Ch 04
PROTECTION OF INFORMATION ASSETS

Learning Objectives

- By the end of this chapter, students will be able to:
  - Explain what information assets are and why they are critical to organizations
  - Describe the role of security governance in protecting information assets
  - Classify information assets based on sensitivity, value, and impact
  - Identify ownership roles and responsibilities for information assets
  - Apply appropriate security controls across different data states
  - Understand data retention, sanitization, and disposal requirements
  - Explain how laws and regulations influence information asset protection

What Is an Information Asset?

An **information asset** is any information that has value to an organization, regardless of its form.

Examples:

- Student or customer records
- Financial data
- Intellectual property
- Research data

Information assets support organizational missions and decision-making.

Main Categories of Information Assets

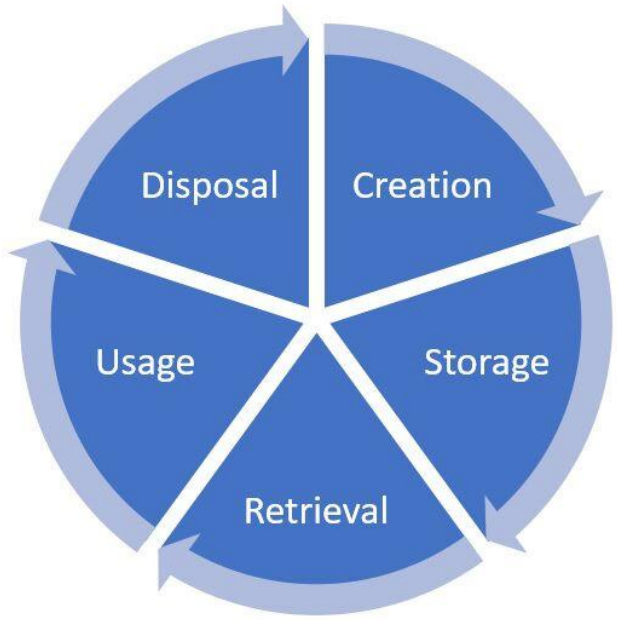
Primary Information Assets		Supporting Information Assets			
Information	Software	Hardware	Network	People	Physical
Customer personal data	Operating systems	Servers	Routers, switches	Employees	Data centers
Student records	Databases (Oracle, MySQL)	PCs and laptops	Internal networks	System administrators	Offices
Financial records	ERP systems	Mobile phones	Internet connections	Faculty members	File cabinets
Research data	Learning Management Systems (LMS)	Storage devices (USBs, NAS)	VPN infrastructure	Students	Power supply
Intellectual property	Mobile applications	Monitors and screens	Wireless access points	Third-party contractors	Cooling systems
Emails, reports, databases	Email systems		Firewalls		
Source code					

Why Protect Information Assets?

- Organizations must protect information assets because:
  - Information is a core business resource that enables operations and decision-making
  - Loss of confidentiality can lead to privacy violations and legal penalties
  - Loss of integrity can result in incorrect decisions and operational failures
  - Loss of availability can disrupt services and business continuity
  - Data breaches damage organizational reputation and stakeholder trust
- Protecting information assets is therefore a **strategic, legal, and governance requirement**, not only a technical concern.

INFORMATION ASSET SECURITY

- **Information Asset Security domain**
  - focuses on collecting, handling and protecting information throughout its lifecycle.
  - A primary step in this domain is classifying information base its value to the organization.



So, what we need to do:
- Collecting information securely
- Processing information safely
- Storing information securely
- Protecting information throughout its lifecycle

How we can do Info. Asset security:
- Secure systems and environments
- Hardware and software controls
- Encryption and access control
- Monitoring and auditing

Security Governance and Information Assets

- **Security governance** defines how information assets are protected and controlled.
- It ensures:
  - Clear accountability
  - Consistent security practices
  - Compliance with laws and standards
  - Oversight and continuous improvement
- Asset protection is enforced through policies, standards, procedures, and audits.

SECURITY GOVERNANCE PRINCIPLES

Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.

Security governance principles are often closely related to and often twisted with corporate and IT governance.

Corporate governance is "**Doing the right things for the organization and doing things the right way independent of personal interests.**"

Cybersecurity Management vs Cybersecurity Governance

Management:

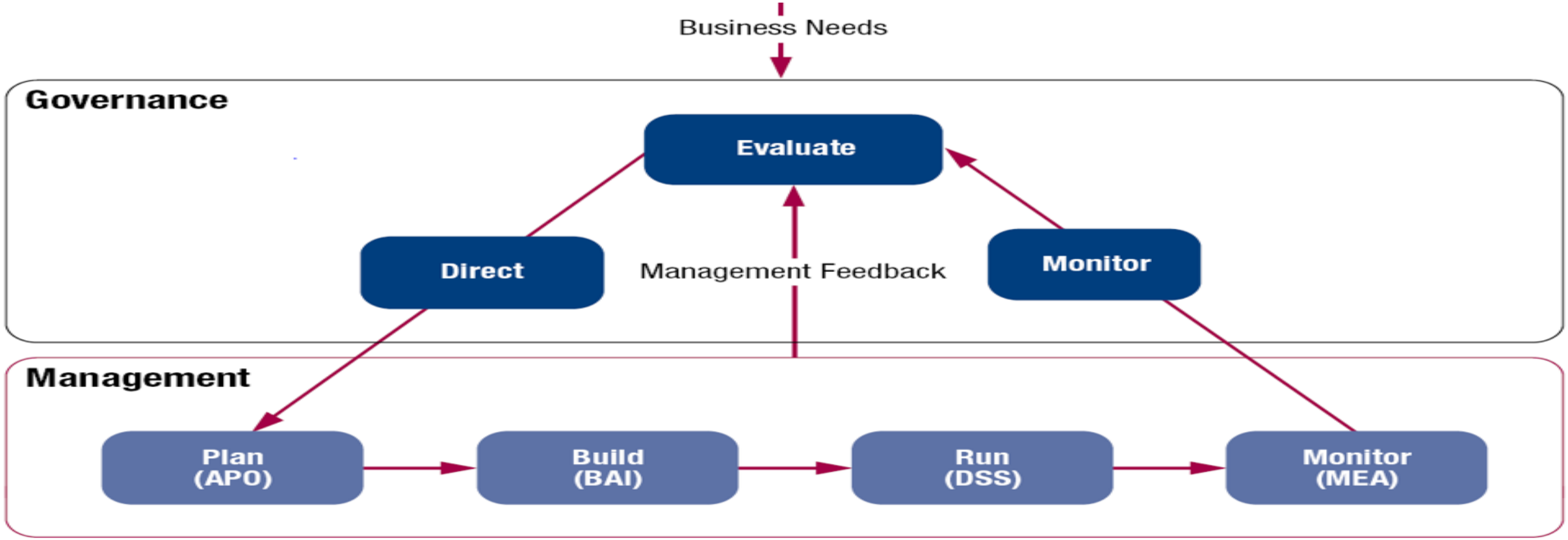
Tactical, operational execution

Governance:

Strategic, oversight, accountability

Cybersecurity Governance

- Cybersecurity Governance is an integral Part of Overall Corporate Governance
- Governance vs. management

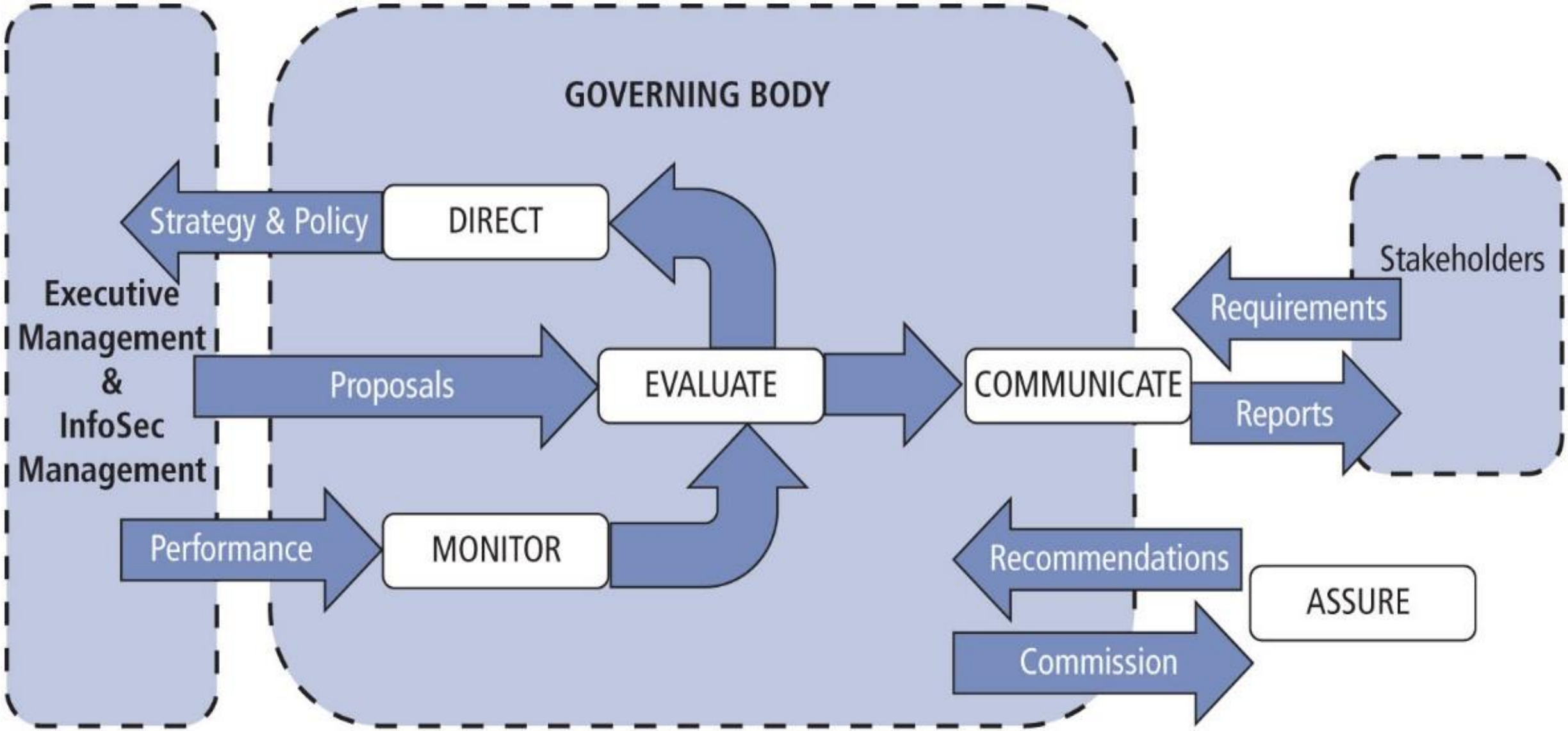


Cybersecurity Governance

- The *strategic* oversight function that ensures the cybersecurity program aligns with business goals and complies with laws, regulations, and policies.
- **Focus**: Direction, accountability, oversight, and control.
- **Who's Involved**: Senior leadership, board of directors, governance committees.
- **Key Questions Addressed**:
  - Are we doing the *right things*?
  - Are our cybersecurity investments aligned with business risk and value?
  - Are roles, responsibilities, and reporting structures clearly defined?
- **Examples**:
  - Approving enterprise security policies.
  - Defining acceptable risk levels.

Cybersecurity Management

- The *operational and tactical* activities performed to implement and maintain cybersecurity controls.
- **Focus**: Execution, operations, monitoring, and incident response.
- **Who's Involved**: CISOs, security managers, security analysts, technical staff.
- **Key Questions Addressed**:
  - Are we doing the *things right*?
  - Are controls properly implemented and maintained?
  - Are we responding effectively to threats and vulnerabilities?
- **Examples**:
  - Deploying firewalls and endpoint protection.
  - Monitoring for cyber incidents.
  - Conducting vulnerability scans and risk assessments.



ISO/IEC 27014:2013 governance processes[19]

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

EVALUATE AND APPLY SECURITY GOVERNANCE PRINCIPLES

- Many organizations expand and adapt to deal with a global market,
- So, governance issues become more complex. This is especially **problematic when laws in different countries differ or conflict**.
- The organization needs a direction, guidance, and tools to provide sufficient oversight and management to address threats and risks with a focus on eliminating downtime and keeping potential loss or damage to a minimum.



