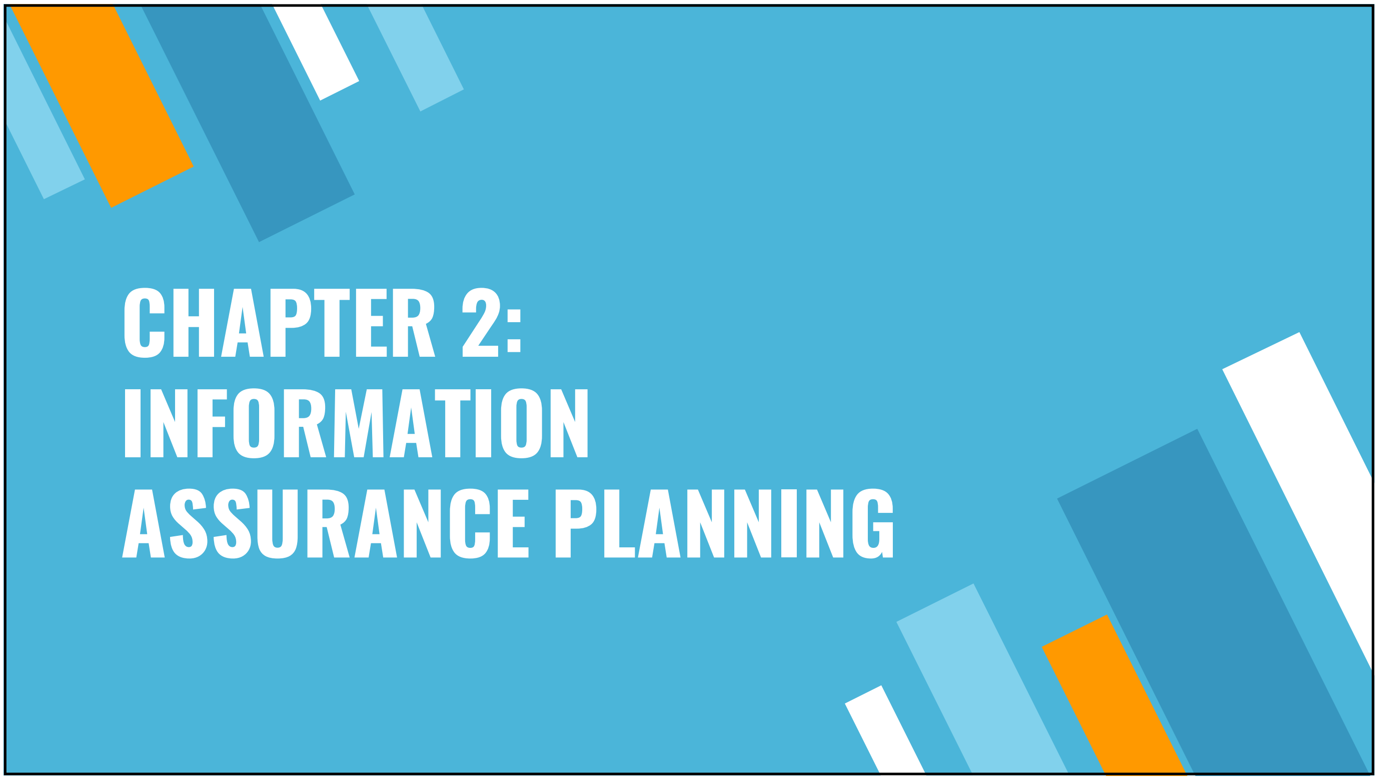
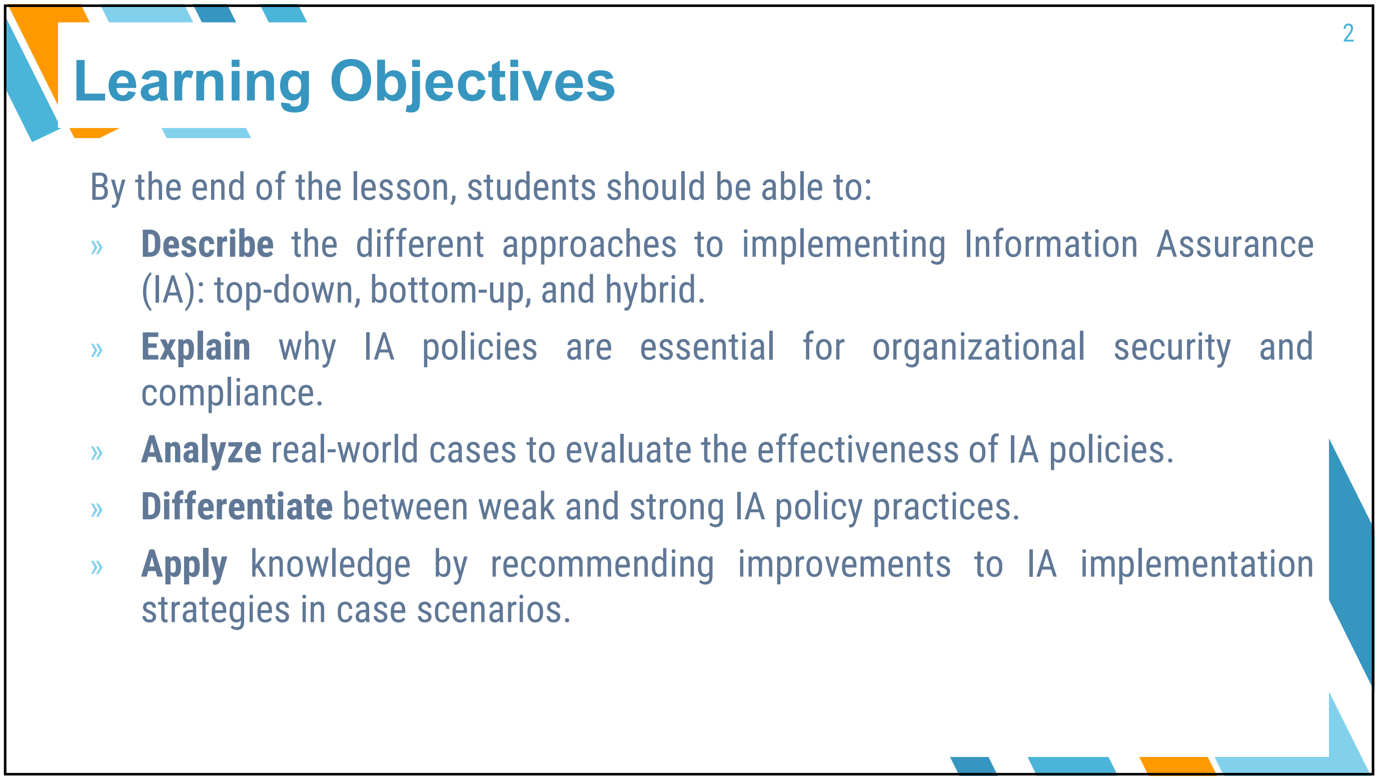


