Access Control, Authentication, and Public Key Infrastructure

Lesson 3

Business Drivers for Access Controls

Learning Objective

- Analyze how a data classification standard impacts an IT infrastructure's access control requirements and implementation.

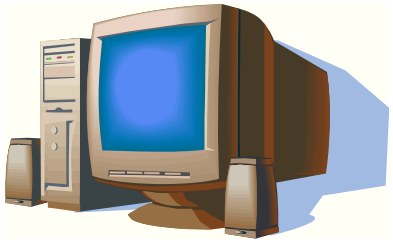
Key Concepts

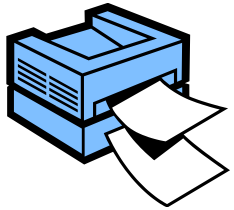
- Business requirements for asset protection
- Privacy and privacy laws
- Privacy regulations compliance
- Access control implementation
- Data classification

Data or Information Assets

An intangible asset with no form or substance:

- Paper records
- Electronic media
- Intellectual property stored in people's heads





Importance of Policy and Senior Management Role

- Organizations value intellectual property
- Must control access to information to ensure survival
- Protecting confidential information involves:
  - Technical controls
  - Clear policies and sound business processes that implement those policies
- Access control policies are effective only with support of senior executives

Classification Schemes

- **Classification scheme** is a method of organizing sensitive information into access levels
- Only a person with the approved level of access is allowed to view information
- This access is called clearance
- Every organization has its own method of determining clearance levels

Classification Schemes (Cont.)

- National Security Classification
  - Unclassified
  - Confidential
  - Secret
  - Top Secret
- Corporations
  - Public
  - Internal
  - Sensitive
  - Highly sensitive

Sensitivity-Based Data Classification

In a hospital, for example, a data classification scheme would identify the sensitivity of every piece of data in the hospital, from the cafeteria menu to patient medical records.

Classified as Public

For use by defined category within job role

Need to Know and Least Privilege

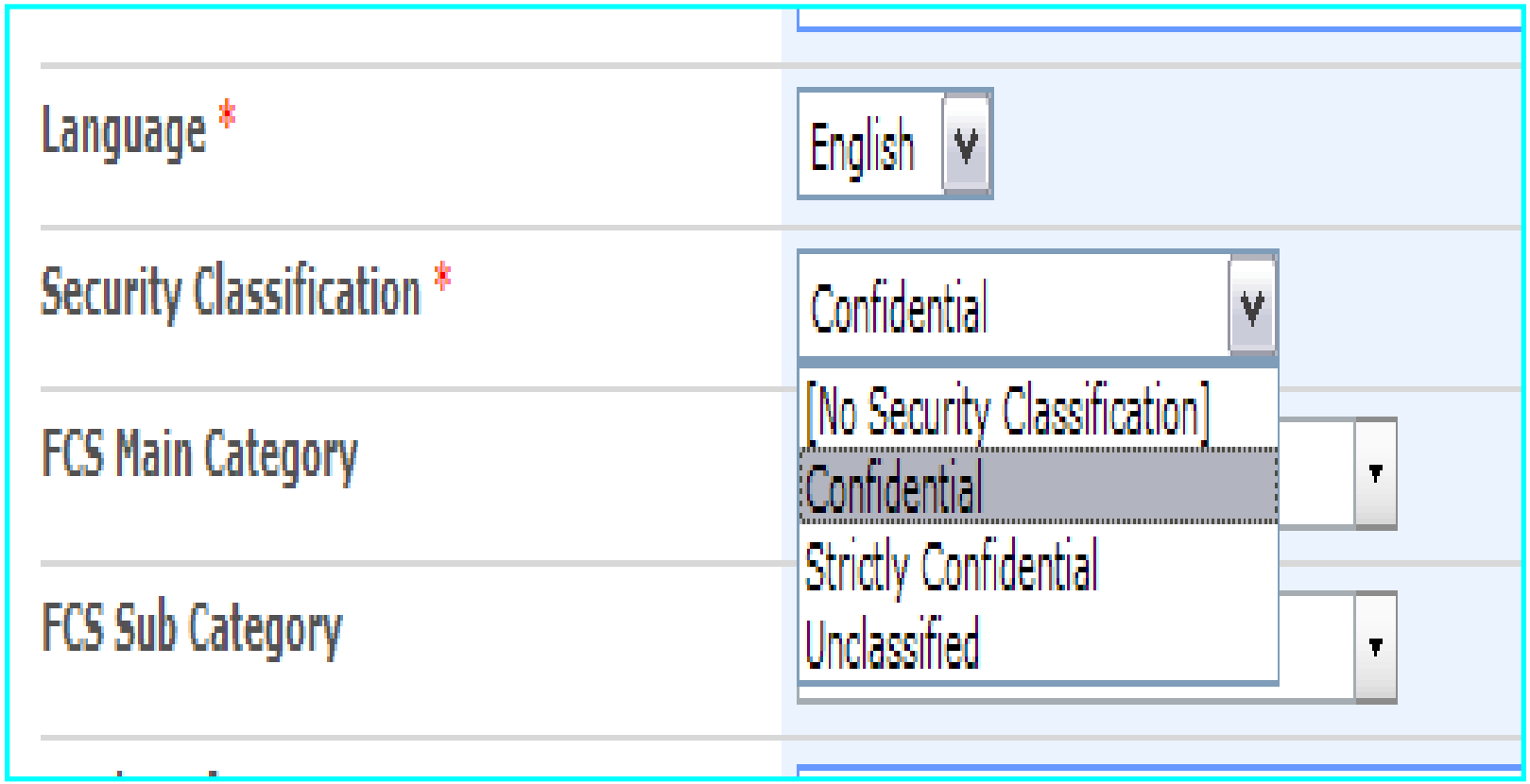
- Need to know
  - Requester should not receive access just because of his or her clearance, position, or rank
  - Requester must establish a valid need to see information
  - Access should be granted only if information is vital for requester's official duties
- Least privilege
  - A computer user or program should have only the access needed to carry out its job