EVALUATE AND APPLY SECURITY GOVERNANCE PRINCIPLES

Security is not and should not be treated as an IT issue only.

It is no longer just something the IT staff can handle on their own.

Security is a business operations issue.

Security is an organizational process

Security governance is commonly managed by a governance committee or at least a board of directors whose primary task is to oversee and guide the actions of security and operations for an organization.

Security frameworks and governance guidelines include NIST 800-53 or 800-100.

NIST guidance is focused on government and military use. It can be used by other types of organization as well.

Third-Party and Cloud Governance

ASP: An Application Service Provider (ASP) is a company that delivers software applications over the internet. Instead of hosting the software on your own servers, the ASP hosts and maintains it on their servers.

When using ASPs or cloud providers:

- Organizations remain accountable for data protection
- Due diligence must be performed before engagement
- Contracts and SLAs must define security responsibilities

Governance ensures third-party risks are managed effectively.

Due Care vs. Due Diligence

Due Care refers to the reasonable steps an organization takes to protect its information assets by following accepted security practices. Examples include:		
Enforcing strong password policies	Applying security patches	Using antivirus and firewalls



Due Diligence goes further and involves actively identifying and analyzing risks. Examples include:		
Conducting risk assessments	Auditing third-party providers	Reviewing incident history and vulnerabilities

Due Care vs. Due Diligence

- From a governance perspective:
  - Due care demonstrates responsible operation
  - Due diligence demonstrates proactive risk management
- Both are essential to avoid negligence and legal liability.

Information Classification

- **Information classification** organizes information assets based on sensitivity and impact.
- Classification helps:
  - Apply appropriate security controls
  - Control access and handling
  - Reduce risk of data exposure

Classification Systems

- Two common approaches:
  - Government and military systems

Top Secret	Secret	Confidential	Unclassified

  - Commercial (organizational) systems

Restricted	Confidential	Internal	Public

- Higher classification requires stronger security controls.
- More regulated organizations tend to adopt more detailed classification schemes.

Government and military systems

Top Secret

- applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause an **exceptionally grave damage** to the national security”

Secret

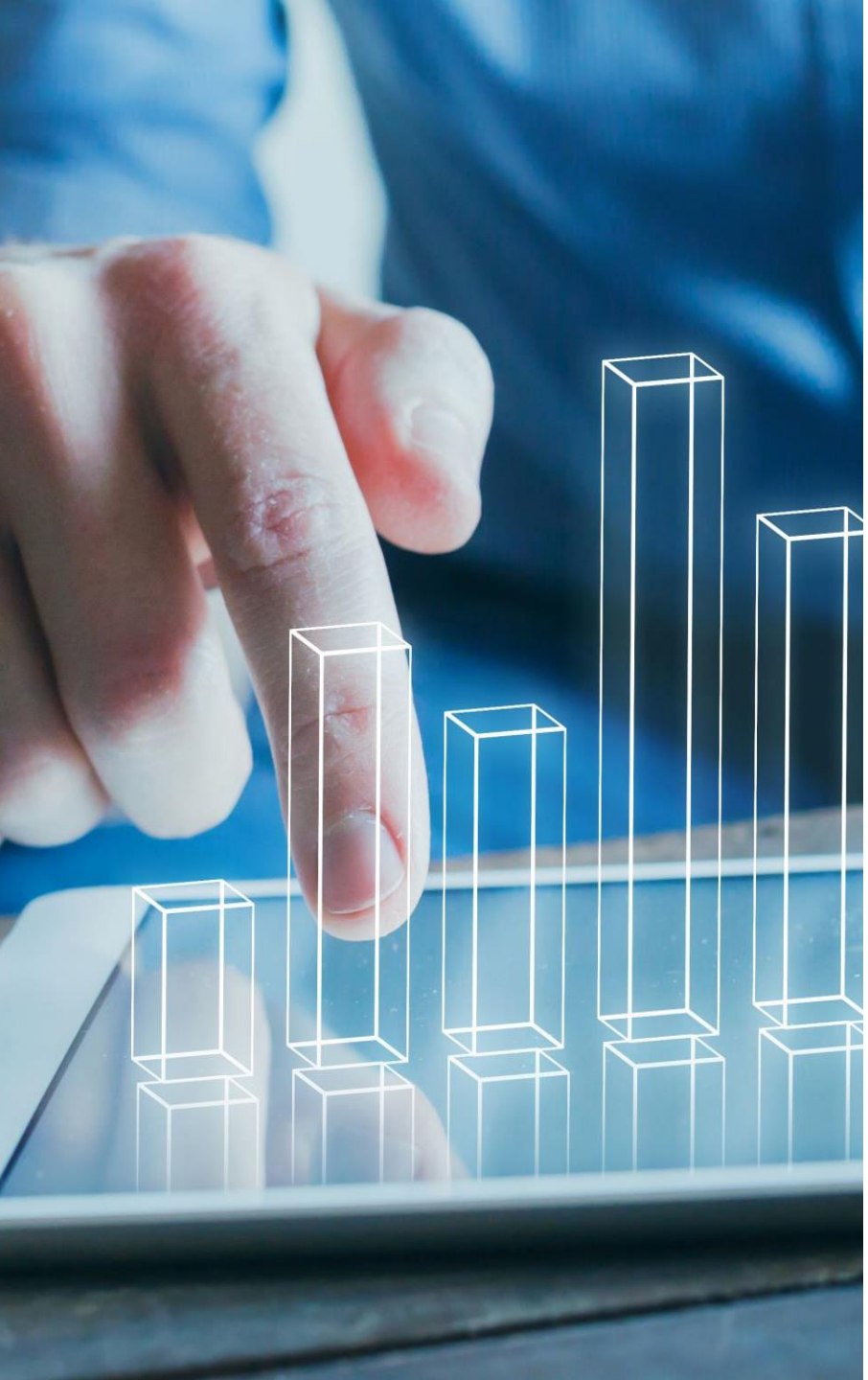
- applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security”

Confidential

- applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security”

Unclassified

- applied to “any information that can generally be distributed to the public without any threat to national interest”



Commercial classification systems

- No standard: each company can choose its own system that matches its culture and needs
- Usually less complex than the government system
- The more regulated a company, the more complex the classification system they adopt

Classification Criteria

- Information classification is based on evaluating multiple factors, including:
  - **Business Value**: How critical the information is to operations or competitiveness
  - **Legal and Regulatory Impact**: Laws requiring protection (e.g., PDPL, GDPR)
  - **Reputational Damage**: Loss of customer or public trust if disclosed
  - **Operational Impact**: Disruption caused by unauthorized modification or loss
- A common guiding question is: *What is the worst possible impact if this information is disclosed, altered, or destroyed?*
- The higher the impact, the higher the classification level and required controls.

