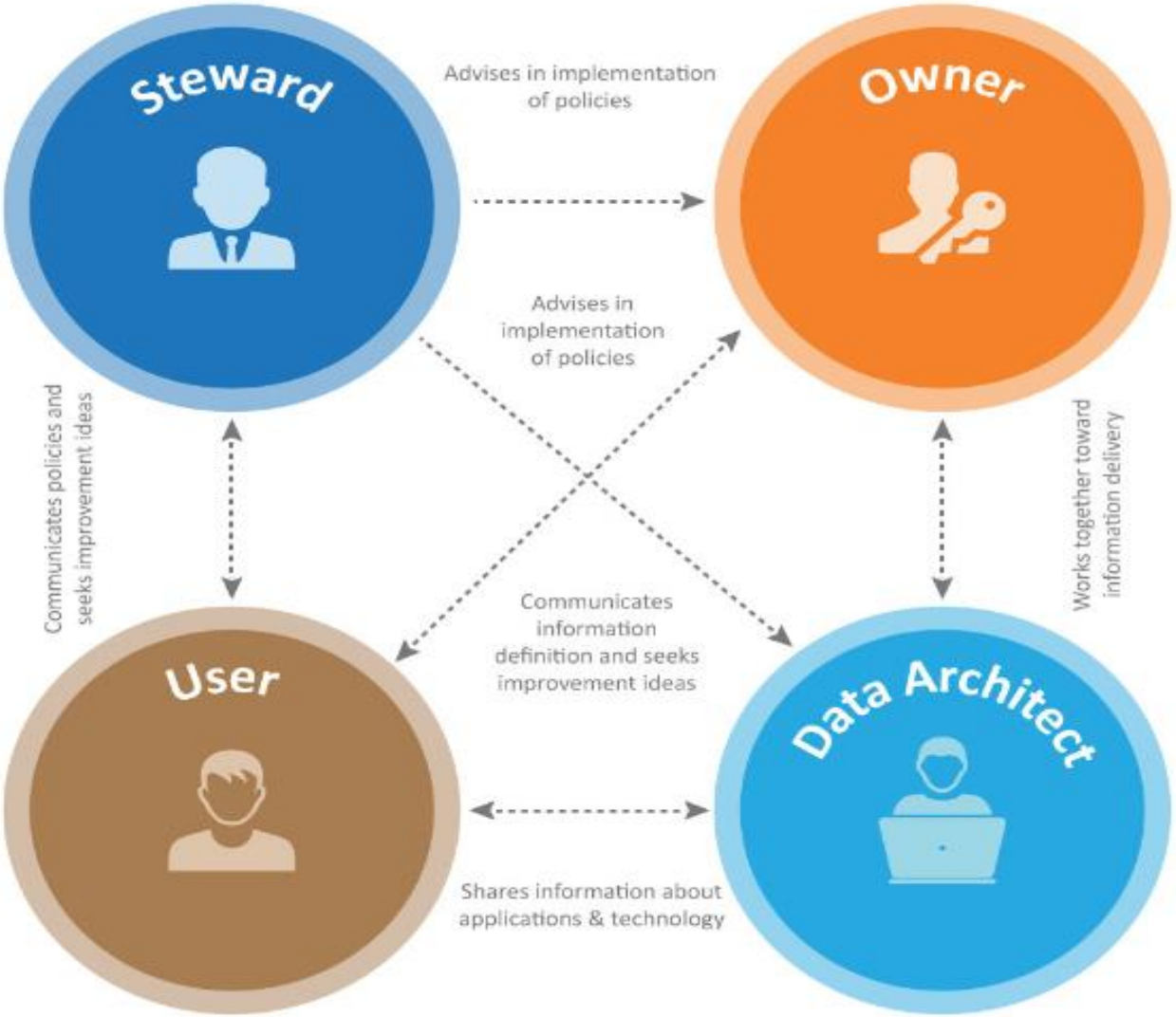
Data Governance

Data governance (DG) is the process of managing the availability, usability, integrity and security of the data in enterprise systems, based on internal data standards and policies that also control data usage. Effective data governance ensures that data is consistent and trustworthy and doesn't get misused. It's increasingly critical as organizations face new data privacy regulations and rely more and more on data analytics to help optimize operations and drive business decision-making.