CHAPTER 2: INFORMATION ASSURANCE PLANNING

1

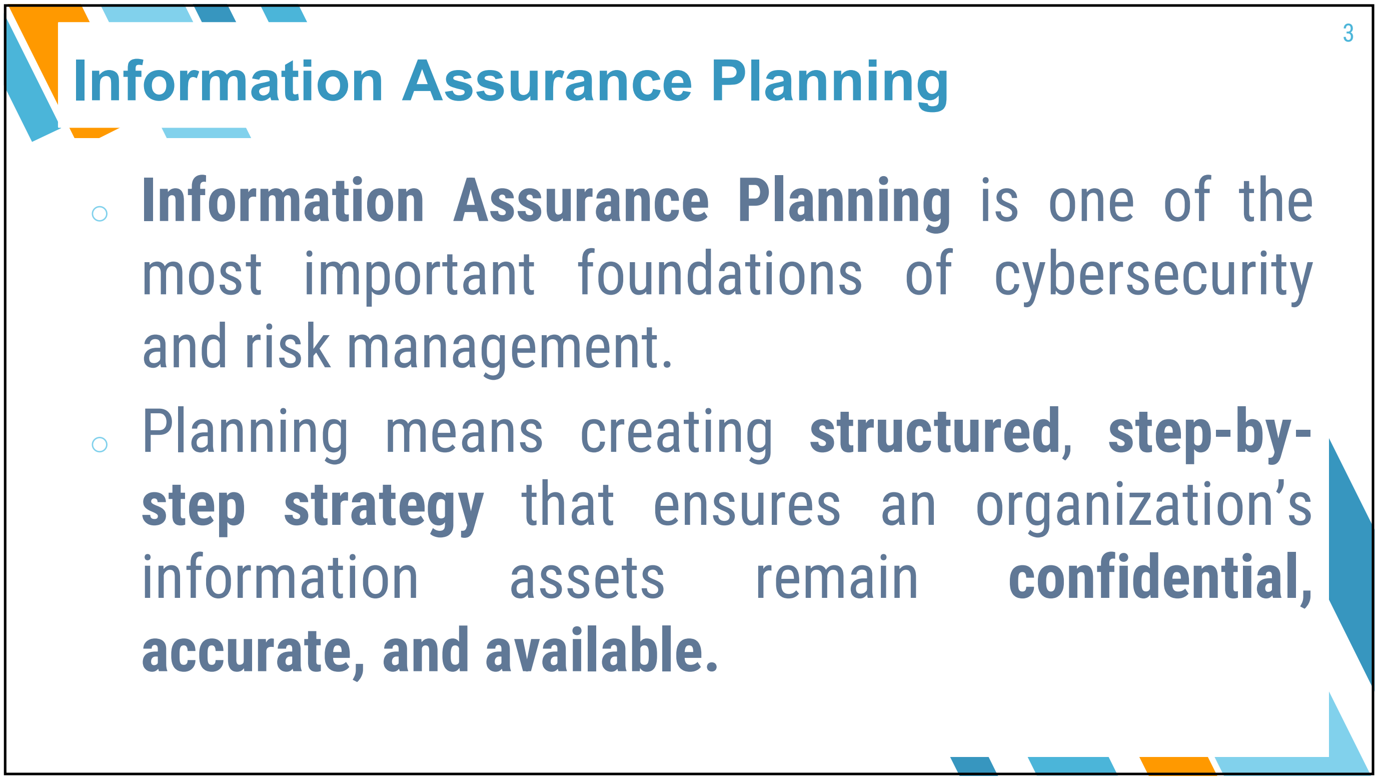


Learning Objectives

By the end of the lesson, students should be able to:

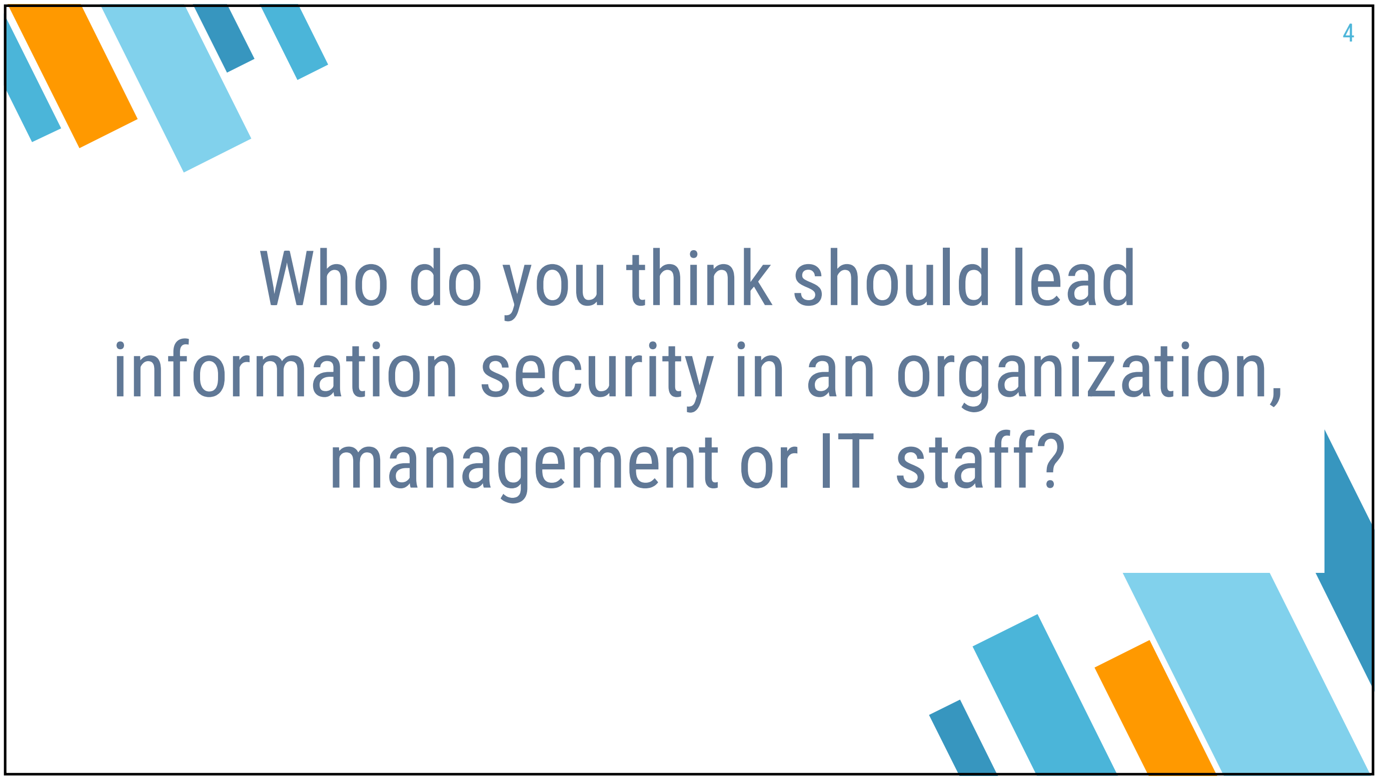
- **Describe** the different approaches to implementing Information Assurance (IA): top-down, bottom-up, and hybrid.
- **Explain** why IA policies are essential for organizational security and compliance.
- **Analyze** real-world cases to evaluate the effectiveness of IA policies.
- **Differentiate** between weak and strong IA policy practices.
- **Apply** knowledge by recommending improvements to IA implementation strategies in case scenarios.

2



Information Assurance Planning

- **Information Assurance Planning** is one of the most important foundations of cybersecurity and risk management.
- Planning means creating **structured**, **step-by-step strategy** that ensures an organization's information assets remain **confidential, accurate, and available.**



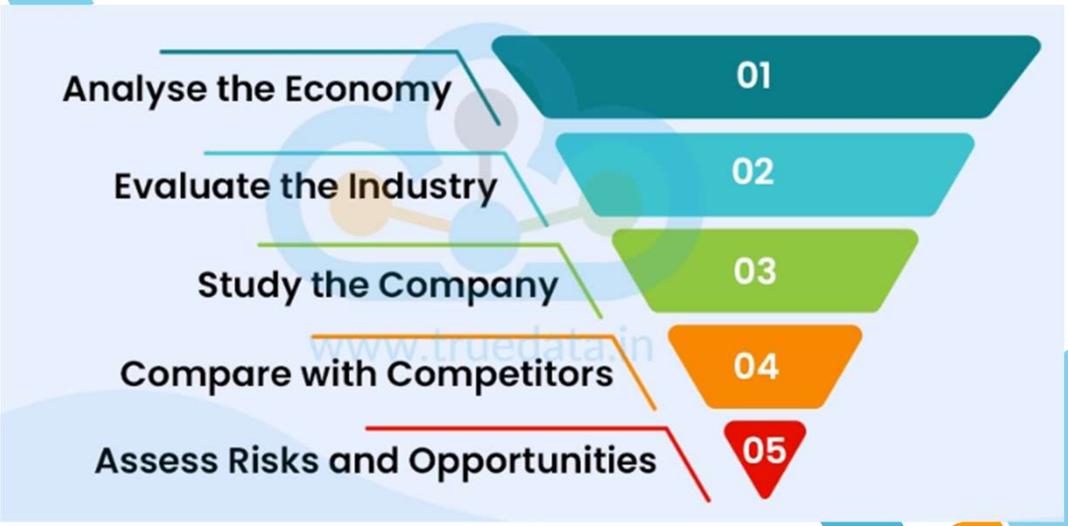
Who do you think should lead information security in an organization, management or IT staff?