Commercial classification systems

- Most systems revolve around these four classification levels:

Public	Internal Only	Confidential	Restricted
Data that may be freely disclosed to the public For example: marketing materials, contact information, price lists, etc.	**Internal data not meant for public disclosure** For example: battlecards, sales playbooks, organizational charts, etc.	**Sensitive data that if compromised could negatively affect operations** For example: contracts with vendors, employee reviews, etc.	**Highly sensitive corporate and customer data that if compromised could put the organization at financial or legal risk** For example: IP, credit card information, social security numbers, PHI)

EXAMPES OF RESTRICTED DATA

PERSONALLY IDENTIFIABLE INFORMATION *(PII)* is any information that can identify an individual.

- 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;

PROTECTED HEALTH INFORMATION *(PHI)* is any health-related information that can be related to a specific person.

- received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;

PROPRIETARY DATA refers to any data that helps an organization maintain a competitive edge.

- software code, technical plans for products, internal processes, Copyrights, patents, and trade secret laws provide a level of protection for proprietary data etc.

Class Exercise

Credit card numbers (PCI)	Supplier contracts	Content of public websites	marketing materials	student education records
Patient Health Information	PSU Newsletters	customer personal data	Social Security numbers	intellectual property
press releases	IT service management information	financial account numbers	Internal emails carrying Announcements	employee directory
Social media feeds	Third- Party vendor Contracts	Employee pay cheques	employee records	Trade secrets

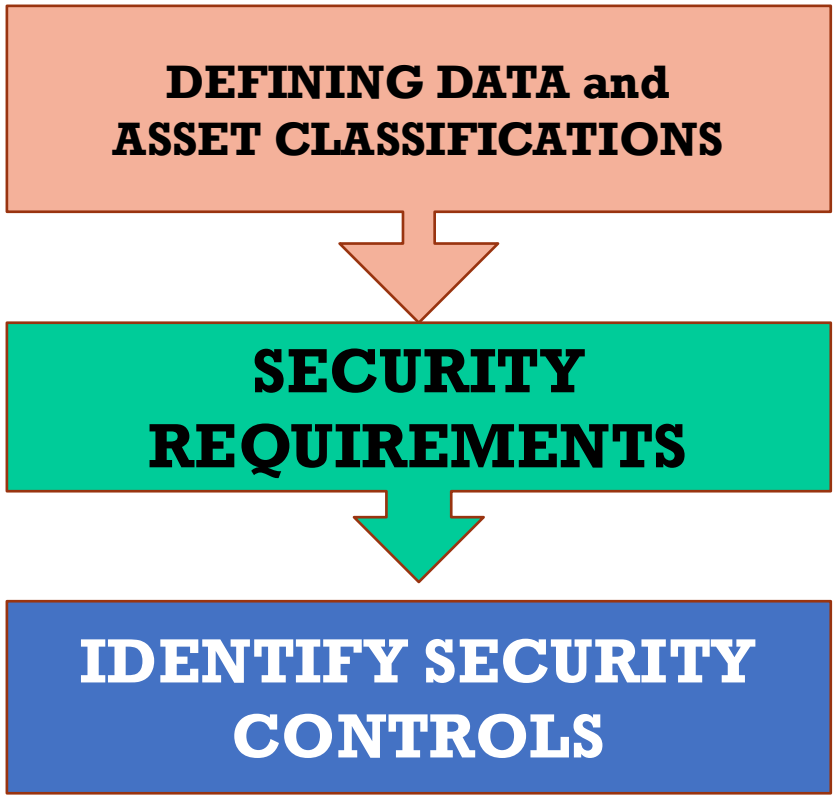
Review the list of the above information assets and decide the appropriate sensitivity leve:

Category 4: **Highly sensitive data**	
Category 3: **Sensitive internal data**	
Category 2: **Internal data that is not meant for public disclosure**	
Category 1: **Data that may be freely disclosed with the public**	

DEFINING ASSET CLASSIFICATIONS

Asset classifications should match the data classifications.

DETERMINING DATA SECURITY CONTROLS



SECURITY REQUIREMENTS FOR DIFFERENT DATA CLASSES

Data Classification	Data Example	Security controls for Storing Accessing and Transferring
Sensitive/ Critical	• Biometric data • Personal Medical Data	• Stored in encrypted format in agreed storage location e.g. SharePoint • Backed up weekly to secure local drive held in locked fireproof safe • Transferred in encrypted format • Not to be transferred by email • Accessed by Username and Password by authorised researchers only
Confidential	• Names, addresses, dates of birth of Living individuals (Subject to GDPR)	• Stored in encrypted format in agreed storage location e.g. SharePoint • Backed up weekly to secure local drive held in locked fireproof safe • Transferred in encrypted format • Not to be transferred by email unless encrypted • Accessed by Username and Password by authorised researchers only
Private/ Internal	• Research project Communications	• Stored in in agreed storage location e.g. Email, OneDrive etc • Accessed by Username and Password • Can be transferred by email to authorised staff
Public/ unclassified	• Staff names, job titles and work contact details • Project Public website	• Authorised for public use on Research Project website etc • Encryption not necessary • Backed up weekly

Marking Sensitive Data and Assets

MARKING (often called labeling) sensitive information ensures that users can easily identify the classification level of any data.

Marking includes both physical and electronic marking and labels.

PHYSICAL LABELS indicate the security classification for the data stored on assets such as media or processed on a system.

ELECTRONIC LABELS - as a **header and/or footer in a document, or embed it as a watermark**.

- A benefit of these methods is that they also appear on printouts.



CONFIDENTIAL RECOMMENDATION FORM
Executive MBA Program
College of Business Administration
San Diego State University

PLICANT:

ly the information requested below. You may solicit more than the two required evaluations, if, in your opinion, the information th
ly affect the consideration of your application.

