14.1 Laws, regulations, and standards

Laws and regulations

Effective security governance is achieved with clear policies that account for both internal and external factors. Policy development requires consideration of internal factors such as alignment with business objectives, utilization of internal data, and resource allocation. Ex: Determining which employee roles require access to financial data.

External considerations include laws, regulations, and industry standards, influenced by location, industry, and purpose. Ex: The Sarbanes-Oxley act (SOX) regulates US public companies' financial disclosures, while the California consumer privacy act (CCPA) protects California residents' privacy, applying to companies with California customers.

An organization must comply with relevant laws and regulations. Non-compliance may result in fines, sanctions, loss of license, or contractual impacts. Ex: An organization loses a US Federal contract due to non-compliance with the Federal information security management act (FISMA).

Compliance may be monitored and reported internally or by a third party. Automation can be leveraged for monitoring and reporting to ensure that compliance is maintained. ***Due diligence*** is the process of setting controls to maintain compliance, while ***due care*** is the process of implementing, maintaining, and responding to those controls. The executive responsible for compliance signs official documentation to acknowledge and attest to the organization's alignment with compliance requirements.

Table 14.1.1: Laws and regulations.

Law	Purpose	Jurisdiction	Applies to
Health insurance portability and accountability act (HIPAA)	Regulate and protect electronic healthcare records	US	Any company that stores or processes healthcare information of US residents
Sarbanes-Oxley act (SOX)	Protect investors by regulating financial disclosures	US	US-based public companies
Federal information security management act (FISMA)	Require security of information and information systems	US	US federal agencies

California consumer privacy act (CCPA)	Protect personal information and privacy	California	Any company that stores or processes personal information of California residents
General data protection regulation (GDPR)	Protect personal information and privacy	EU	Any company that stores or processes personal information of EU residents
Digital personal data protection act (DPDP act)	Protect personal information and privacy	India	Any company that stores or processes personal information of India residents

PARTICIPATION ACTIVITY 14.1.1: Laws and regulations.

1) Which US law establishes processes to maintain patient privacy?
   - HIPAA
   - GDPR
   - SOX

2) An organization operating in Italy, Greece, or Spain is subject to which data protection law?
   - CCPA
   - FISMA
   - GDPR

3) Which law details information security requirements for a PC connected to a US military base's LAN?
   - SOX
   - FISMA
   - GDPR

4) Which law enables a California resident to request all collected personal data from an organization?

- CCPA
- GDPR
- FISMA

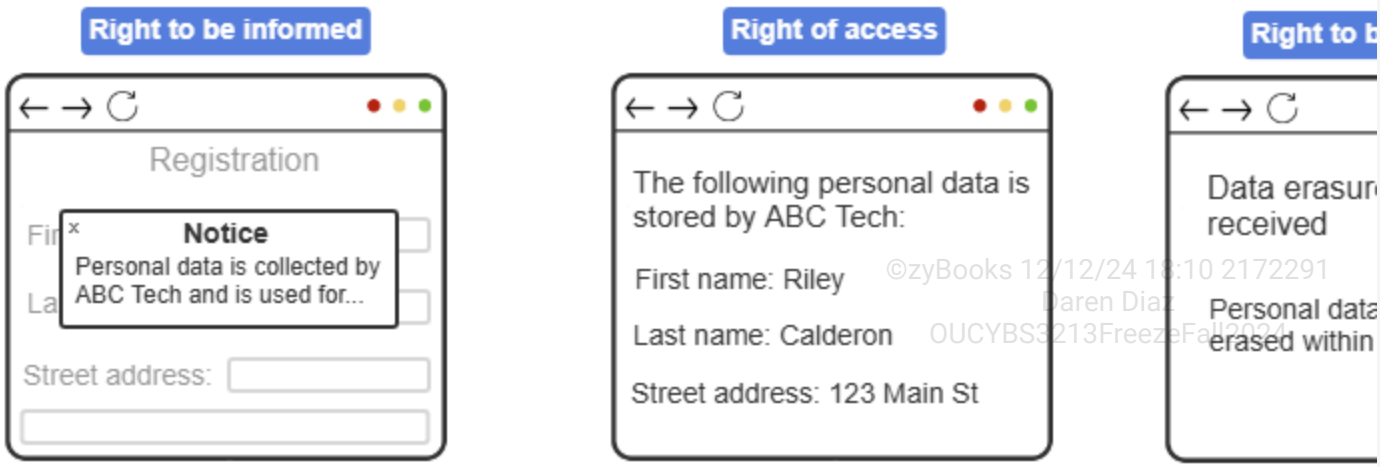
GDPR

Organizations handling EU residents' personal data must comply with GDPR regulations. Violation of the GDPR can result in fines as high as $20 million. The GDPR mandates limited storage, transparency, and legitimate collection of personal information.

The GDPR grants EU residents eight privacy rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to be forgotten
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

PARTICIPATION ACTIVITY 14.1.2: Rights granted by the GDPR.



Animation content:

Static figure: Three web browsers labeled Right to be informed, Right of access, and Right to be forgotten.
Step 1: When personal data is collected, an organization must inform the individual of the data being collected, the purpose of the data collection, and the identity of the organization collecting the data.
A web page appears in the Right to be informed web browser. A cursor clicks a "Register" button. A registration page appears with fields for first name, last name, and street address. A popup appears that says, "Notice: Personal data is collected by ABC Tech and is used for..."
Step 2: An individual has the right to request information about personal data including a copy of the personal data, the purpose of the data collection, and any recipients to whom the data has been disclosed.
An account settings page appears in the Right of access web browser. A cursor clicks a "Request data access" button. The following text appears on the web page: "The following personal data is stored by ABC Tech: First name: Riley, Last name: Calderon, Street address: 123 Main St."
Step 3: An individual has the right to request the removal of personal data. An organization must grant the request within 30 days unless the data is necessary for legal compliance or public health.
An account settings page appears in the Right to be forgotten web browser. A cursor clicks a "Request data erasure" button. The following text appears on the web page: "Data erasure request received. Personal data will be erased within 30 days."

Animation captions:

1. When personal data is collected, an organization must inform the individual of the data being collected, the purpose of the data collection, and the identity of the organization collecting the data.
2. An individual has the right to request information about personal data including a copy of the personal data, the purpose of the data collection, and any recipients to whom the data has been disclosed.
3. An individual has the right to request the removal of personal data. An organization must grant the request within 30 days unless the data is necessary for legal compliance or public health.

PARTICIPATION ACTIVITY 14.1.3: GDPR individual rights.

How to use this tool

The right to rectification **The right to be informed** **The right to be forgotten**

The right to restrict processing | The right to object | The right of access | The right to data portability

	When personal data is collected, an individual must be notified of the purpose.
	An individual can obtain a copy of stored personal data.
	An individual can correct inaccurate or incomplete personal data.
	An individual can have personal data erased.
	An individual can prevent further processing of personal data.
	An individual can obtain and transfer personal data in a structured, machine-readable format.
	An individual can protest the storage or processing of personal data.