Approaches to Implementing IA

Three main approaches used in organizations:

- **Top-Down Approach**
  - Start with senior management (executives, board of directors, CIO, or CISO)
  - Security strategy and policies flow downward to IT staff and employees.

5

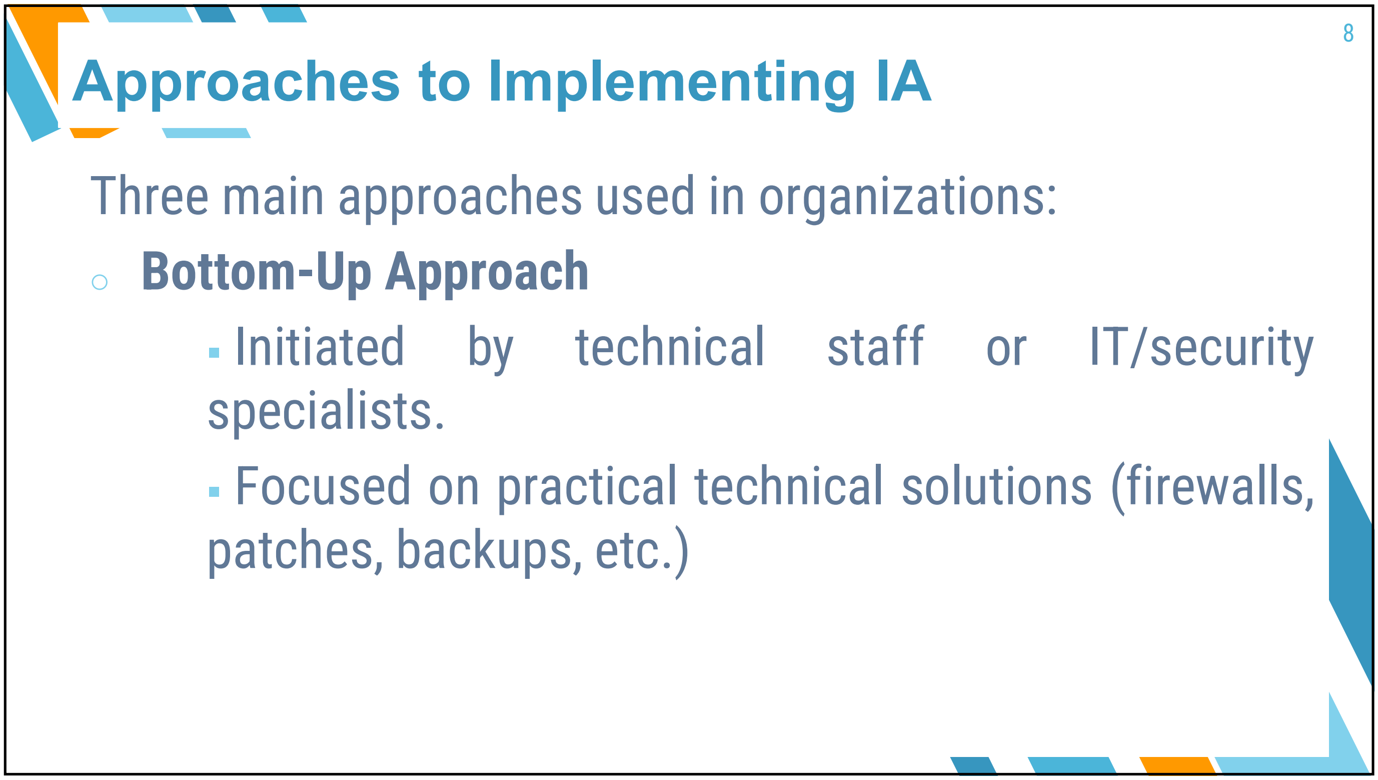


6

7

What might happen if employees find these policies impractical but are forced to follow them?

7



8

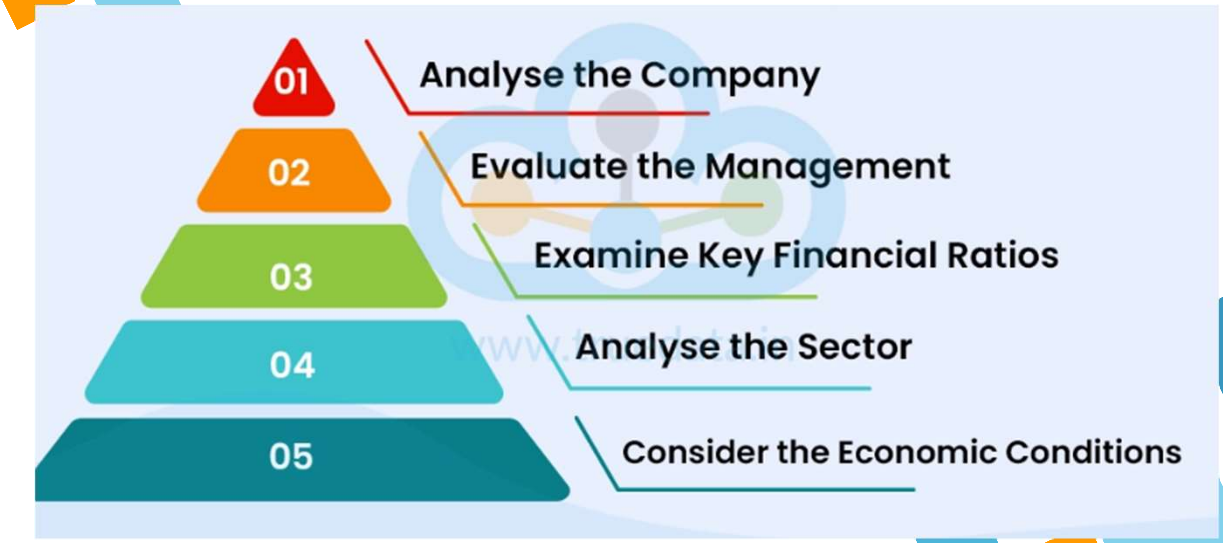
Approaches to Implementing IA

Three main approaches used in organizations:

- **Bottom-Up Approach**
  - Initiated by technical staff or IT/security specialists.
  - Focused on practical technical solutions (firewalls, patches, backups, etc.)