Declassification

- Automatic
- Systematic
- Mandatory declassification review
- Freedom of Information Act request

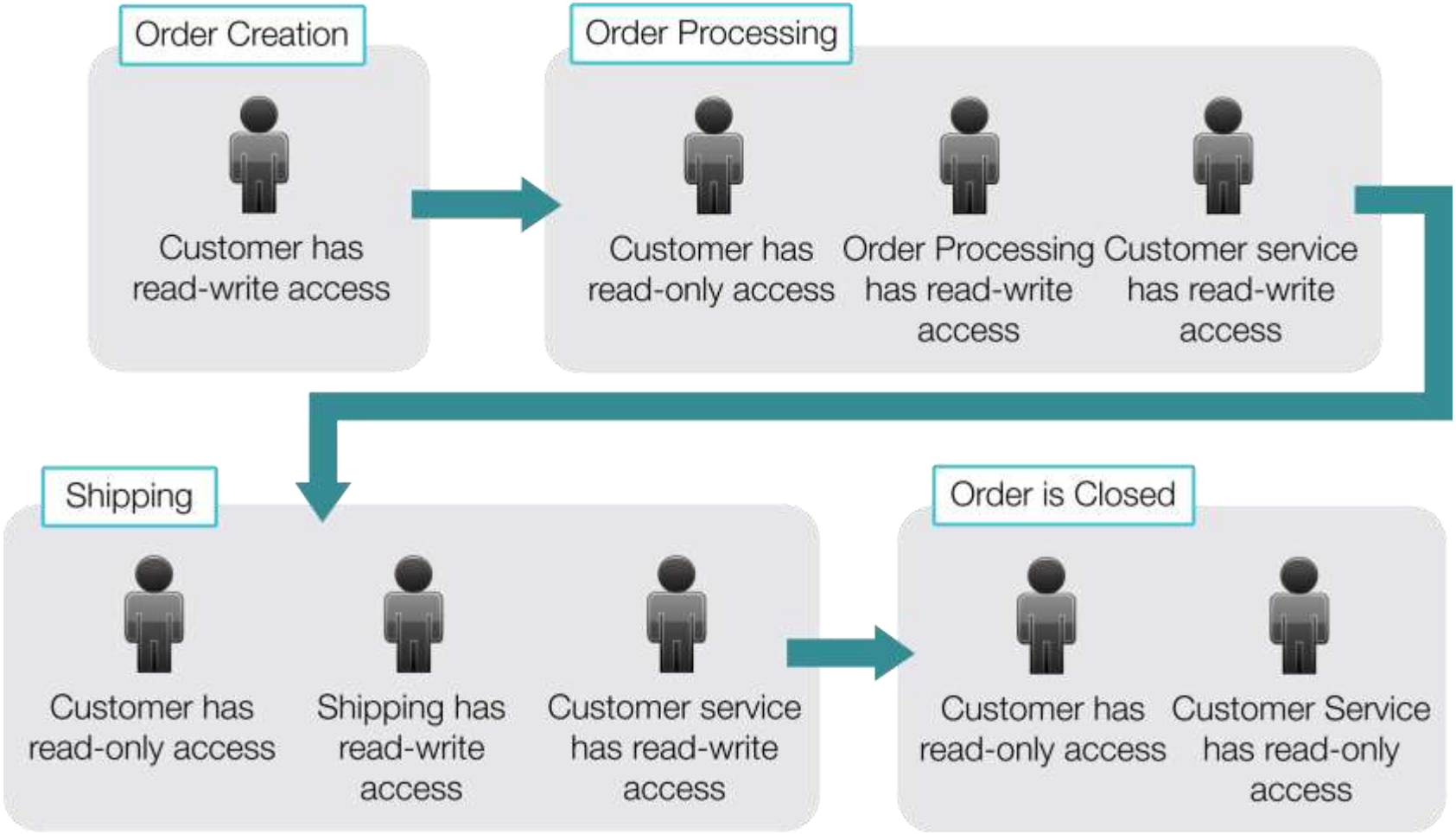
Business Drivers for Access Control

Electronic Records

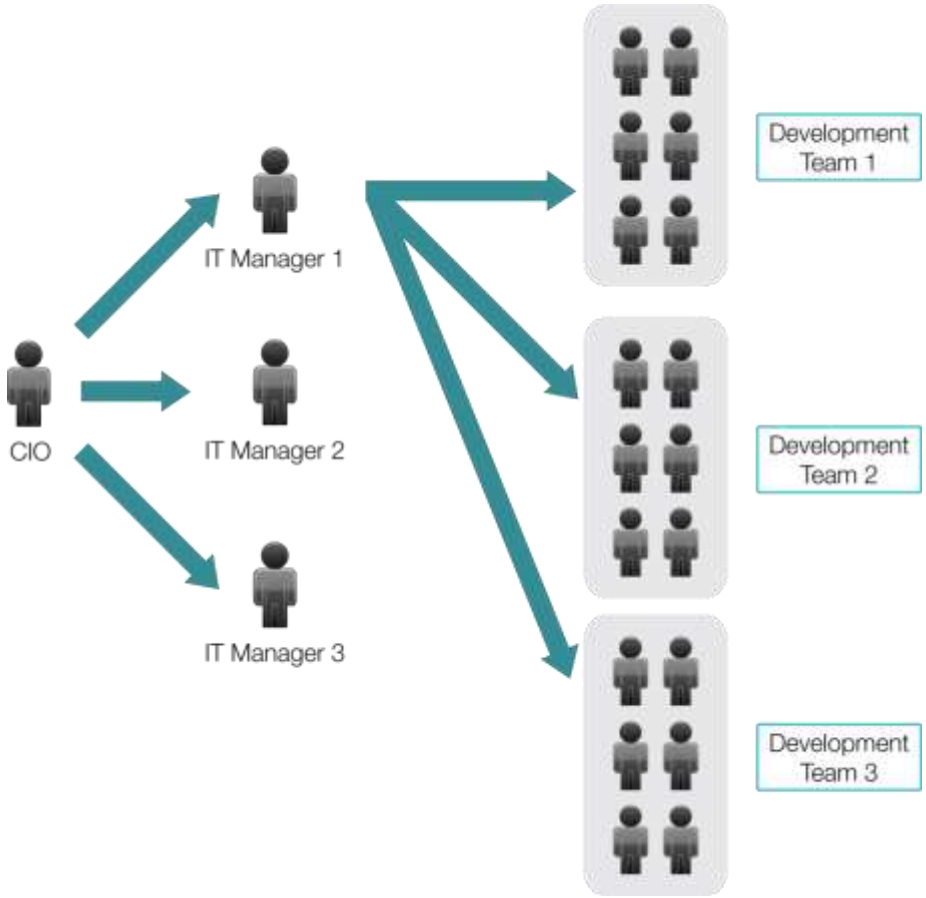


United Nations Electronic Data Classification

The Life Cycle of an Order



Accidental Dissemination of Electronic Information



Controlling Access and Protecting Value

- Importance of internal access controls
- Importance of external access controls
- Implementation of access controls with respect to contractors, vendors, and third parties

Summary

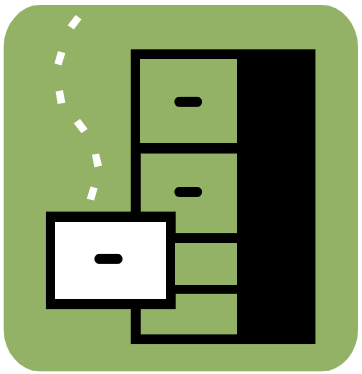
- Business requirements for asset protection
- Privacy and privacy laws
- Privacy regulations compliance
- Access control implementation
- Data classification