Reset

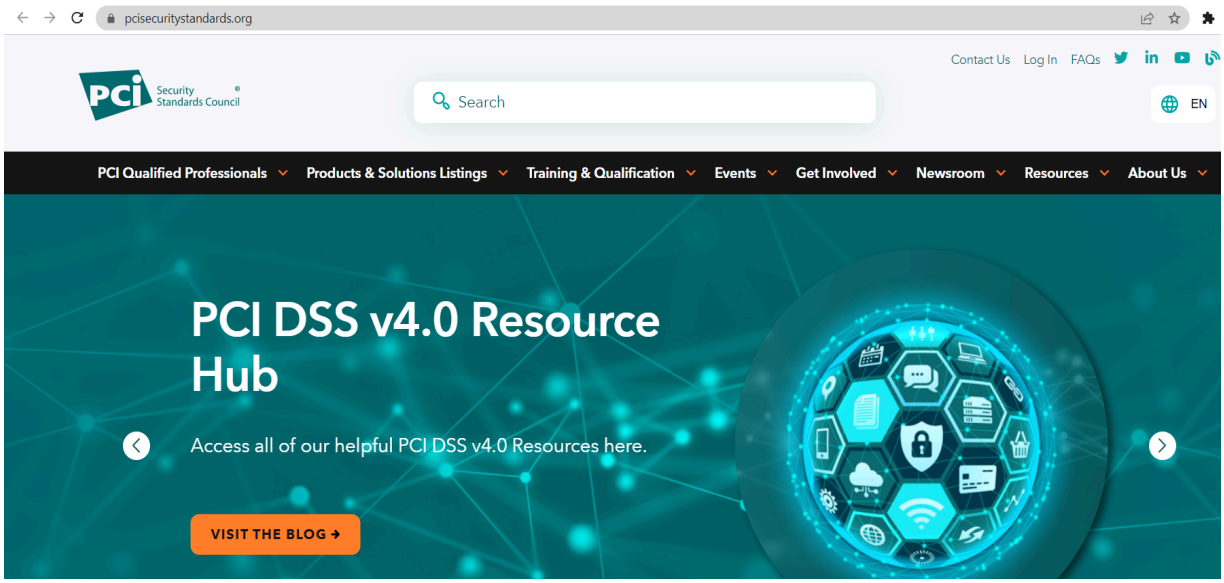
Payment Card Industry Data Security Standard

The ***payment card industry (PCI)*** includes financial institutions and organizations who process or are involved in the processing of payment cards (debit card, credit card, prepaid card, etc.). The ***PCI Security Standards Council (PCI SSC)*** is a coalition of PCI stakeholders who develop security standards to secure payment card accounts and transactions. The ***PCI Data Security Standard (PCI DSS)*** is the PCI SSC's payment card account protection standard. PCI DSS includes 12 compliance requirements:

1. Install and maintain network security controls
2. Apply secure configurations to all system components
3. Protect stored account data

4. Protect cardholder data with strong cryptography during transmission over open, public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict access to system components and cardholder data based on business requirements
8. Identify users and authenticate access to system components
9. Restrict physical access to cardholder data
10. Log and monitor all access to system components and cardholder data
11. Test security of systems and networks regularly
12. Support information security with organizational policies and programs

Figure 14.1.1: The PCI SSC website.



PARTICIPATION ACTIVITY 14.1.4: PCI DSS compliance regulations.

Select the PCI DSS compliance requirement each security control satisfies.

1) Deploying an NGFW.

- ○ Install a network security control
- ○ Restrict system component access
- ○ Restrict physical access to cardholder data

2) Using a complex password rather than a default password for a WAP administrator account.

- Test security of systems regularly
- Test security of networks regularly
- Apply secure configurations to all system components

3) Encrypting transmissions between an organization's headquarters and a branch office.

- Protect cardholder data with strong cryptography
- Identify users and authenticate access
- Log and monitor all access to system components

4) Installing anti-malware software on all endpoints.

- Protect stored account data
- Support information security with organizational policies
- Protect all systems from malicious software

CHALLENGE ACTIVITY 14.1.1: Regulations and standards.

581480.4344582.qx3zqy7

Start

Company S is a sales company in the private sector. Company S is based in Latvia, a member of the European Union and does business across the United States, including California. Company S processes payment cards.

Select all laws that apply to Company S.

- [ ] HIPAA
- [ ] GDPR
- [ ] FISMA
- [ ] CCPA
- [ ] PCI DSS

1 2

Check Next

14.2 Frameworks

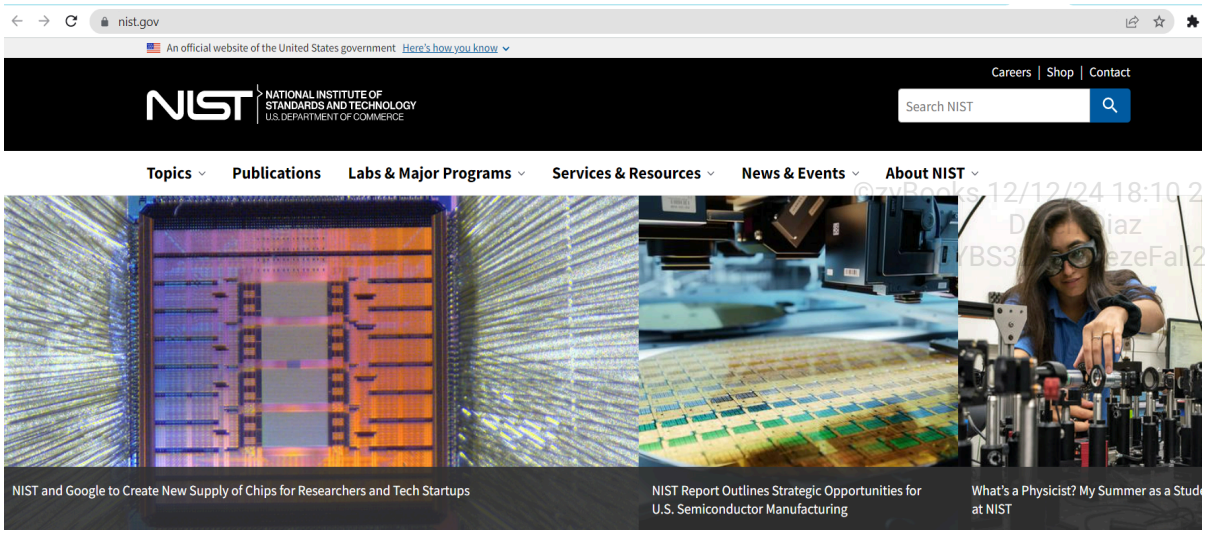
Framework organizations

A ***framework*** is a collection of guidelines, best practices, or policies a third-party develops for another organization to use. Framework organizations include:

- The ***Center for Internet Security (CIS)*** is a nonprofit organization focused on developing best practices and frameworks for cyber threat protection.
- The ***National Institute of Standards and Technology (NIST)*** is a US Department of Commerce agency focused on advancing measurement science, standards, and technology for US federal information systems.
- The ***International Organization for Standardization (ISO)*** is a standards-development cohort for the standards bodies of member countries.
- The ***International Electrotechnical Commission (IEC)*** is an international electrical and electronic technology, or electrotechnology, standards-development organization.
- The ***American Institute of Certified Public Accountants (AICPA)*** is a nonprofit organization of certified public accountants (CPAs) who develop resources to protect public interest.
- The ***Cloud Security Alliance (CSA)*** is an organization focused on developing cloud computing environment best practices.

A framework is not a regulation, but a framework may be created in response to a regulation for compliance purposes. Ex: The NIST special publication (SP) 1800-13 establishes procedures to ensure compliance with the US Cybersecurity Enhancement Act of 2014.

Figure 14.2.1: The NIST website.