8

9



01 Analyse the Company

02 Evaluate the Management

03 Examine Key Financial Ratios

04 Analyse the Sector

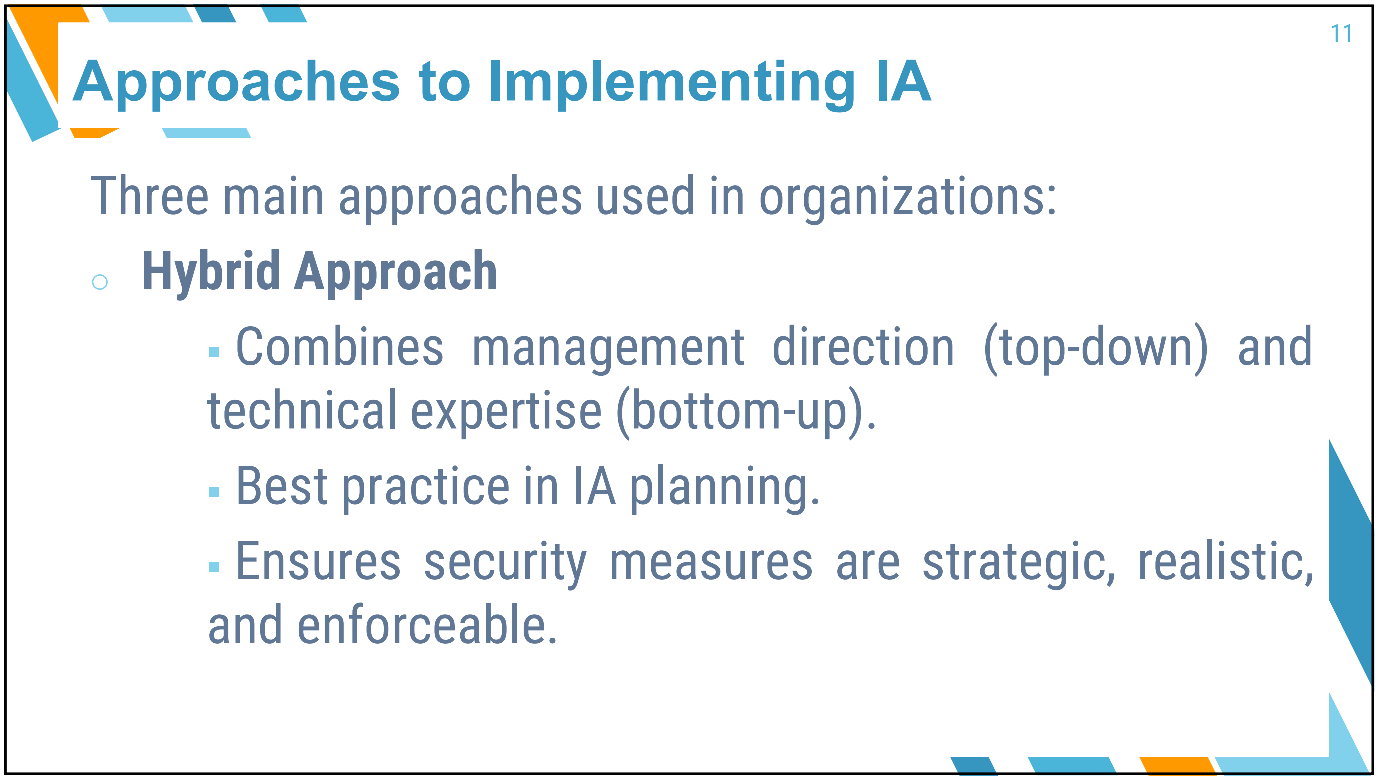
05 Consider the Economic Conditions

9

10

“Why might management sometimes ignore security concerns raised by staff?”

10



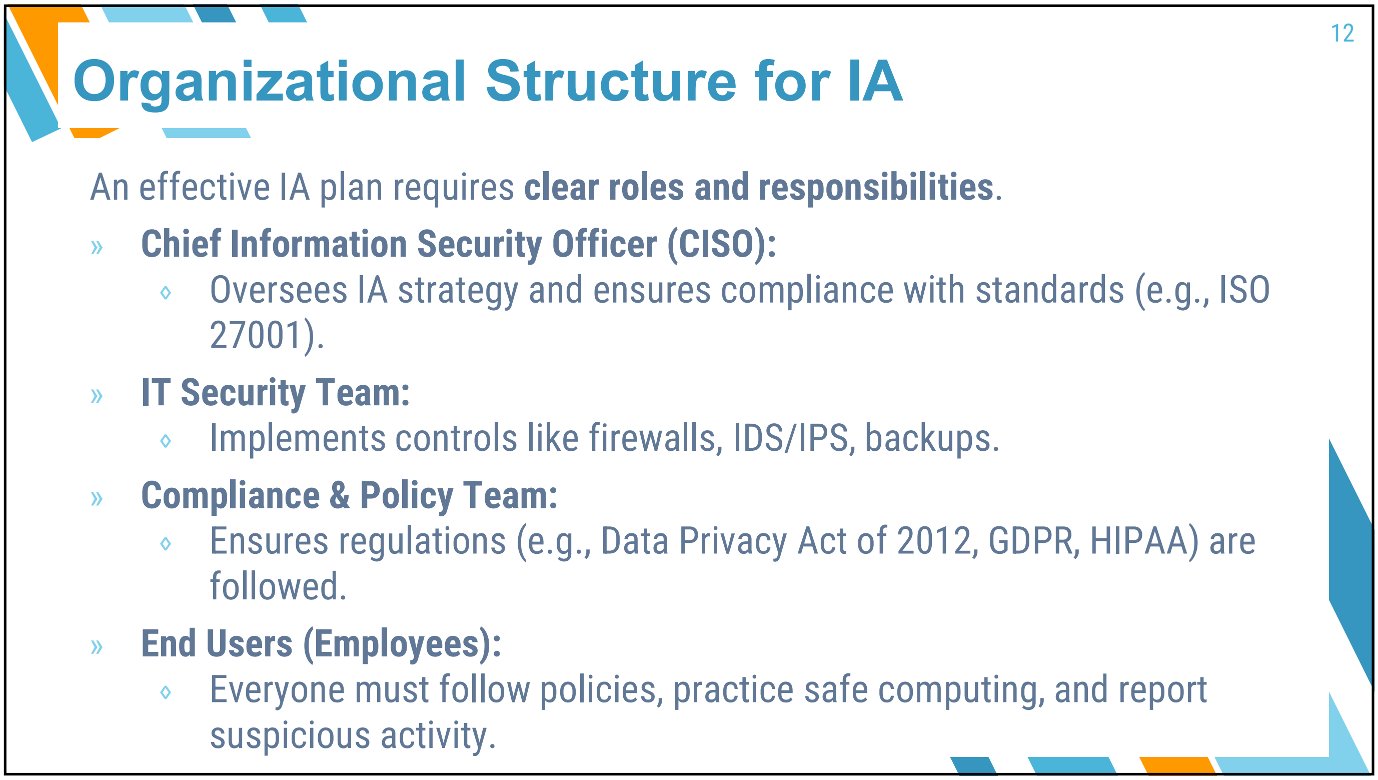
11

Approaches to Implementing IA

Three main approaches used in organizations:

- **Hybrid Approach**
  - Combines management direction (top-down) and technical expertise (bottom-up).
  - Best practice in IA planning.
  - Ensures security measures are strategic, realistic, and enforceable.

11



12

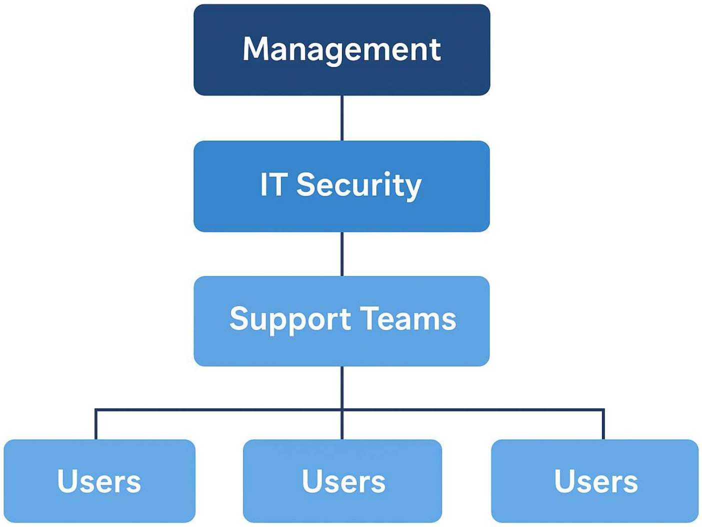
Organizational Structure for IA

An effective IA plan requires **clear roles and responsibilities**.