Steward
• Defines Policies
• Advises In Implementation of Polices
• Plans Information Requirements
• Ensures Control Of Information
• Coordinates Delivery Efforts
• Resides In Business user Organization
Advises in Implementation of policies
Owner
• Defines Requirement For Information
• Defines Information
• Ensure Quality And Availability Of Information
• Authorizes Access To Information
• Resides in Business User Organization
Advises in implementation of policies
Communicates policies and seeks improvement ideas
Works together toward the delivery of information
User
• Selects The Best Information Source And Application To Meet Needs
• Understands The Information Accessed
• Complies With Information Management Policies
• Creates Data Extract To Meet Specific Needs
Communicates information definition and seeks improvement ideas
Shares information about applications and technology
Data Manager
• Captures, Stores, Retains And Disposes Of Information As Per Owner Requirements
• Designs Technical Infrastructure To Meet Requirements
• Ensure Security Of Information
• Resides In IT Organization

1- Data Ownership: When a personal device is used for business tasks, comingling of personal data and business data is likely to occur. Some devices can support storage segmentation, but not all devices can provide data-type isolation. Establishing data ownership can be complicated. For example, if a device is lost or stolen, the company may wish to trigger a remote wipe, clearing the device of all valuable information.

However, the employee will often be resistant to this, especially if there is any hope that the device will be found or returned. A wipe may remove all business and personal data, which may be a significant loss to the individual especially if the device is recovered, because then the wipe would seem to have been an overreaction. Clear policies about data ownership should be established.


Steward
Owner
User
Data Architect
Advises in implementation of policies
Advises in implementation of policies
Communicates policies and seeks improvement ideas
Communicates information definition and seeks improvement ideas
Works together toward information delivery
Shares information about applications & technology

2- A data steward is an oversight or data governance role within an organization, and is responsible for ensuring the quality and fitness for purpose of the organization's data assets, including the metadata for those data assets. A data steward may share some responsibilities with a data custodian, such as the awareness, accessibility, release, appropriate use, security and management of data. A data steward would also participate in the development and implementation of data assets. A data steward may seek to improve the quality and fitness for purpose of other data assets their organization depends upon but is not responsible for.

3- Users: A user is any person who accesses data via a computing system to accomplish work tasks. Users have access to only the data they need to perform their work tasks. You can also think of users as employees or end users.

4- The Data Governance Manager runs the Data Governance effort and is the head of the Data Governance Program Office. While the Data Governance Manager has many tasks, those most associated with maintaining effective Data Stewardship include:

- Managing and ensuring adequate staffing levels for the Data Governance Program Office.
- Ensuring that all appropriate business functions are represented on the Data Governance Board and Data Stewardship Council.

- Obtaining appropriate involvement from support organizations.
- Reporting to the Data Governance Board on Data Governance performance.
- Ensuring that Data Governance and Data Stewardship processes are inserted into and aligned with appropriate enterprise processes

Handling refers to the secure transportation of media through its lifetime. Personnel handle data differently based on its value and classification, and as you'd expect, highly classified information needs much greater protection. Even though this is common sense, people still make mistakes. Many times people get accustomed to handling sensitive information and become lackadaisical with protecting it.

Policies and procedures need to be in place to ensure that people understand how to handle sensitive data. This starts by ensuring systems and media are labeled appropriately. These controls verify that sensitive information is handled appropriately before a significant loss occurs. If a loss does occur, investigators use audit trails to help discover what went wrong. Any incidents that occur because personnel didn't handle data appropriately should be quickly investigated and actions taken to prevent a reoccurrence.