PARTICIPATION ACTIVITY 14.2.1: Framework organizations.

Select the organization that develops a framework for each scenario.

1) A framework for mitigating Internet-based cyber threats for the private sector.
   - CIS
   - NIST
   - ISO

2) A framework for ensuring federal information system compliance with a law or regulation.
   - CIS
   - NIST
   - CSA

3) A security framework intended for cloud customers and cloud service providers.
   - CSA
   - TCP/IP

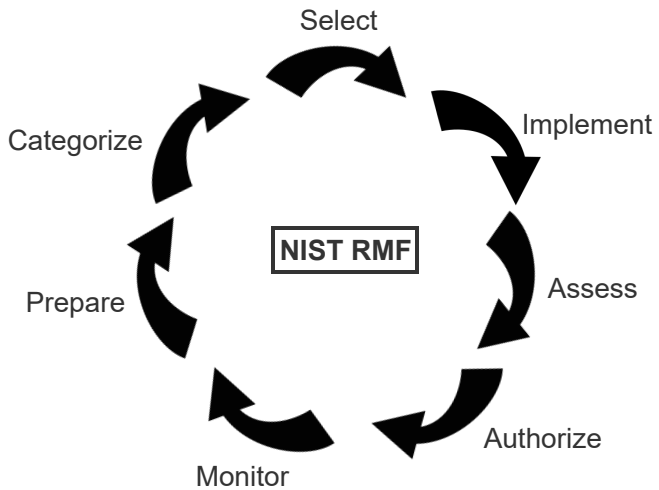
CSAB

Security frameworks

An organization is required or chooses to implement a security framework based on organizational security needs. Several security framework examples exist:

- The ***CIS Critical Security Controls (CSC)*** is a security framework consisting of recommended security controls organized in 18 different areas.
- The ***NIST Risk Management Framework (RMF)*** is a security framework required by a public sector organization to implement a systematic process of addressing the risks facing an organization known as ***risk management***.
- The ***NIST Cybersecurity Framework (CSF)*** is a NIST security framework consisting of resources to implement risk management for a private sector organization.
- The ***CSA Cloud Controls Matrix (CCM)*** is a security framework consisting of recommended security controls for each party in a cloud computing environment.
- The ***CSA enterprise architecture (EA) reference guide*** is a CSA security framework used to align organizational goals with recommended cloud infrastructure security controls.

PARTICIPATION ACTIVITY 14.2.2: The NIST RMF.



The NIST RMF consists of seven steps - prepare, categorize, select, implement, assess, authorize, and monitor.

Animation content:

Static figure: The NIST RMF steps of prepare, categorize, select, implement, assess, authorize, and monitor are represented by seven arrows arranged in a cyclical fashion.
Step 1: Preparation includes essential activities to manage security and privacy. A resource is categorized by the resource's impact analysis. The arrows representing the prepare and categorize

steps appear.
Step 2: A recommended security control is selected and implemented based on resource categorization. The arrows representing the select and implement steps appear.
Step 3: Post-implementation results are assessed to determine security control effectiveness. The arrow representing the assess step appears.
Step 4: Organizational leadership authorizes a protected resource for operation after which security professionals monitor the resource for future risks. The arrows representing the authorize and monitor steps appear. A NIST RMF label appears in the middle of the NIST RMF cycle.
.

Animation captions:

1. Preparation includes essential activities to manage security and privacy. A resource is categorized by the resource's impact analysis.
2. A recommended security control is selected and implemented based on resource categorization.
3. Post-implementation results are assessed to determine security control effectiveness.
4. Organizational leadership authorizes a protected resource for operation after which security professionals monitor the resource for future risks.

PARTICIPATION ACTIVITY 14.2.3: Security frameworks.

1) Which security framework can an organization use to implement recommended security controls?
   - CIS CSC
   - NIST RMF
   - NIST CSF

2) Which security framework requires implementation by a public sector organization?
   - CIS CSC
   - NIST RMF
   - NIST CSF

3) Which guide is used to align organizational goals with recommended cloud infrastructure security controls?
   - CSA EA

- NIST RMF
- NIST CSF

4) Which CSA framework recommends security controls for a cloud customer?

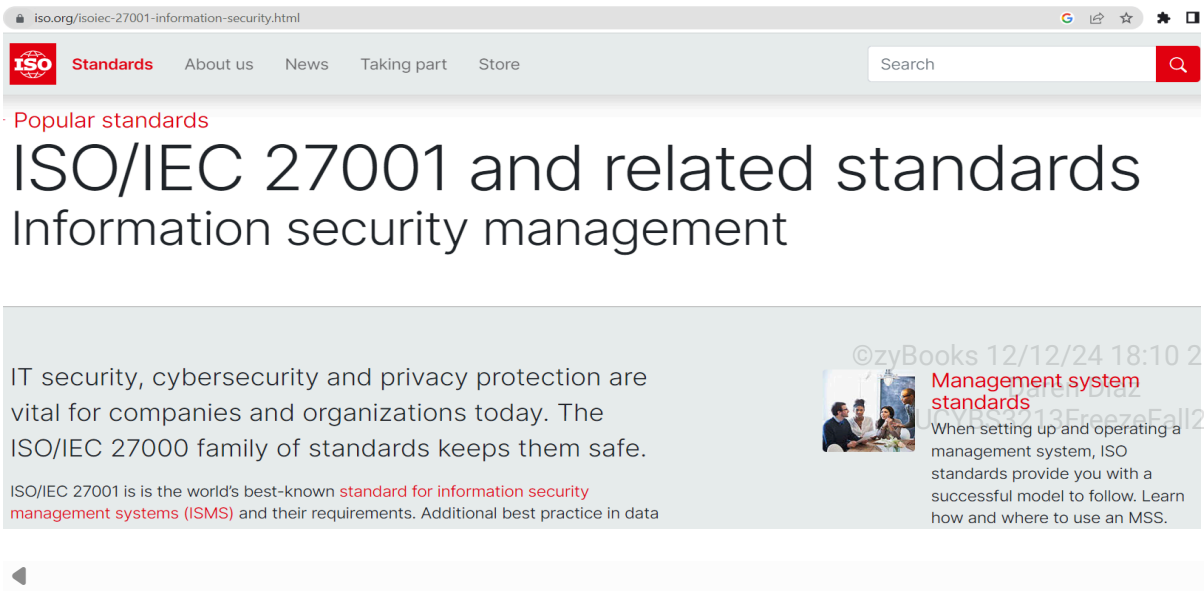
- CSC
- CSF
- CCM

ISO/IEC standards and frameworks

The ISO and IEC are both international organizations and often collaborate on standards-development to ensure consistency in a global economy. A co-developed ISO and IEC standard is referred to as an ISO/IEC standard. Several ISO/IEC security standards and frameworks exist:

- ***ISO/IEC 27001*** is a security standard and framework for the implementation of an ***information management security system (ISMS)*** for public and private sector organizations.
- ***ISO/IEC 27002*** is a security standard and framework used to guide information security control implementation within an ISMS for public and private sector organizations.
- ***ISO/IEC 27701*** is a security standard and framework for the implementation of a ***privacy information management system (PIMS)*** for public and private sector organizations.
- ***ISO/IEC 31000*** is a security standard and framework used to implement risk management.

Figure 14.2.2: The ISO/IEC 27001 and related standards website.



PARTICIPATION ACTIVITY 14.2.4: ISO/IEC standards.