- **Chief Information Security Officer (CISO):**
  - Oversees IA strategy and ensures compliance with standards (e.g., ISO 27001).
- **IT Security Team:**
  - Implements controls like firewalls, IDS/IPS, backups.
- **Compliance & Policy Team:**
  - Ensures regulations (e.g., Data Privacy Act of 2012, GDPR, HIPAA) are followed.
- **End Users (Employees):**
  - Everyone must follow policies, practice safe computing, and report suspicious activity.

12

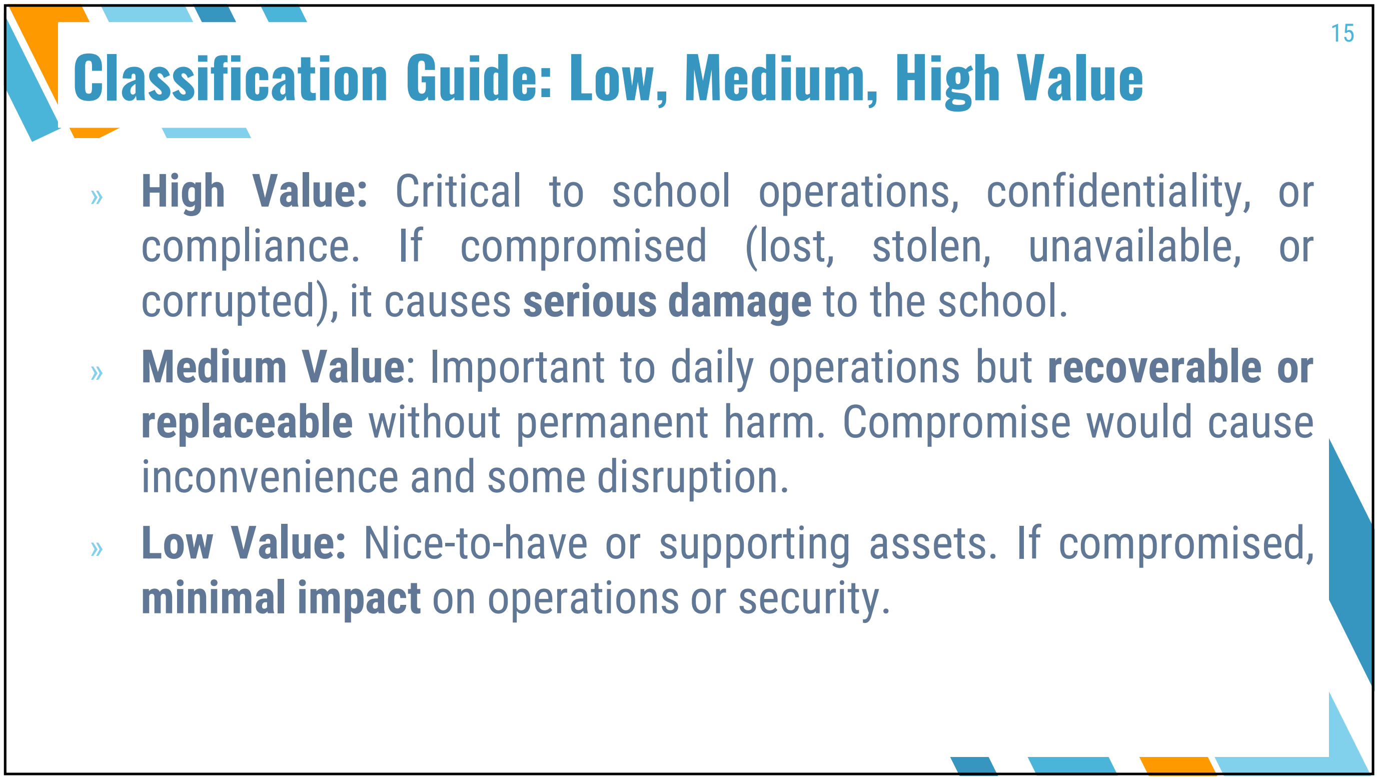
Sample Organizational Chart



Asset Management in IA

Steps in Asset Management:

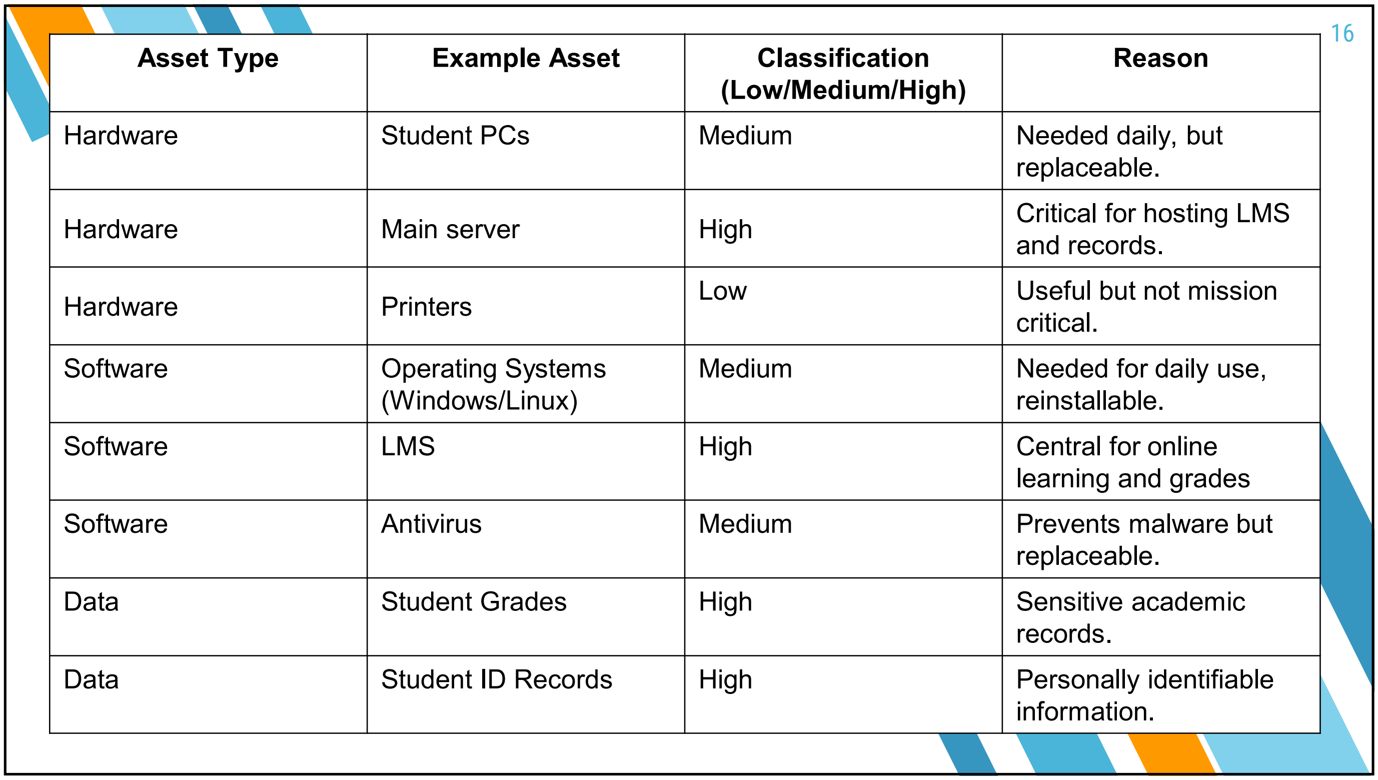
- **Inventory:** List all assets (hardware, software, data, people, processes).
  - Example: Servers, laptops, databases, customer records.
- **Classification:** Assign categories based on sensitivity.
  - Public, Internal Use, Confidential, Restricted.
- **Valuation:** Assess importance to the organization.
  - What would happen if the asset is lost, stolen, or compromised?



Classification Guide: Low, Medium, High Value

- **High Value:** Critical to school operations, confidentiality, or compliance. If compromised (lost, stolen, unavailable, or corrupted), it causes **serious damage** to the school.
- **Medium Value**: Important to daily operations but **recoverable or replaceable** without permanent harm. Compromise would cause inconvenience and some disruption.
- **Low Value:** Nice-to-have or supporting assets. If compromised, **minimal impact** on operations or security.