إخلاء مسؤولية: هذه الرسالة خاصة وسرية بالأشخاص المرسلة لهم وقد تحتوي على معلومات سرية، اذا تلقيت هذه الرسالة بالخطأ او لم تكن الشخص المقصود يرجى عدم نشرها او نسخها جزئيا او كليا وإخطارنا عن طريق العنوان البريدي المذكور أعلاه

* يرجى مراعاة المحافظة على البيئة قبل طباعة هذا البريد

Disclaimor: This message is intended only for the individual or entity in which it is addressed to and may contain information that is confidential. If you are not the intended recipient or have received this email in error. Please be advised that you may not disclose, disseminate, distribute, or copy this communication in full or in part. You are also requested to notify melus.

Please consider the environment before printing this email.

HANDLING INFORMATION AND ASSETS

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

- A **DATA BREACH** is **any event** in which an **unauthorized entity can view or access classified data**.

Protecting Data at Rest

Data at rest includes information stored on:

- Hard drives and databases
- Backup tapes and storage systems
- USB drives and removable media

Key protection controls include:

- Encryption (e.g., AES-256)
- Strong access controls and authentication
- Secure storage facilities and physical protection
- Environmental controls (HVAC, fire suppression)
  - HVAC: Heating, Ventilation, and Air Conditioning

These controls reduce the risk of unauthorized access, theft, or loss.



Protecting Data in Transit

- Encrypted communication channels
- Secure network protocols
- Network monitoring

Protecting Data in Use



Access control



Endpoint security



Memory protection

Record and Asset Retention

- Record and asset retention refers to keeping information for as long as it is needed for:
  - Business operations
  - Legal and regulatory compliance
  - Audit and accountability purposes
- Retention periods may be defined by:
  - Organizational policies
  - Industry standards
  - Laws and regulations (e.g., 3 years, 7 years, or indefinitely)
- Once the retention period expires, information must be securely destroyed to reduce risk.

Secure Data Destruction

- Deleting files is not sufficient.
- Secure destruction prevents:
  - Data recovery
    - A process of **retrieving lost, deleted, corrupted, or inaccessible data** from storage devices when normal access is no longer possible.
  - Data remanence
    - The data that remains on media after the data was supposedly erased.

Destroying Sensitive Data

- When we no longer need a certain media, we must dispose of it in a manner that ensures that data can't be retrieved. This pertains to both electronic media and paper copies of data.
- **Paper Disposal:** It is highly encouraged to dispose of any paper with any sensitive data on it in a secure manner. This also has a standard and cross shredding is recommended.
- **Digital disposal:** The digital disposal procedures are determined by the type of media containing data.

Common terms associated with Digital Data Disposal:



Erasing media is simply **performing a delete operation** against a file, a selection of files, or the entire media. Everything is still recoverable.



Formatting it does the same, but it also puts a new file structure over the old one full stop still recoverable in most cases.



Clearing - or **overwriting**, is a process of preparing media for reuse and ensuring that the cleared data cannot be recovered using traditional recovery tools.



Purging (multiple overwrite/degaussing) - is a more intense form of clearing that prepares media for reuse in less secure environments.



Destruction - is the final stage in the lifecycle of media and is the most secure method of sanitizing media.



Declassification involves any process that purges media or a system in preparation for reuse in an unclassified environment.

DEGAUSSER MACHINES

A degausser generates a heavy magnetic field, which realigns the magnetic fields in magnetic media such as traditional hard drives, magnetic tape, and floppy disk drives. Degaussers using power will reliably rewrite these magnetic fields and remove data remanence.

Degaussing SSDs won't remove data.