1) Which ISO/IEC standard guides the creation of an ISMS?
   - ISO/IEC 11801
   - ISO/IEC 27001
   - ISO/IEC 27002

2) An organization can use which ISO/IEC standard to implement ISMS security controls?
   - ISO/IEC 27002
   - ISO/IEC 27701
   - ISO/IEC 31000

3) Which ISO/IEC security standard guides the creation of a PIMS?
   - ISO/IEC 11801
   - ISO/IEC 27001
   - ISO/IEC 27701

4) Which ISO/IEC standard helps an organization implement a systematic process of addressing the risks facing the organization?
   - ISO/IEC 27001
   - ISO/IEC 27701
   - ISO/IEC 31000

System and organization control reports

The AICPA developed system and organization controls (SOC) reports to ensure a service entity's secure handling of a user entity's financial information. A ***user entity*** is an entity who engages another entity, or ***service entity***, to process certain financial transactions. The AICPA SOC reports are included in the AICPA auditing standard known as ***statement on standards for attestation engagements number 18 (SSAE 18)***.

Three SOC options exist. However, only SOC 2 audits a service entity's security controls for compliance and operations. Two SOC 2 report types exist:

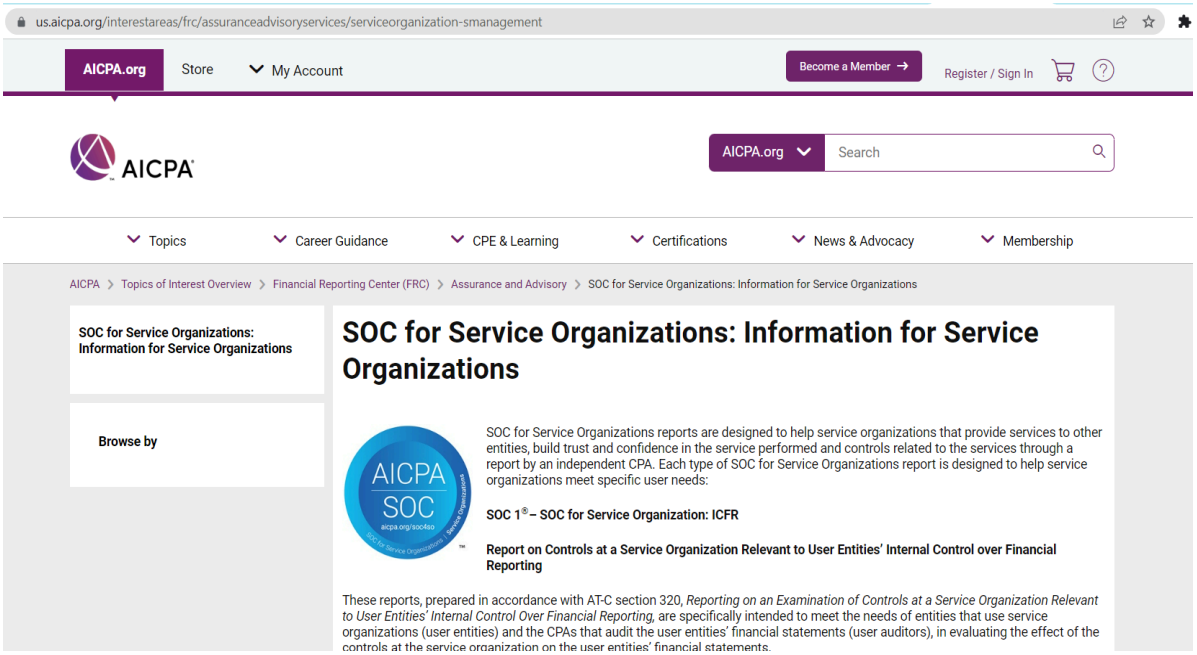
- ***SOC 2 Type 1*** is an AICPA point-in-time audit of a service entity's security controls.
- ***SOC 2 Type 2*** is an AICPA periodic, usually annual, audit of a service entity's security controls.

SOC 2 Type 1 results are intended to improve security control effectiveness whenever a subsequent SSA SOC Type 2 audit is conducted.

SOC 1 and 3.

SOC 1 and SOC 3 are the other two SOC options. Only a user entity can request SOC 1 or SOC 2. Anyone from the general public can request SOC 3. SOC 1 focuses on service entity's financial reporting. SOC 3 is a high-level report on a service entity's SOC 2 results.

Figure 14.2.3: The AICPA website.



PARTICIPATION ACTIVITY 14.2.5: System and organization control reports.

Identify which SOC option or SOC 2 type applies to each scenario.

1) A user entity requests an initial audit of a service entity's security controls.

- SOC 1
- SOC 2
- SOC 3

2) The general public requests a report on a service entity's audit results.

- SOC 1
- SOC 2
- SOC 3

3) A service entity's security controls are audited at a specific point in time.

- SOC 2 Type 1
- SOC 2 Type 2
- SOC 2 Type 3

4) A user entity requests an annual evaluation of a service entity's security control effectiveness.

- SOC 2 Type 1
- SOC 2 Type 2
- SOC 2 Type 3

14.3 Configuration guides

Platforms

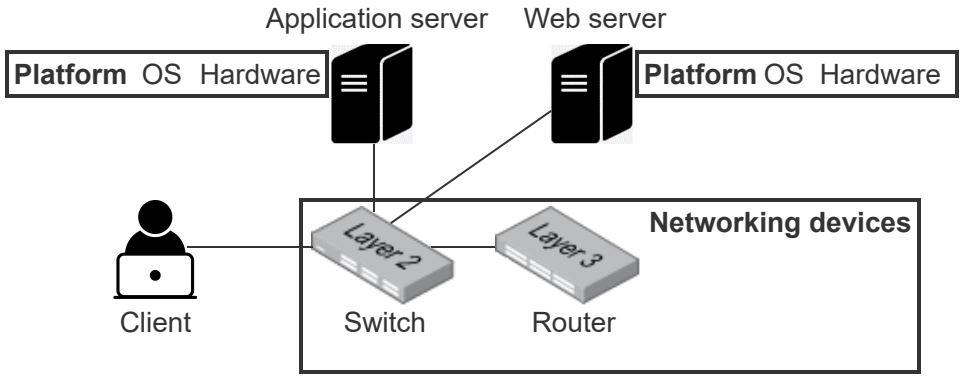
A network is an assortment of at least two connection points, or nodes, capable of sharing technology resources via a link. Various node types exist:

- A ***client*** is a node that accesses a network resource from a server, but does not share network resources with other clients.
- A ***server*** is a node that shares a network resource with a client.
- A ***networking device*** is a device used to establish network connectivity.

An ***operating system (OS)*** is software used to manage computer hardware by acting as an intermediary between a computer user, computer hardware, and computer applications. A ***platform*** is the configuration of hardware and an OS to a specific server or networking device type. Several platforms exist:

- A ***web server*** is a server platform configured to respond to a client's request for a website a server hosts.
- An ***application server*** is a server platform configured to respond to a client's request for an application a server hosts.
- A ***switch*** is a networking device or server platform serving as a central node for at least two other nodes.
- A ***router*** is a networking device server platform connecting at least two networks.

PARTICIPATION ACTIVITY 14.3.1: Nodes and platforms.