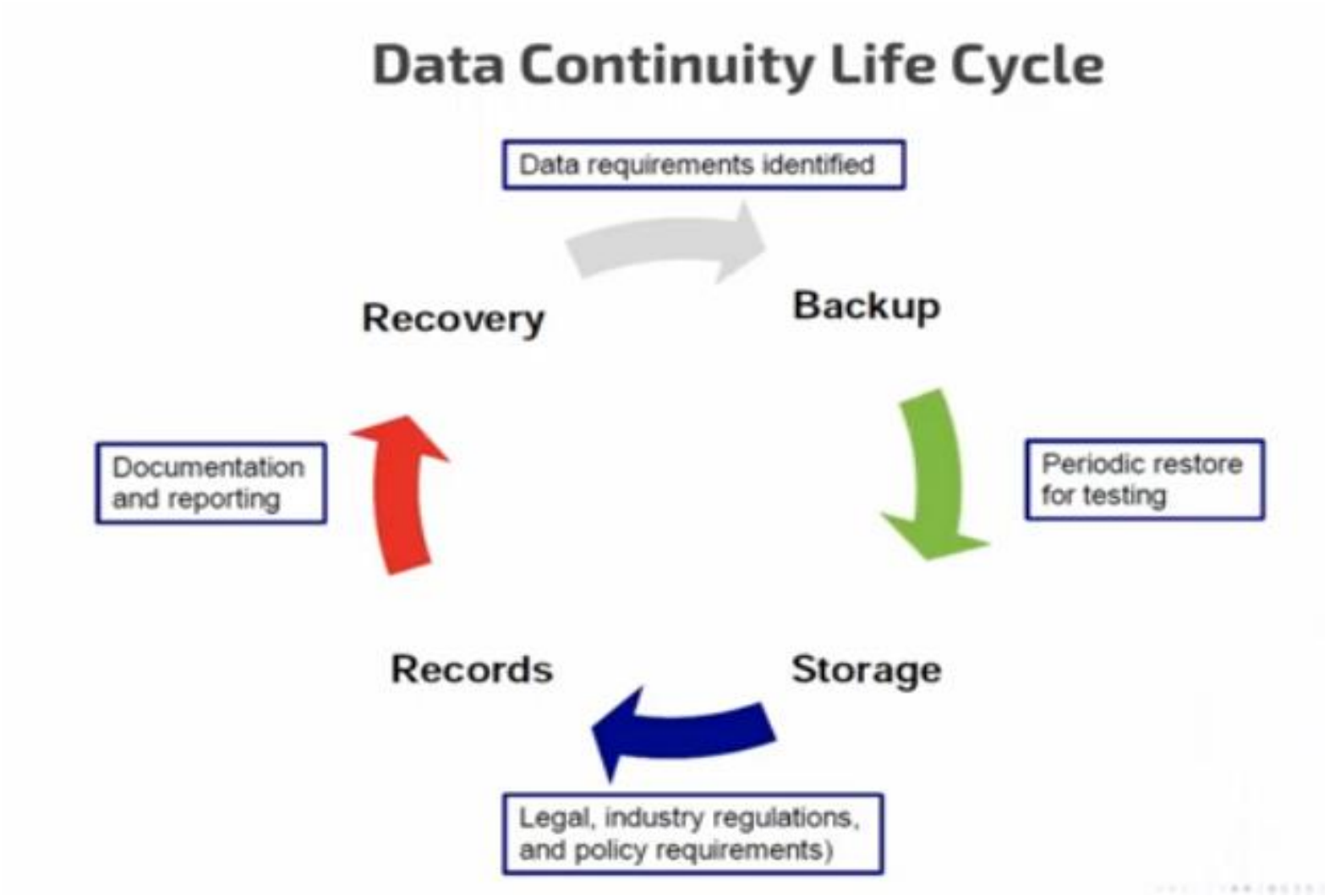
Organizations have an obligation to protect data that they collect and maintain. This is especially true for both PII and PHI data. Many laws and regulations mandate the protection of privacy data, and organizations have an obligation to learn which laws and regulations apply to them. Additionally, organizations need to ensure their practices comply with these laws and regulations.

Many laws require organizations to disclose what data they collect, why they collect it, and how they plan to use the information. Additionally, these laws prohibit organizations from using the information in ways that are outside the scope of what they intend to use it for. For example, if an organization states it is collecting email addresses to communicate with a customer about purchases, the organization should not sell the email addresses to third parties.

When **protecting privacy,** an organization will typically use several different security controls. Selecting the proper security controls can be a daunting task, especially for new organizations. However, using security baselines and identifying relevant standards makes the task a little easier.

Media Management

Media Management: Media management refers to the steps taken to protect media and data stored on media. In this context, media is anything that can hold data. It includes tapes, optical media such as CDs and DVDs, portable USB or FireWire drives, external SATA (eSATA) drives, internal hard drives, solid-state drives, and USB flash drives. Many portable devices, such as smartphones, include memory cards that can hold data so they fall into this category too. Media also includes any type of hard-copy data. Backups are often contained on tapes, so media management directly relates to tapes. However, media management extends beyond just backup tapes to any type of media that can hold data.