15



Asset Type	Example Asset	Classification (Low/Medium/High)	Reason
Hardware	Student PCs	Medium	Needed daily, but replaceable.
Hardware	Main server	High	Critical for hosting LMS and records.
Hardware	Printers	Low	Useful but not mission critical.
Software	Operating Systems (Windows/Linux)	Medium	Needed for daily use, reinstallable.
Software	LMS	High	Central for online learning and grades
Software	Antivirus	Medium	Prevents malware but replaceable.
Data	Student Grades	High	Sensitive academic records.
Data	Student ID Records	High	Personally identifiable information.

16

Group Activity:

Threat Identification for School Computer Lab

- Select three assets from the school computer lab (e.g., PCs, LMS, student grades).
- For each asset, identify at least on possible threat (e.g., malware, unauthorized, access, hardware failure).
- Rate the impact of each threat as **Low**, **Medium**, or **High**.
- Write your answers in the table format.

IA Risk Management

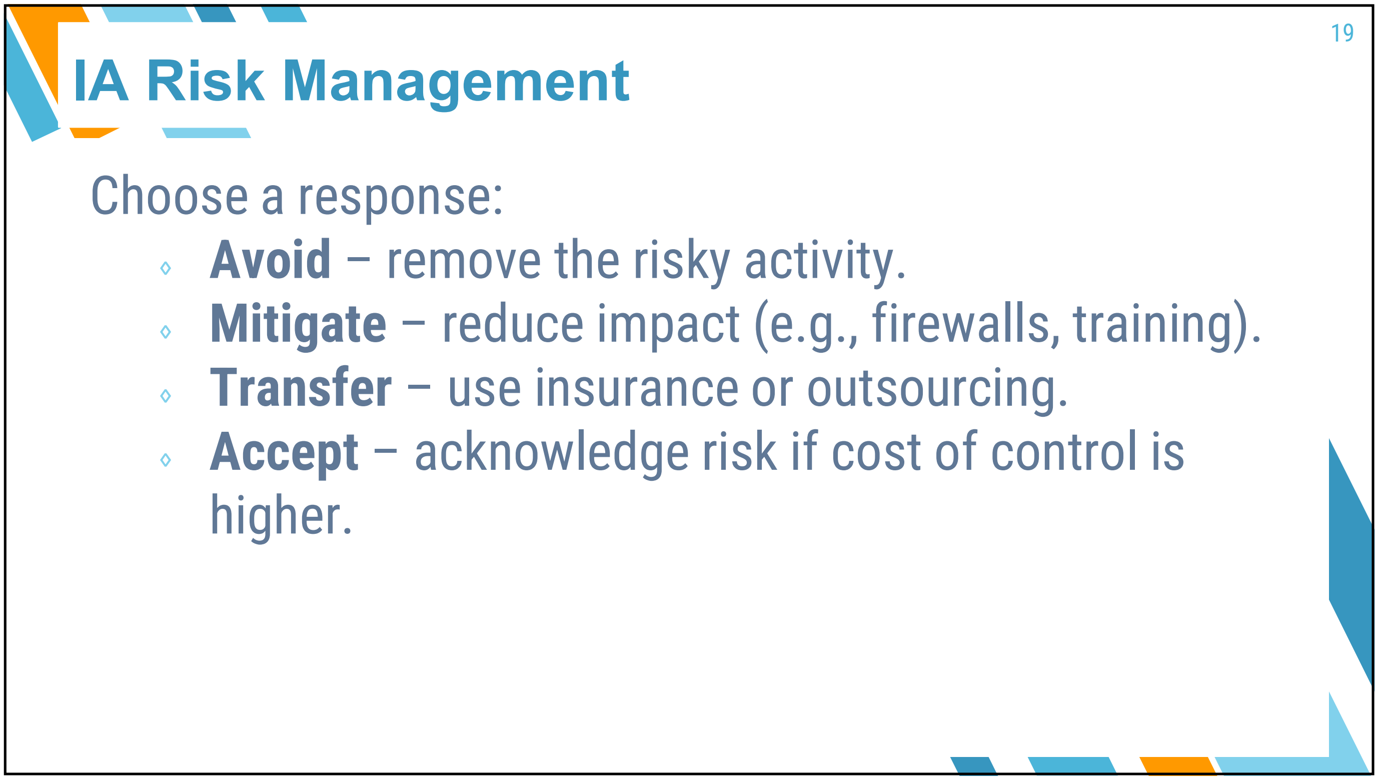
Risk management is the process of identifying, assessing, and responding to potential threats.

Steps in IA Risk Management (NIST SP 800-30, ISO/IEC 27005):

- Identify risks.
- Analyze risks (likelihood × impact).
- Evaluate risks (decide which need treatment).
- Threat risks (avoid, transfer, mitigate, accept).
- Monitor and review continuously.

Risk Matrix Example:

- Low likelihood + High impact ⟶ Monitor.
- High likelihood + High impact ⟶ Immediate action.

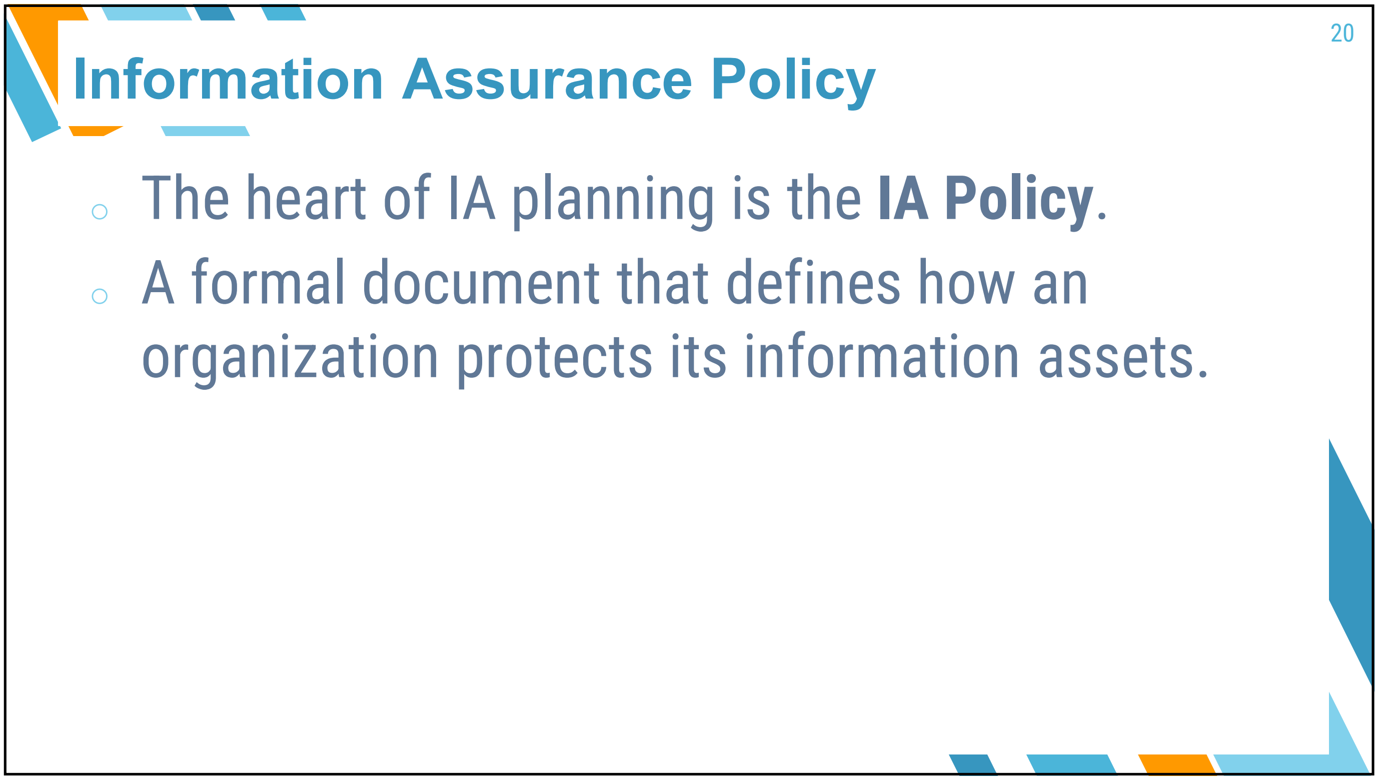


19

IA Risk Management

Choose a response:

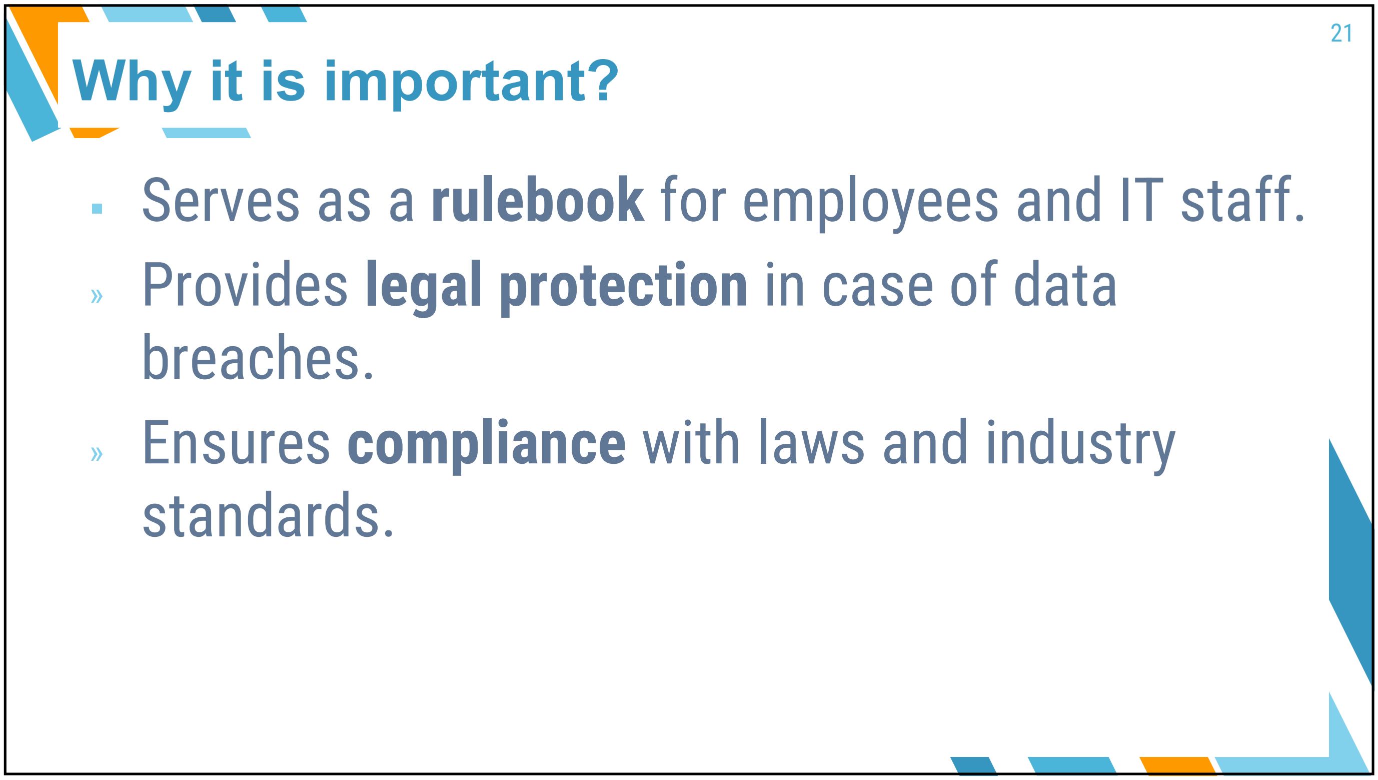
- **Avoid** – remove the risky activity.
- **Mitigate** – reduce impact (e.g., firewalls, training).
- **Transfer** – use insurance or outsourcing.
- **Accept** – acknowledge risk if cost of control is higher.



20

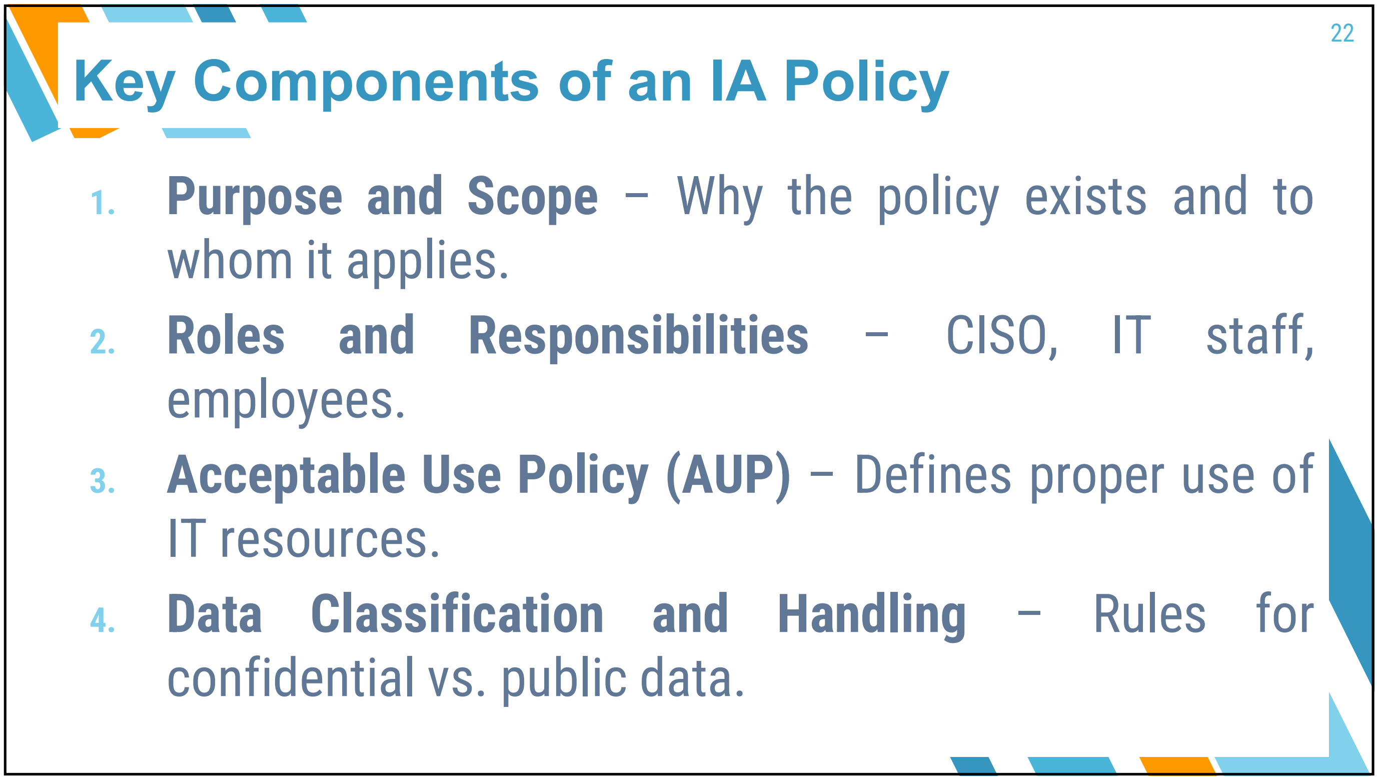
Information Assurance Policy

- The heart of IA planning is the **IA Policy**.
- A formal document that defines how an organization protects its information assets.