Animation content:

Static figure: Icons representing a client, a switch, a router, an application server, a web server are connected to a LAN. Both the application and web servers are labeled as a platform, which is a combination of an OS and hardware. Both the switch and the router are labeled as a networking device.
Step 1: A server's platform is configured to build a web or application server. OS and hardware labels appear from the icons representing an application server and a web server. The OS and hardware labels are combined to indicate a platform is the combination of an OS and hardware.
Step 2: A web server responds to a client request for a website by providing the website to the requesting client. A web server is built to respond to many client requests. A box representing a client request for a website travels from the client to the web server. A box representing the website the client requested travels from the web server to the client.
Step 3: An application server is similar to a web server. However, an application server hosts applications, or software, instead of websites. A box representing a client request for an application travels from the client to the application server. A box representing the application the client requested travels from the application server to the client.

Step 4: Networking devices such as switches and routers provide the connections, or links, between clients and servers. A box appears around the switch and the router to indicate both devices are examples of networking devices.

Animation captions:

1. A server's platform is configured to build a web or application server.
2. A web server responds to a client request for a website by providing the website to the requesting client. A web server is built to respond to many client requests.
3. An application server is similar to a web server. However, an application server hosts applications, or software, instead of websites.
4. Networking devices such as switches and routers provide the connections, or links, between clients and servers.

PARTICIPATION ACTIVITY 14.3.2: Nodes and platforms.

Select the node or platform described.

1) A node configured to share resources with a client.
   - Server
   - Networking device
   - Router

2) A node connecting two networks.
   - Switch
   - Router
   - Client

3) A platform used for website hosting.
   - Client
   - Application server
   - Web server

4) A server a client can request software from.
   - Application server
   - Web server
   - File server

Secure baselines

A ***secure baseline*** is a set of standardized security configurations and controls created to provide a minimum level of security for IT systems and applications within an organization. Designed to reduce vulnerabilities and enhance threat protection, secure baselines promote consistency and compliance in security practices. Managing secure baselines consists of three phases:

- Establish: Define and develop a secure baseline configuration by identifying and prioritizing security controls and configurations based on industry standards and organizational requirements. Ex: Define a set of password complexity requirements and encryption protocols as part of the baseline security configuration.
- Deploy: Deploy the secure baseline uniformly across all applicable IT systems and applications, ensuring consistent application of security controls. Ex: Install antivirus software on all company laptops according to the established security baseline.
- Maintain: Continuously monitor, update, and refine the secure baseline to adapt to evolving security threats and organizational requirements while ensuring ongoing effectiveness and compliance. Ex: Regularly update firewall rules to address new security threats and organizational changes.

Table 14.3.1: Secure baselines.

Phase	Actions	Tools/techniques	Expected outcomes
Establish	Define security settings, research best practices and industry standards	Security guidelines, policy frameworks	Comprehensive security standards established
Deploy	Configure new systems, reconfigure existing systems, automate security controls	Automation tools, configuration management software, security orchestration tools	Secure and uniform system configurations across the company, reduced security vulnerabilities
Maintain	Continuously monitor and audit systems, update security settings, ensure compliance	Monitoring tools, compliance auditing software, threat intelligence feeds	Continuous protection, compliance, and adaptation to emerging threats, improved incident response

PARTICIPATION ACTIVITY 14.3.3: Secure baselines.

1) What is the purpose of a secure baseline?

- To create vulnerabilities within IT systems
- To provide a minimum level of security for IT systems and applications
- To decrease consistency and compliance in security practices.

2) Which tools/techniques are used during the deploy phase?

- Risk assessments
- Automation tools
- Threat intelligence feeds

3) What is the main purpose of continuously monitoring and updating the secure baseline?

- To create new vulnerabilities
- To adapt to evolving security threats and organizational requirements
- To decrease compliance with security standards

4) How do threat intelligence feeds contribute to continuous protection and adaptation to emerging threats during the maintain phase?

- By decreasing system vulnerabilities
- By automating security controls
- By providing real-time information on potential security risks

©zyBooks 12/12/24 18:10 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

5) How does the distributed nature of cloud computing environments influence the establishment of secure baselines?

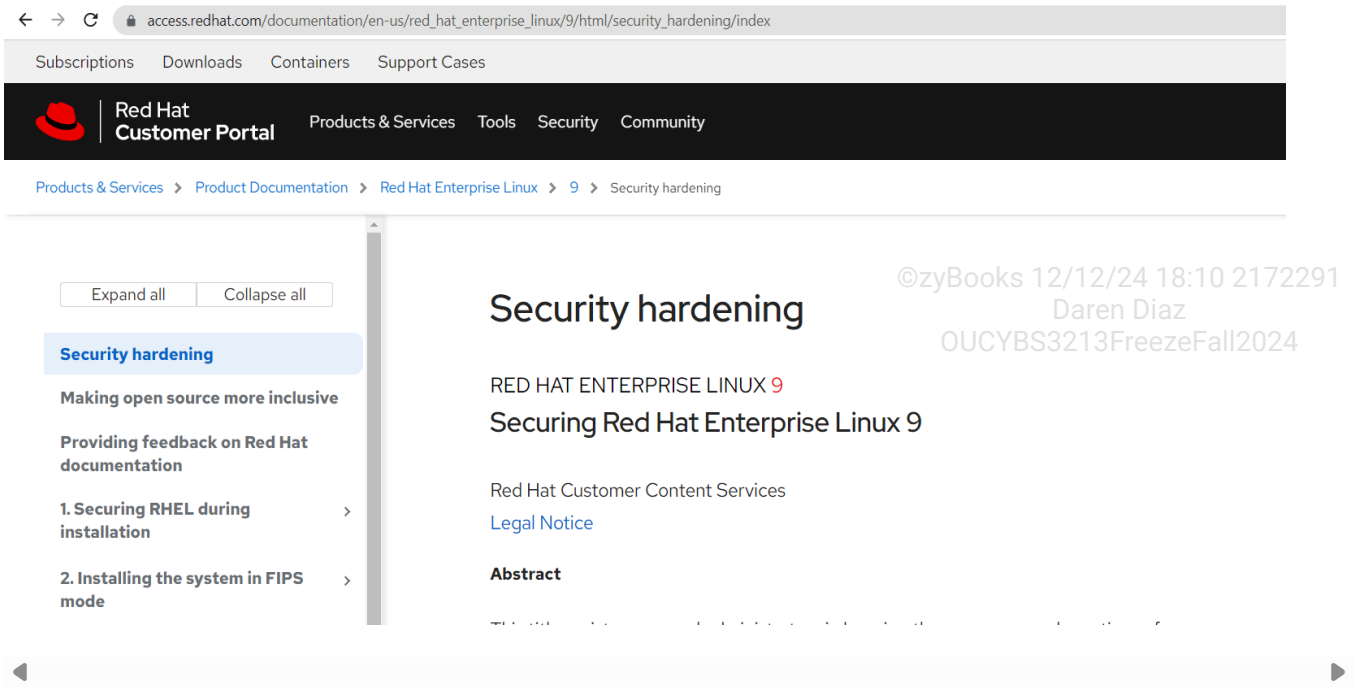
- Decreases the complexity of security settings
- Requires additional measures to ensure uniformity and consistency in security practices
- Reduces the need for continuous monitoring and updating of security settings

Platform configuration guides

A ***configuration guide*** contains vendor-specific recommendations and industry-recognized best practices for platform configuration. Recommendations and best practices vary from vendor-to-vendor and platform-to-platform. However, many configuration guides include similar configurations. Common configuration guide recommendations and best practices include:

- Utilize boot integrity features such as secure boot or measured boot.
- Implement a hardware-validated boot process via a HRoT.
- Change any default credentials to a unique username and complex password.
- Install and enable only necessary software, features, services, and ports.
- Uninstall and disable unnecessary software, features, services, and ports.
- Restrict network connectivity during installation to limit a vulnerable platform's exposure.
- Check for and apply any updates to the platform's OS and software.
- Consider enabling automatic updates to the platform's OS and software.
- Enable logging for critical events.
- Enable SSH and disable telnet if remote access is required.
- Periodically audit the platform for compliance with policies and applicable regulations.
- Physically secure the platform's hardware and enclosure.