DESTROYING DATA MACHINES





https://www.youtube.com/watch?v=gSFFwgtygjU



Data Protection Laws

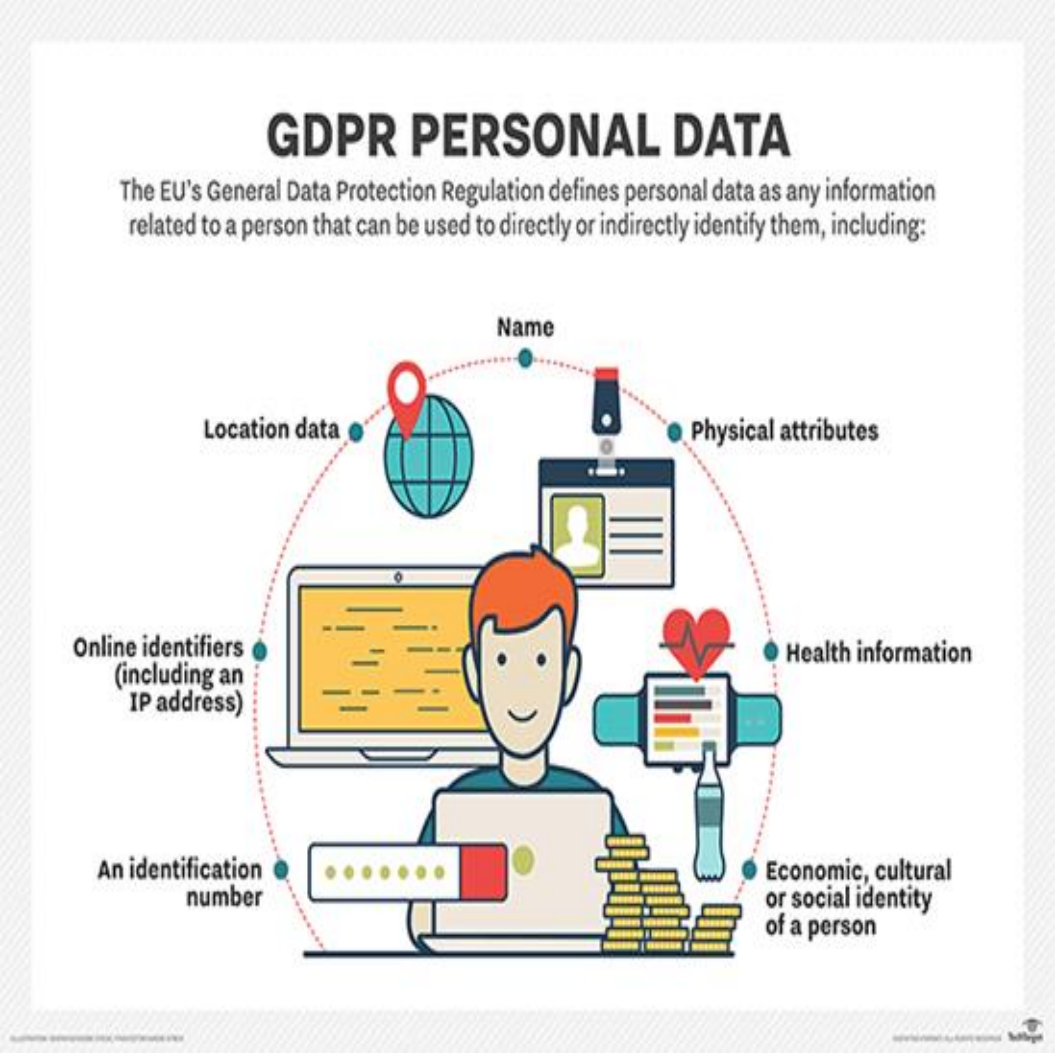


Legal Compliance as a Governance Driver

- Laws and regulations require organizations to:
  - Protect personal and sensitive data
  - Implement security controls
  - Report breaches
- Non-compliance leads to penalties and loss of trust.

European Union – General Data Protection Regulation (GDPR)

- Is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).
- Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.
- Heavy fines for non-compliance



United States – Sectoral & State-Based

- No single federal data protection law
- Key Laws:
  - **CCPA (**California Consumer Privacy Act) **/ CPRA** (California Privacy Rights Act) - gives consumers more control over the personal information that businesses collect about them
  - **HIPAA** (Health Insurance Portability and Accountability Act) establishing national standards to protect sensitive patient health information (PHI) from unauthorized disclosure.
  - **GLBA** (Gramm-Leach-Bliley Act) - requires financial institutions, companies that offer consumers financial products or services like loans, financial, investment advice, insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
  - Generally, more business-friendly than GDPR

Saudi Arabia - Personal Data Protection Law (PDPL)

- The PDPL is Saudi Arabia's comprehensive data protection legislation, issued by Royal Decree and **in force since 14 September 2023**. It modernizes data privacy protections and aligns many principles with global standards like the EU GDPR.
- Applies to **all personal data processing** of individuals in Saudi Arabia — whether done by organizations inside the country or by foreign entities processing data of Saudi residents
- Covers both electronic and non-electronic data
- **Cross-border Transfers:** Specific rules apply to transferring personal data outside Saudi Arabia
- **Enforcement & Penalties:**
  - **Regulator:** The Saudi Data & AI Authority (SDAIA) oversees enforcement and issues guidance.
  - **Fines & Sanctions:** Administrative fines up to **SAR 5 million** for PDPL violations (can be doubled for repeat offenses).
  - **Criminal penalties** — e.g., up to 2 years' imprisonment and/or fines for unlawful disclosure of sensitive data with intent to harm

PDPL establishes robust protections for personal data - advancing the Kingdom's data privacy framework toward international norms.

ASSET OWNERSHIP

- **Information ownership** means **assigning clear responsibility and authority for a specific information asset** to a person or role in the organization.

- The **information owner** is accountable for how the information is:
  - Classified
  - Protected
  - Used
  - Shared
  - Retained and disposed of
- Example: Student Records at a University:
  - **Information asset:** Student education records
  - **Information owner:** Registrar's Office (or Registrar role)

ASSET OWNERSHIP

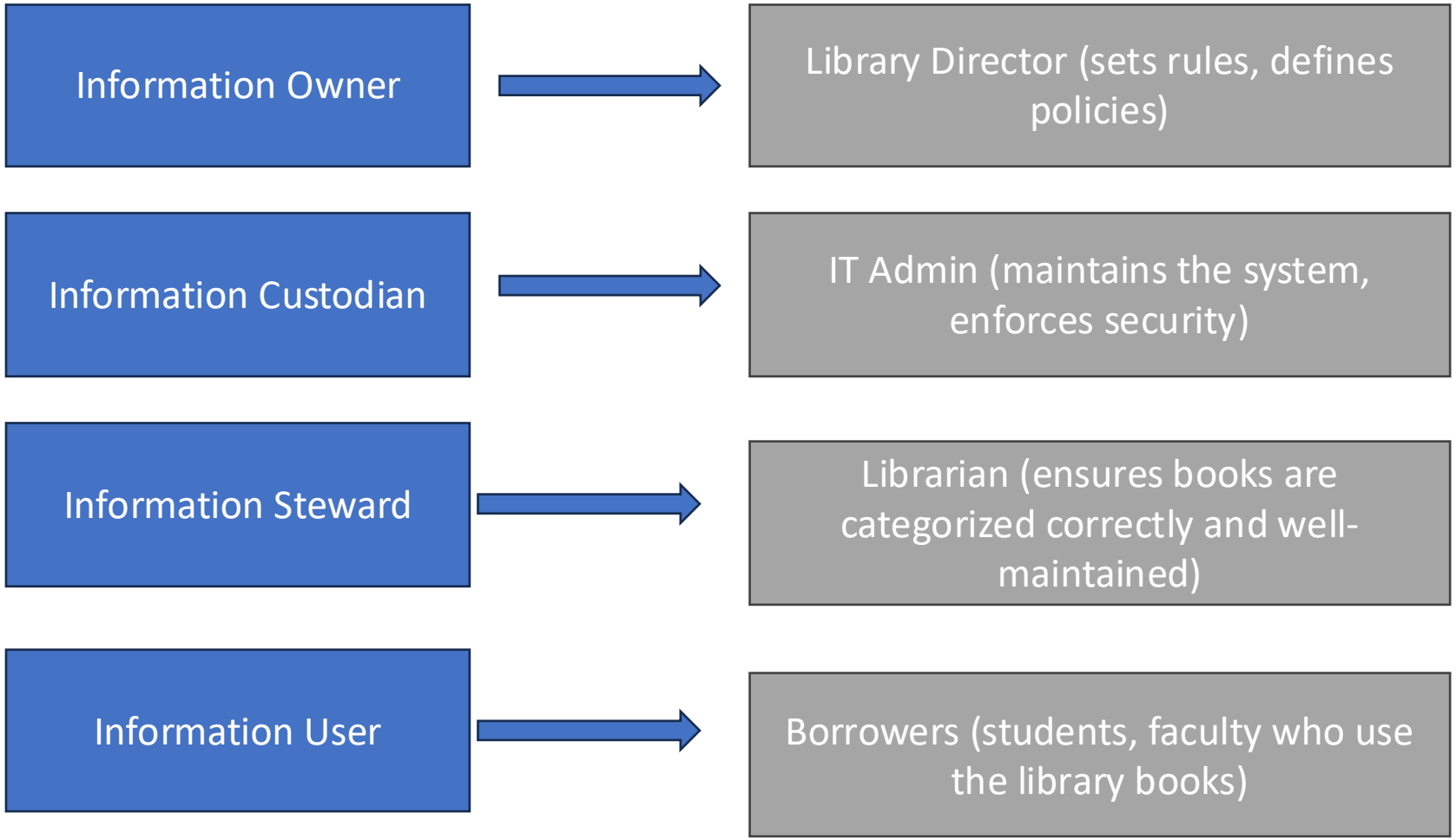
- Why Ownership Matters:
  - Effective protection requires:
    - Clear accountability
    - Defined decision-making authority
  - Without ownership, security controls cannot be enforced properly.