Data Continuity Life Cycle
Data requirements identified
Backup
Periodic restore for testing
Storage
Legal, industry regulations, and policy requirements)
Records
Documentation and reporting
Recovery

When media includes sensitive information, it should be stored in a secure location with strict access controls to prevent losses due to unauthorized access. Additionally, any location used to store media should have temperature and humidity controls to prevent losses due to corruption. Media management can also include technical controls to restrict device access from computer systems. For example, due to the risks USB drives represent, many organizations use technical controls to block their use and/or detect and record when users attempt to use them. In some situations, a written security policy prohibits the use of USB flash drives, and automated detection methods detect and report any violations.

Data Recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often the data are being salvaged from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

The most common "Data Recovery" scenario involves an operating system (OS) failure (typically on a single-disk, single-partition, single-OS system), in which case the goal is simply to copy all wanted files to another disk. This can be easily accomplished using a Live CD, many of which provide a means to mount the system drive and backup disks or removable media, and to move the files from the system disk to the backup media with a file manager or optical disc authoring software. Such cases can often be mitigated by disk partitioning and consistently storing valuable data files (or copies of them) on a different partition from the replaceable OS system files.

Retaining Assets

Retention requirements apply to data or records, media holding sensitive data, systems that process sensitive data, and personnel who have access to sensitive data. Record retention and media retention is the most important element of **asset retention**.

Record retention involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed. An organization's security policy or data policy typically identifies retention timeframes. Some laws and regulations dictate the length of time that an organization should retain data, such as three years, seven years, or even indefinitely. However, even in the absence of external requirements, an organization should still identify how long to retain data.

Most hardware is on a refresh cycle, where it is replaced every three to five years. Hardware retention primarily refers to retaining it until it has been properly sanitized. Personnel retention in this context refers to the knowledge that personnel gain while employed by an organization. It's common for organizations to include nondisclosure agreements (NDAs) when hiring new personnel. These NDAs prevent employees from leaving the job and sharing proprietary data with others.

Sanitization is a combination of processes that removes data from a system or from media. It ensures that data cannot be recovered by any means. When a computer is disposed of, sanitization includes ensuring that all nonvolatile memory has been removed or destroyed, the system doesn't have CD/DVDs in any drive, and internal drives (hard drives and SSDs) have been purged, removed, and/or destroyed. Sanitization can refer to the destruction of media or using a trusted method to purge classified data from the media without destroying it.

Data Security Controls

It's important to protect data while it is at rest, in motion, and in use. **Data at rest** is any data stored on media such as system hard drives, external USB drives, storage area networks (SANs), and backup tapes. **Data in transit** (sometimes called data in motion) is any data transmitted over a network. This includes data transmitted over an internal network using wired or wireless methods and data transmitted over public networks such as the Internet. Data in use refers to data in temporary storage buffers while an application is using it.

DATA AT REST

DATA IN TRANSIT

The best way to protect the confidentiality of data is to use strong encryption protocols. Additionally, strong authentication and authorization controls help prevent unauthorized access. As an example, consider a web application that retrieves credit card data for an ecommerce transaction. The credit card data is stored on a separate database server and is protected while at rest, while in motion, and while in use.

Database administrators take steps to encrypt sensitive data stored on the database server (data at rest). For example, they would encrypt columns holding sensitive data such as credit card data. Additionally, they would implement strong authentication and authorization controls to prevent unauthorized entities from accessing the database.

When the web application sends a request for data from the web server, the database server verifies the web application is authorized to retrieve the data and, if so, the database server sends it. However, this entails several steps. For example, the database management system first retrieves and decrypts the data and formats it in a way that the web application can read it. The database server then uses a transport encryption algorithm to encrypt the data before transmitting it. This ensures that the data in transit is secure.

The web application server receives the data in an encrypted format. It decrypts the data and sends it to the web application. The web application stores the data in temporary buffers while it uses it to authorize the transaction. When the web application no longer needs the data, it takes steps to purge memory buffers, ensuring all residual sensitive data is completely removed from memory.