Virtual Lab

- Configure Windows File System Permissions

Physical Security of Sensitive Information

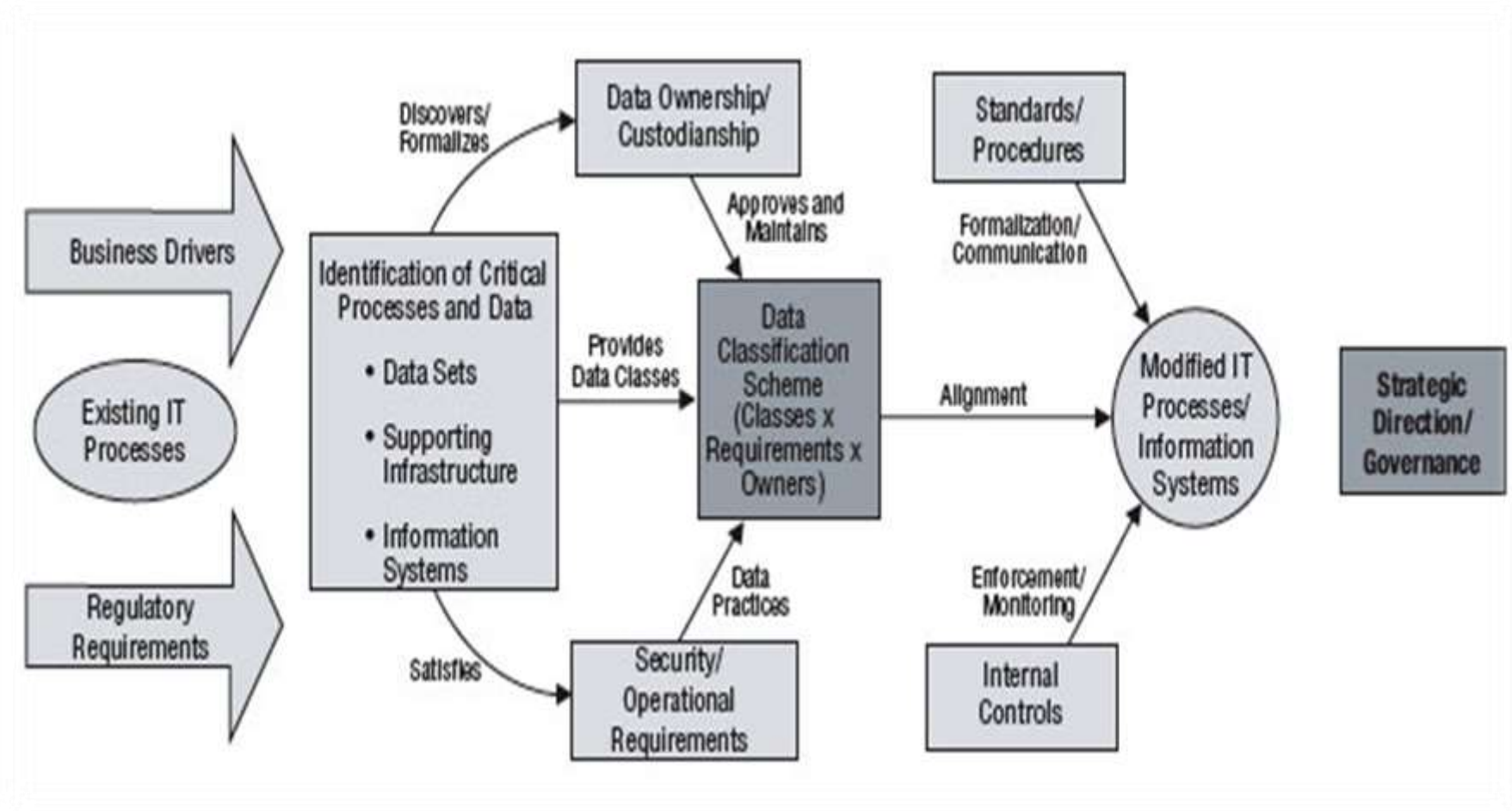
- Refers to security of records and information not in electronic systems and applications
- Access is regularly linked to functional responsibilities and not to position or grade
- Security or background investigation required



Secure storage and limited access

Can/Should this information be shared?

ISACA Model for Business Data Classification



Data Destruction

- Use appropriate secure destruction method for the media and format.
- Do not put in trash bins.
- Data awaiting destruction should be placed in lockable containers.
- Strictly confidential and confidential data is destroyed in accordance with specific guidelines.

Data Destruction (Continued)

Light office shredder/disintegrator

Portable devices

Electronic media

Shredder/Degausser

Portable devices