ASSET OWNERSHIP

- Information Ownership (who is the owner)
  - CISO is accountable for the protection of the organizational data.
    - Information owner: Typically a business or department head
      - Determines data classification
      - Approves access rights
      - Ensures appropriate protection
    - Information steward: owns the technical accountability for how information supports business process (Data analytics). Ensures data quality and business usage
    - Information custodian Handles the technical environment and implements measures to protect data. Ensure data is accessible to users as per the guidelines set by the data owner and steward. Implements technical controls
    - Information user is responsible for using the information in accordance with its classification level

Example:

- **Student Records at a University:**
  - **Information asset:** Student education records
  - **Information owner:** Registrar's Office (or Registrar role)
  - **System custodian:** IT Department
  - **Users:** Faculty members and academic advisors
- **What the owner decides:**
  - Who is allowed to access student records
  - Whether the data is confidential or highly sensitive
  - How long records must be kept
  - When data can be shared (e.g., with accreditation bodies)
- **What IT does (not the owner):**
  - Manages servers and databases
  - Applies access controls
  - Performs backups and security updates


Information Owner
Library Director (sets rules, defines policies)
Information Custodian
IT Admin (maintains the system, enforces security)
Information Steward
Librarian (ensures books are categorized correctly and well-maintained)
Information User
Borrowers (students, faculty who use the library books)

DETERMINING OWNERSHIP

- Many people within an organization manage, handle, and use data, and they have different requirements based on their roles.
- One of the most important concepts here is ensuring that personnel know who owns information and assets.
- The owners have a primary responsibility of protecting the data and assets.

DATA OWNER RESPONSABILITIES

According to NIST SP 800-18 – **the responsibilities for the information owner**:

- ✓Establishes the rules for appropriate use and protection of the subject data/information
- ✓Provides input to **information system owners** regarding the security requirements and security controls for the information system(s)
- ✓Decides who has access to the information system and with what types of privileges or access rights
- ✓Assists in the identification and assessment of the common security controls where the information resides.



ASSET OWNERS

- The asset owner (or system owner) is the person who owns the asset or system that processes sensitive data.

NIST SP 800-18 - **responsibilities for the system owner**:

✓Develops a system security plan in coordination with information owners, the system administrator, and functional end users

✓Maintains the system security plan and ensures that the system is deployed and operated according to the security requirements

✓Ensures that system users and support personnel receive appropriate security training

✓Updates the system security plan whenever there is a significant change

✓Assists in the identification, implementation, and assessment of the common security controls

Best Practices for Information Asset Protection

- Identify and classify data & assets correctly
- Apply Principle of least privilege
- Strong Authentication and Identity Security
- Encrypt sensitive data
- Monitor & log access
- Data Loss Prevention (DLP)
- Regular audits and user awareness training

ALIGNMENT OF SECURITY FUNCTION TO BUSINESS STRATEGY, GOALS, MISSION, AND OBJECTIVES

BUSINESS/MISSION OWNERS

- The business/mission owner role is viewed differently in different organizations.
- NIST SP 800-18 refers to the business/mission owner as a program manager or an information system owner.
- The responsibilities of the business/mission owner can overlap with the responsibilities of the system owner or be the same role.
- In businesses, business owners are responsible for ensuring that systems provide value to the organization.

ALIGNMENT OF SECURITY FUNCTION

- Security management planning ensures the **proper creation, implementation, and enforcement of security policies** within an organization.
- The main objective of security management planning is to **align security functions with the organization's strategy, goals, mission, and objectives**.
- Effective security **does not operate in isolation**; it supports business priorities and enables safe operations.
- One of the most effective approaches to security management planning is the **Top-Down Approach**.

Top-Down Approach

- Senior (upper) management is responsible for:
  - Initiating security policies
  - Approving security objectives
  - Defining acceptable risk
- Security policies provide **direction and authority** for all levels of the organization.
- Top-down support is essential for policy enforcement and accountability.

THE INFORMATION SECURITY (INFOSEC) TEAM

- The team or department responsible for security within an organization should be autonomous.
- Chief information security officer (CISO) – the leader of Cybersecurity team, must report directly to senior management.

The security management plan include

- defining **security roles**;
- prescribing how security will be managed,
- who will be responsible for security.
- how security will be tested for effectiveness;
- developing security policies;
- performing risk analysis; and
- requiring security education for employees.

- These efforts are guided through the development of management plans.