Figure 14.3.1: The Red Hat Enterprise Linux (RHEL) Security Hardening configuration guide.



PARTICIPATION ACTIVITY 14.3.4: Platform configuration guides.

Select the configuration guide recommendation that addresses each security concern.

1) Prevent malware installation before a platform's OS is loaded.
   - ○ Physically secure the platform's hardware and enclosure.
   - ○ Utilize boot integrity features.
   - ○ Enable logging for critical events.

2) A platform's default username and password are included in a vendor's online documentation.
   - ○ Change any default credentials.
   - ○ Install and enable only necessary software.
   - ○ Install and enable only necessary features.

3) An out-of-date platform is missing a required software patch.

©zyBooks 12/12/24 18:10 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

- Enable logging for critical events.
- Uninstall and disable unnecessary software.
- Consider enabling automatic updates.

4) A new HIPAA version is released and contains new platform compliance requirements.
   - Check for and apply any updates.
   - Periodically audit the platform.
   - Enable SSH and disable telnet.

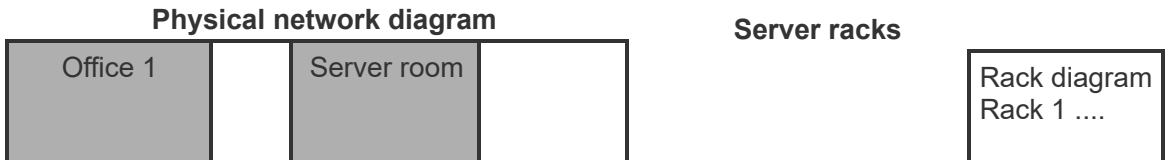
14.4 Documentation

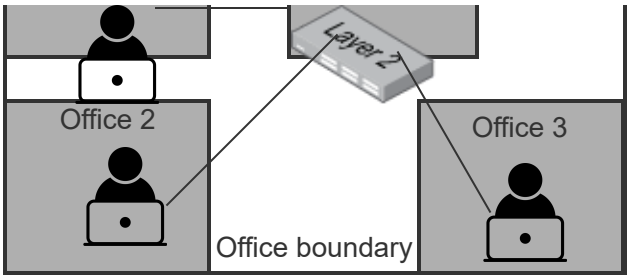
Physical network documentation

Network documentation is a collection of records documenting a network's hardware, software, and configurations. Physical network documentation types:

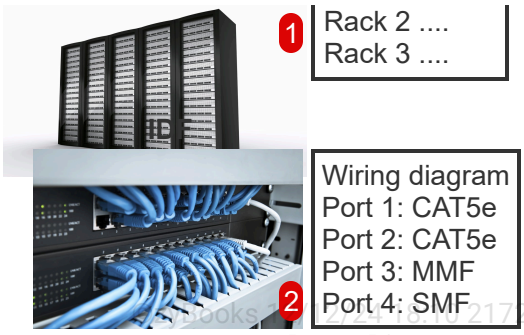
- A ***physical network diagram*** is a graphical representation of a network's physical topology.
- A ***floor plan*** is a graphical representation of a location's physical layout.
- A ***rack diagram*** is a graphical representation of the equipment in a structure used to house IT equipment known as a ***server rack***.
- A ***wiring diagram*** is a graphical representation of connections between server rack equipment, an IDF, and an MDF.
- A ***site survey report*** is the documentation generated by a site survey.

PARTICIPATION ACTIVITY 14.4.1: Physical network documentation.





Floor plan



Animation content:

Static figure: A physical network diagram, a floor plan, a server rack, and an IDF are presented.
Step 1: A physical network diagram can be overlaid on a floor plan to identify where nodes and equipment are located within a given space. A floor plan appears as a rectangle representing an office. Within the floor plan, three offices and a server room are pictured. The three offices and the server room are highlighted as physical network diagram components.
Step 2: A server rack houses IT equipment to both protect and organize equipment. A rack diagram documents the IT equipment in a server rack. A server rack photo appears from the server room. A rack diagram appears near the server rack photo and includes a list of the equipment each server rack contains.
Step 3: A wiring diagram represents IDF and MDF connections. A wiring diagram photo appears from the server room and includes a list of the cable types connected to each port.

Animation captions:

1. A physical network diagram can be overlaid on a floor plan to identify where nodes and equipment are located within a given space.
2. A server rack houses IT equipment to both protect and organize equipment. A rack diagram documents the IT equipment in a server rack.
3. A wiring diagram represents IDF and MDF connections.

Image sources:

1: Getty Images/iStockphoto

2: Getty Images/iStockphoto

PARTICIPATION ACTIVITY 14.4.2: Physical network documentation.

1) Which network documentation graphically represents a star topology?

- Physical network diagram
- Rack diagram

- Wiring diagram

2) Which network documentation graphically represents an office layout?
   - Network diagram
   - Floor plan
   - Wiring diagram

3) An organization's servers, switches, patch panels, and routers are graphically represented by which network documentation type?
   - Rack diagram
   - Network drop
   - Floor plan

4) A server rack's connections are graphically represented by which network documentation type?
   - Network diagram
   - Graphical topology
   - Wiring diagram

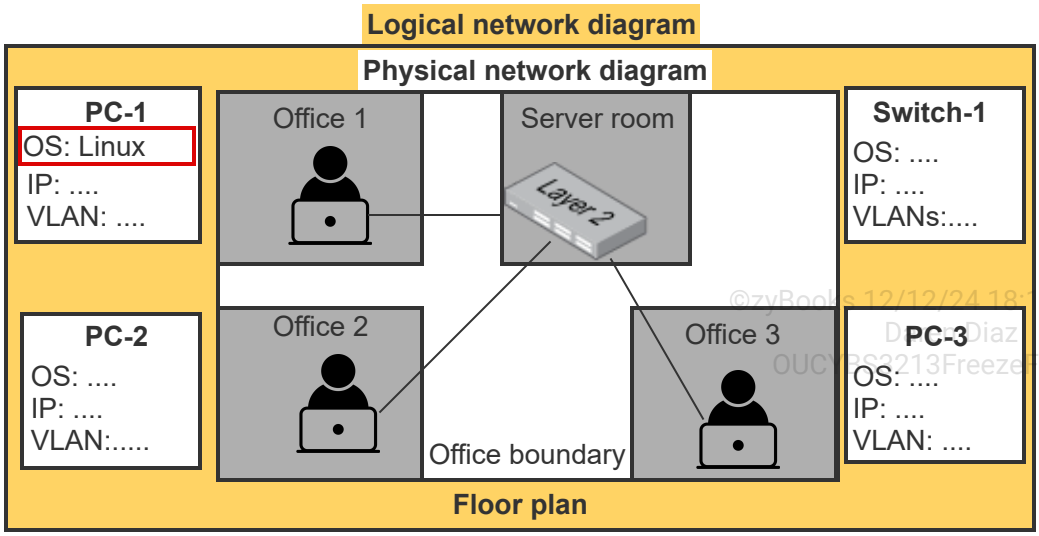
Logical network documentation

A network's configurations, or logical topology, are captured in logical network documentation. Several logical network documentation types exist:

- A ***logical network diagram*** is text-based documentation used to record a network's logical topology.
- A ***baseline configuration*** is a node's initial configuration at time of deployment.
- A ***standard naming convention*** is the use of a consistent naming scheme, or convention, for computing resources.
- An ***IP schema*** is the use of a consistent IP addressing plan, or schema, for network resources.