Why it is important?

- Serves as a **rulebook** for employees and IT staff.
- Provides **legal protection** in case of data breaches.
- Ensures **compliance** with laws and industry standards.



Key Components of an IA Policy

1. **Purpose and Scope** – Why the policy exists and to whom it applies.
2. **Roles and Responsibilities** – CISO, IT staff, employees.
3. **Acceptable Use Policy (AUP)** – Defines proper use of IT resources.
4. **Data Classification and Handling** – Rules for confidential vs. public data.

Key Components of an IA Policy

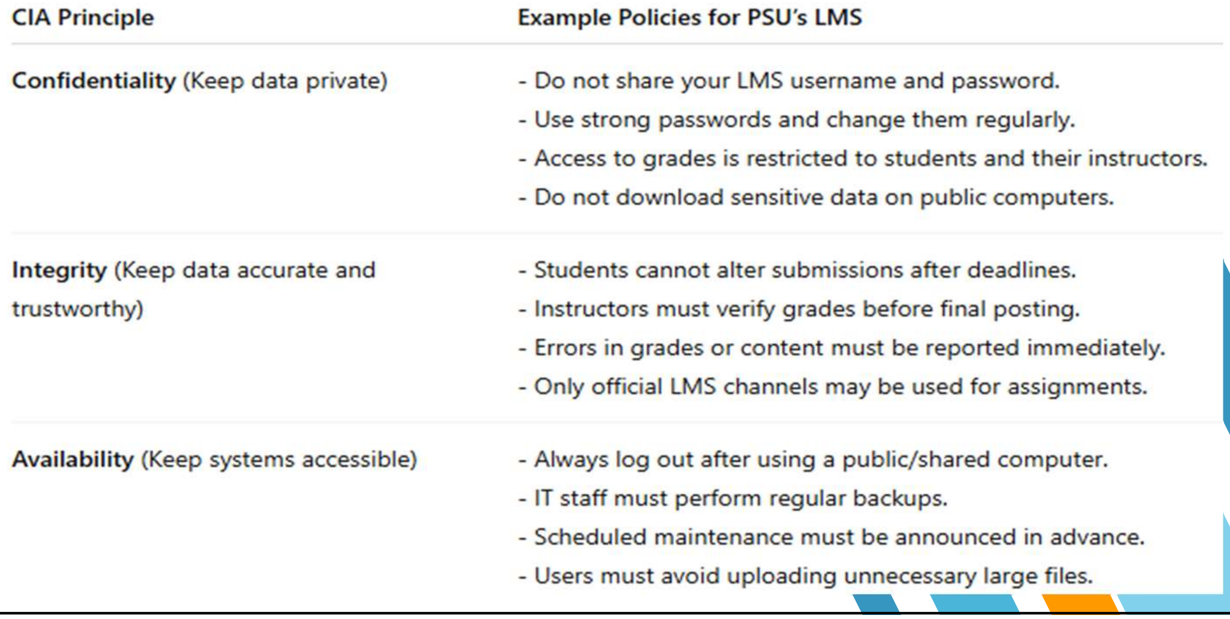
5. **Access Control Rules**– Who can access what data.

6. **Risk Management Procedures**– how risks are identified and mitigated.

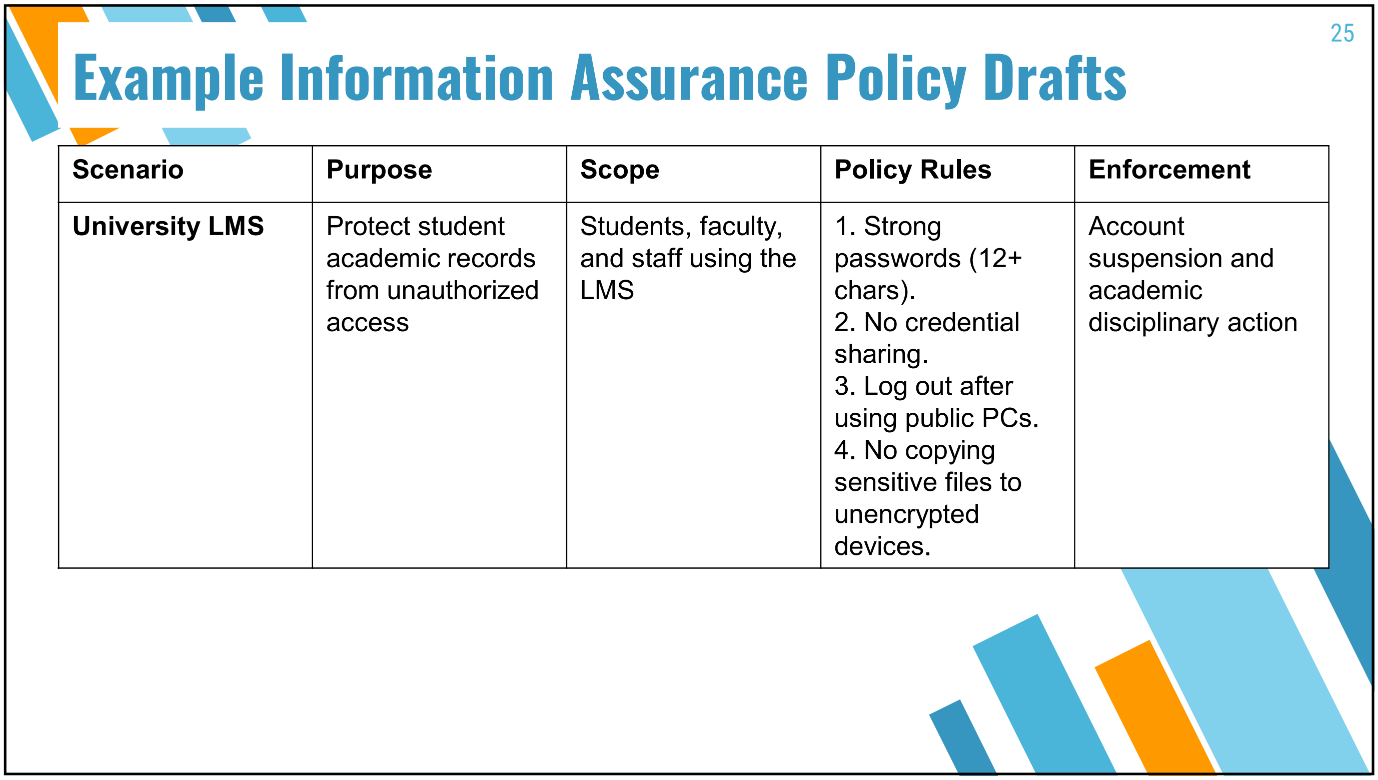
7. **Incident Response** – How to respond to a breach or cyberattack.

8. **Compliance Requirements** – Data Privacy Act, ISO standards, etc.

Policy PSU's LMS



CIA Principle	Example Policies for PSU's LMS
Confidentiality (Keep data private)	- Do not share your LMS username and password. - Use strong passwords and change them regularly. - Access to grades is restricted to students and their instructors. - Do not download sensitive data on public computers.
Integrity (Keep data accurate and trustworthy)	- Students cannot alter submissions after deadlines. - Instructors must verify grades before final posting. - Errors in grades or content must be reported immediately. - Only official LMS channels may be used for assignments.
Availability (Keep systems accessible)	- Always log out after using a public/shared computer. - IT staff must perform regular backups. - Scheduled maintenance must be announced in advance. - Users must avoid uploading unnecessary large files.



Example Information Assurance Policy Drafts

Scenario	Purpose	Scope	Policy Rules	Enforcement
University LMS	Protect student academic records from unauthorized access	Students, faculty, and staff using the LMS	1. Strong passwords (12+ chars). 2. No credential sharing. 3. Log out after using public PCs. 4. No copying sensitive files to unencrypted devices.	Account suspension and academic disciplinary action