DEVELOPING AND IMPLEMENTING A SECURITY POLICY

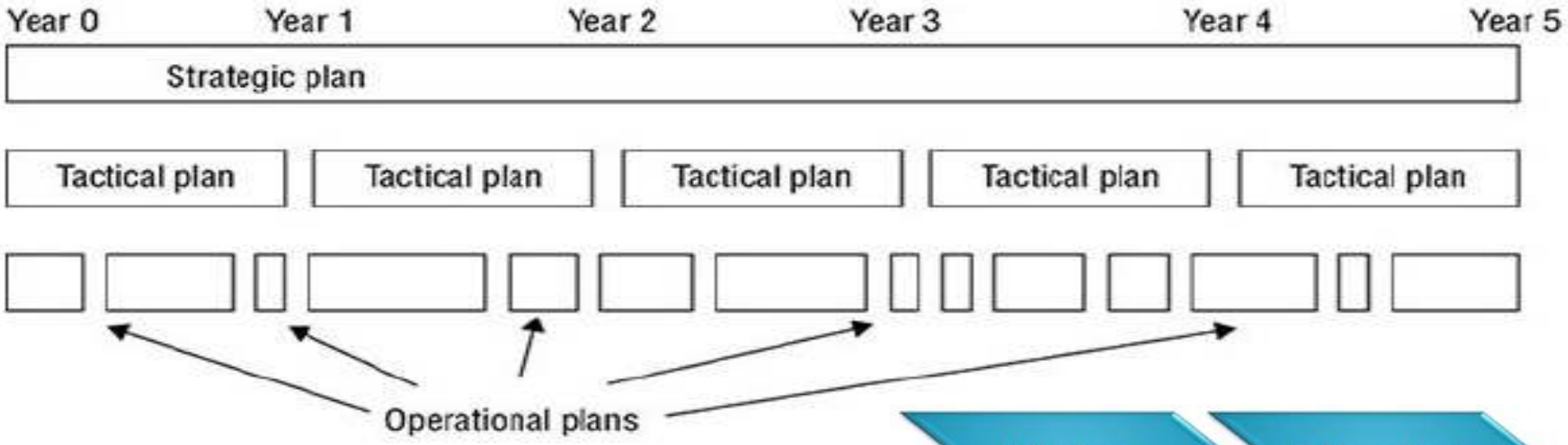
- A security management planning team should develop three types of plans



Figure-1: Planning three levels.

DEVELOPING AND IMPLEMENTING A SECURITY POLICY

- A security management planning team should develop three types of plans





STRATEGIC SECURITY PLAN

- A **long-term, high-level plan** that defines the organization's overall security direction.
- Aligns the security function with:
  - Business mission
  - Organizational goals
  - Strategic objectives
- Typically valid for **3–5 years**, with **annual reviews and updates**.
- Serves as the **planning horizon** for all other security activities.

- Key Characteristics:
  - Includes a **risk assessment**
  - Defines security priorities and principles
  - Establishes governance structure
  - Security documentation must be:
    - Clear
    - Concrete
    - Well-defined

Strategic plans answer the question: *"Why are we securing our information assets?"*

TACTICAL SECURITY PLAN

- A **mid-term plan** that translates strategic objectives into actionable initiatives.
- Provides details on **how to achieve strategic security goals**.
- Usually valid for **about one year**.
- Can also be developed **ad hoc** in response to unexpected events (e.g., incidents, new regulations).

- Examples of Tactical Plans:
  - Project plans
  - Acquisition plans
  - Hiring plans
  - Budget plans
  - Maintenance and support plans
  - System development plans

Tactical plans define **which protection controls** will be implemented for information assets.

OPERATIONAL SECURITY PLAN

- A **short-term, highly detailed plan** focused on daily security operations.
- Derived from both strategic and tactical plans.
- Must be updated frequently (monthly or quarterly) to remain effective and compliant.

- Operational Plans Describe:
  - Step-by-step implementation procedures
  - Resource allocation
  - Budget usage
  - Staffing and scheduling
  - How controls comply with security policies

Operational plans explain *how protection is actually applied to information assets*.

Planning Levels vs Asset Protection

Planning Level	Focus	Relation to Assets
Strategic	Direction & purpose	Defines which assets are critical
Tactical	Control selection	Chooses protection methods
Operational	Execution	Applies controls daily

Example

- Online Banking System (Financial Institution)
- A bank provides **online and mobile banking services** to customers. Its **critical information assets** include:
  - Customer personal data (PII)
  - Account balances and transaction records
  - Online banking platform
  - Authentication credentials

Ex. Strategic Security Plan (Long-Term – “WHY”)

- Business Strategy:
  - Expand digital banking services while maintaining customer trust and regulatory compliance.
- Strategic Security Objective
  - Protect customer data and ensure continuous availability of online banking services.
- Strategic Security Decisions:
  - Security is treated as a **business risk management function**
  - Adoption of **ISO/IEC 27001** as the security governance framework
  - Commitment to comply with: Banking regulations and Data protection laws
- Strategic Outcomes:
  - Information assets are classified (e.g., *Highly Confidential*)
  - A formal **security governance structure** is approved
  - A **CISO role** is established reporting to senior management
- Strategic plans explain *why security exists* and *what must be protected*.

Ex. Tactical Security Plan (Mid-Term – “WHAT”)

- Translating Strategy into Actions:
  - To support the strategic goal, the bank develops **tactical security plans** for the coming year.
- Tactical Security Decisions:
  - Implement **multi-factor authentication (MFA)** for online banking
  - Deploy **encryption** for customer data at rest and in transit
  - Introduce **Security Information and Event Management (SIEM)**
  - Develop an **incident response plan**
  - Allocate budget for:
    - Security tools**,** Staff training**, and** Penetration testing
- Example Tactical Plans:
  - Project plan for MFA deployment
  - Hiring plan for SOC analysts
  - Training plan for employees on phishing awareness
- Tactical plans define *which controls* will be used to protect information assets.

Operational Security Plan (Short-Term – “HOW”)

- Daily Security Operations:
  - Operational plans describe **how security is executed daily**.
- Operational Security Activities
  - SOC analysts monitor logs **24/7**
  - Incident response procedures are followed step-by-step
  - Weekly vulnerability scans are performed
  - Monthly access reviews for critical systems
  - Daily backup verification and recovery testing

- Example Operational Procedures
  - Step-by-step procedure to respond to a suspected data breach
  - Checklist for approving user access
  - Backup restoration testing schedule

Operational plans show *how controls are applied in practice*.

How the Plans Work Together (Big Picture)

Level	Question Answered	Example
Strategic	Why protect?	Protect customer trust & comply with law
Tactical	What to implement?	MFA, encryption, SIEM
Operational	How to operate?	Log monitoring, access reviews

Thank you