Some physical network documentation includes logical network documentation content. Ex: A site survey report showing the SSIDs and channel selection of a nearby WLAN.

PARTICIPATION ACTIVITY 14.4.3: Logical network documentation.



Animation content:

Static figure: A logical network diagram and a physical network diagram are displayed. The physical network diagram consists of three offices with a PC and a server room with a switch. The PCs' and switch's configurations make up the logical network diagram.
Step 1: Logical network documentation compliments physical network documentation by recording network configurations. The logical network diagram appears alongside the physical network diagram. The logical documentation for the PCs and the switch consists of each device's OS, IP address, and VLAN information.
Step 2: All nodes are deployed with a baseline configuration and any configuration changes must be recorded. Ex: Changing PC-1's OS from Windows to Linux. The OS for PC-1 changes from Windows to Linux. The logical network documentation is updated with the OS change to ensure the logical network documentation remains accurate.

Animation captions:

1. Logical network documentation compliments physical network documentation by recording network configurations.
2. All nodes are deployed with a baseline configuration and any configuration changes must be recorded. Ex: Changing PC-1's OS from Windows to Linux.

PARTICIPATION ACTIVITY 14.4.4: Logical network documentation.

1) Which documentation type identifies node configurations?

- Logical topology
- Floor plan

- Physical topology

2) What documentation records a WAP's channel section?
   - Physical network documentation
   - Logical network documentation
   - Rack diagram

3) What is a switch's initial configuration known as?
   - A full-duplex configuration.
   - A half-duplex configuration.
   - A baseline configuration.

4) Which of the following is recorded in logical network documentation?
   - A WAP's SSID
   - A WAP's location
   - A WAP's antenna type

14.5 Asset management

IT asset management

An IT asset is a hardware or software component utilized in an organization's infrastructure. ***IT asset management*** is the process of acquiring, operating, maintaining, and disposing of IT assets. Ex: A company purchases a cloud storage system, monitors system usage and performance, ensures current security controls, and securely deletes old data upon upgrading to a newer system. IT asset management allows an organization to optimize resource efficiency, enhance security controls, and achieve cost savings.

Implementing an IT asset management strategy involves maintaining up-to-date inventory records, ensuring compliance for all assets, and securely disposing of outdated technology. Recommended practices include automating inventory management when feasible, continuously reviewing and updating security controls to counter new threats, and following established protocols for data sanitization and hardware disposal.

Table 14.5.1: Asset management phases.

Phase	Description	Examples
Identification & classification	Determine asset sensitivity and value	Identify laptops with sensitive data; classify cloud storage types
Acquisition & procurement	Acquire necessary assets	Negotiate software licenses; purchase cloud storage
Inventory maintenance	Catalog and maintain asset inventory through enumeration	Track software licenses; assign ownership to servers
Security control implementation	Apply security controls based on asset sensitivity	Implement multi-factor authentication on sensitive devices; encrypt data at rest
Review & update	Update inventory and security controls	Annual security assessment; quarterly access rights reviews
Disposal & decommissioning	Securely remove assets, deleting data or destroying hardware.	Erase obsolete hard drive data; physically destroy outdated storage media

PARTICIPATION ACTIVITY 14.5.1: Asset management.

1) What is the primary goal of IT asset management?

- To reduce the number of IT staff
- To increase employee onboarding time
- To optimize resource utilization and enhance security

2) What does the identification and classification phase of asset management involve?

- Determining an asset's financial value
- Assigning employee usage schedules
- Determining security needs based on asset sensitivity

3) During the inventory maintenance phase, how does enumeration contribute to IT asset management?

- By actively scanning and documenting all network-connected devices and software
- By facilitating the office relocation process and the physical setup of IT assets
- By calculating the depreciation value of IT assets over time for financial reporting

4) Considering emerging security threats, which approach to updating security controls is most effective in IT asset management?

- Waiting for an annual review to make all necessary updates
- Implementing security updates only when new assets are purchased
- Regularly reviewing and updating security controls in response to new threats

5) What is the importance of maintaining an up-to-date and accurate IT asset inventory for disaster recovery planning?

- Not relevant to disaster recovery as assets can be easily replaced
- Enables efficient recovery by identifying critical assets and

protection requirements

- Complicates disaster recovery efforts by focusing on existing assets rather than recovery strategies

6) Considering the shift towards remote work, how should IT asset management strategies adapt to ensure security and efficiency?

- By centralizing all IT assets in corporate offices to enhance security
- By reducing the number of assets assigned to remote workers to minimize risk
- By incorporating remote access controls and secure communication protocols

IT asset disposal and decommissioning

Secure disposal and decommissioning reduces risks in the final lifecycle stage of an IT asset, protecting sensitive information beyond the asset's operational period and preventing obsolete technology from becoming a security threat. The secure disposal and decommissioning of assets includes two practices:

- Sanitization involves the thorough cleaning of data from a storage device to ensure that no recoverable information remains. Sanitization techniques vary from overwriting data to cryptographic erasure (deletion of cryptographic keys), depending on the sensitivity of the data and the future use of the device.
- Destruction involves rendering a device unusable and data irretrievable. Destruction techniques vary from shredding hard drives to pulverizing storage media. Destruction of an asset occurs when the asset is too sensitive or when sanitization cannot guarantee complete data removal.

Data retention occurs before the disposal or decommissioning of any asset in consideration of legal and regulatory requirements. Data retention ensures that any data needing preservation, according to compliance standards, is securely backed up or archived before asset disposal. Certification, when issued by a recognized authority, validates the sanitization or destruction of an asset without data leakage, confirming adherence to industry and legal standards.

Table 14.5.2: Comparison of data sanitization and data destruction.

Criteria	Data sanitization	Data destruction
Purpose	Removes data to make recovery impossible	Damages device to prevent data retrieval and use
Applicability	Devices to be reused or resold	Devices at end-of-life with highly sensitive data
Compliance	Meets data protection regulations	Enures compliance by complete elimination
Cost	Lower, due to preservation of devices	Higher, due to physical destruction of devices
Implementation techniques	Cryptographic erasure, degaussing, software-based overwriting	Shredding, pulverizing, crushing, burning

PARTICIPATION ACTIVITY 14.5.2: Asset disposal and decommissioning.

1) What is the main purpose of secure disposal and decommissioning of IT assets?
   - To increase IT asset lifespan
   - To upgrade obsolete technology
   - To reduce end-of-life IT asset risks

2) What does destruction involve in the context of IT asset disposal?
   - Transferring data to a new device
   - Recycling the device for future use
   - Making devices and data irretrievable

3) What is the role of certification in the disposal or decommissioning of IT assets?

- Upgrades the asset for future use
- Increases the resale value of the device
- Certifies standards compliance and no data leakage

4) Which of the following is a technique associated with data destruction?

- Shredding
- Cryptographic erasure
- Software-based overwriting

5) How does the decision between cryptographic erasure and physical destruction influence a decommissioned asset's data breach risk?

- Cryptographic erasure removes the risk by deleting encryption keys
- Physical destruction increases the risk by leaving recoverable data fragments
- Cryptographic erasure increases the risk by making data temporarily accessible

6) How does the concept of data retention prior to asset disposal align with minimum data retention principles mandated by privacy regulations?

- By retaining only legally required data
- By retaining as much data as preferred

- By retaining all data, regardless of sensitivity

Cloud and virtual assets

In the era of cloud computing, IT asset management extends beyond physical devices to include virtual assets like software-as-a-service (SaaS) applications and cloud storage solutions. Managing virtual assets requires a refined approach to tracking usage, optimizing costs, and ensuring data security in multi-cloud environments. The shift to cloud computing reflects the evolving nature of IT infrastructure and the growing complexity of managing resources effectively in a digital age.

14.6 Change management

IT change management

IT change management refers to a structured approach for managing modifications to an IT system, ensuring changes are controlled, efficient, and secure. The goal of IT change management is to maintain the availability, confidentiality, and integrity of IT systems throughout the change processes, thereby supporting seamless business operations and protecting organizational assets. Covering a wide range of activities, from implementing simple updates and patches to executing significant system overhauls, IT change management emphasizes communications with stakeholders and users to ensure uninterrupted transition to new hardware and/or software.

IT change management involves planning, evaluating, obtaining approval for, implementing, and reviewing changes to minimize potential disruptions, reduce risks, and enhance the stability and security of IT systems. Ex: An organization planning to update accounting software to improve features and security begins by assessing the change's impact and obtaining the necessary approvals. The update is scheduled for off-hours to minimize disruptions. Following implementation, functionality tests are conducted, documentation is updated, and users are trained on the new features, ensuring a seamless transition to the improved accounting software.

Table 14.6.1: IT change management phases.

Phase	Description	Example
1. Request	Initiate the change process by completing required documentation	Request an update for a server to improve performance
2. Evaluation	Assess the change to minimize risks and impacts	Evaluate the server update impact on other systems and applications
3. Planning	Determine the change type and priority, schedule roll-out, and develop contingency plans	Schedule the server update during a maintenance window with a backout plan
4. Approval	Secure approvals from stakeholders to prevent downtime and change failures	Obtain necessary approvals from IT manager and server owner for the update
5. Implementation	Execute the planned change	Update the server during scheduled maintenance window
6. Review	Evaluate the change post-implementation, classifying the change as successful, failed, or incomplete	Review the server's post-implementation performance to identify deviations from expected results

PARTICIPATION ACTIVITY 14.6.1: Change management.

1) What is the primary goal of change management in an IT system?
   - To reduce the IT budget
   - To enhance performance and security
   - To increase the speed of system updates

2) Why is obtaining approvals an essential part of change management?
   - Allows IT staff to bypass standard procedures

- Ensures all changes align with organizational goals
- Removes the need for post-implementation review

3) What is the purpose of conducting functionality tests after implementing a change?

- To comply with international laws
- To reduce the organization's reliance on IT
- To ensure changes achieve objectives seamlessly

4) How does change management enhance an IT system?

- By eliminating all IT policies
- By increasing system vulnerabilities
- By reducing potential disruptions and risks

5) How does the review of changes post-implementation contribute to the overall IT system's stability and security?

- By identifying unintended consequences
- By offering a chance to reverse all changes
- By providing a checklist of completed tasks

6) In the context of GDPR compliance, how does change management ensure that an organization's IT changes comply with privacy regulations?

- By randomly auditing changes after implementation

- By continuous education and training on GDPR requirements
- By assuming compliance with previous regulations is sufficient

7) When evaluating a change in a cloud environment, what unique factor must be considered?

- The impact on cloud resource scalability
- The brand of server hardware being used
- The compatibility with non-cloud applications

Technical implications and documentation

Change management includes the application of controls for mitigating technical risks to system security throughout change processes. To minimize risk exposure during critical updates, temporary restrictions on specific activities may be applied. Ex: Allow/deny lists control access to resources, ensuring only authorized entities can interact with modified systems. Planning for changes affecting system availability includes an analysis of the potential downtime impact and the need to restart services and applications. Additionally, managing updates in legacy applications addresses system dependencies to mitigate unexpected security vulnerabilities and prevent compliance issues. Ex: Updating a bank's outdated transaction system necessitates a phased approach to prevent security flaws and address compliance requirements, thereby ensuring seamless integration with interconnected systems.

Documentation improves security within change management processes by ensuring that all changes are recorded, tracked, and accessible. Ex: Regular updates to network diagrams improve the clarity of IT infrastructure layout, facilitating the identification of potential security vulnerabilities. Similarly, updating policies/procedures ensures that changes are aligned with organizational security standards and compliance requirements. Lastly, version control helps manage changes to documents, code, and configurations, providing a history of modifications used for auditing, troubleshooting, and rolling back changes if necessary. Ex: Using a version control system such as Git enables quick rollback of faulty updates to network configuration scripts.

Table 14.6.2: Control measures in IT change management.

Control	Description	Example

Allow/deny lists	Rules for permitting/denying access to resources	Allow vendor IP access during software update
Restricted activities	Temporary limitations on certain functions during updates	Disable user account creation during critical OS updates
Downtime/restart planning	Assessing and scheduling system unavailability	Schedule database maintenance during off-peak hours
Legacy application management	Considerations for systems using older technologies	Assess legacy payroll application security before integration with new system
Dependency mapping	Understanding how systems are interconnected	Identify web services' dependencies on database updates

PARTICIPATION ACTIVITY 14.6.2: Technical implications and documentation.

1) What is the primary purpose of using allow/deny lists in change management?
   - To document changes
   - To track version history
   - To control resource access

2) How do legacy applications impact change management?
   - Simplify dependency management
   - Remove the need for documentation updates
   - May result in introducing security vulnerabilities

3) Why are service and application restarts necessary?

- To finalize the change process
- To ensure changes take effect properly
- To comply with version control policies

4) Why are restricted activities enforced during change management?

- Minimize risk exposure
- Avoid updating policies
- Increase system downtime

5) Why is updating network diagrams important in change management?

- To facilitate version control
- To enforce restricted activities
- To clarity IT infrastructure layout

6) How does version control contribute to effective change management?

- Tracks changes history
- Enforces allow/deny lists
- Reduces service restarts

7) How do dependencies affect change management in a cloud-native application?

- Dependencies have no impact on cloud-native applications
- Essential for uninterrupted integration and service continuity
- Dependencies are automatically managed by cloud providers

Automation in change management

Integrating automation into change management processes enhances the security, efficiency, and overall effectiveness of IT operations. Automated solutions streamline the submission of change requests, enable systematic tracking of approvals, and facilitate the timely scheduling of updates or patches, minimizing operational interruptions.

Automation reduces the incidence of error, ensures compliance with organizational policies, and decreases system downtime. Additionally, automated tools generate detailed audit trails for every change, which optimizes documentation practices and simplifies the process of reviewing or rolling back changes as required.

14.7 Plans

System development lifecycle

A ***system lifecycle*** is a system's operational lifespan from initiation to ***end of life (EOL)*** or ***end of service life (EOSL)***. The ***system development lifecycle (system SDLC)*** is a conceptual model describing system development phases from initiation through maintenance. The exact number of system SDLC phases varies depending on the source. However, seven system SDLC phases exist:

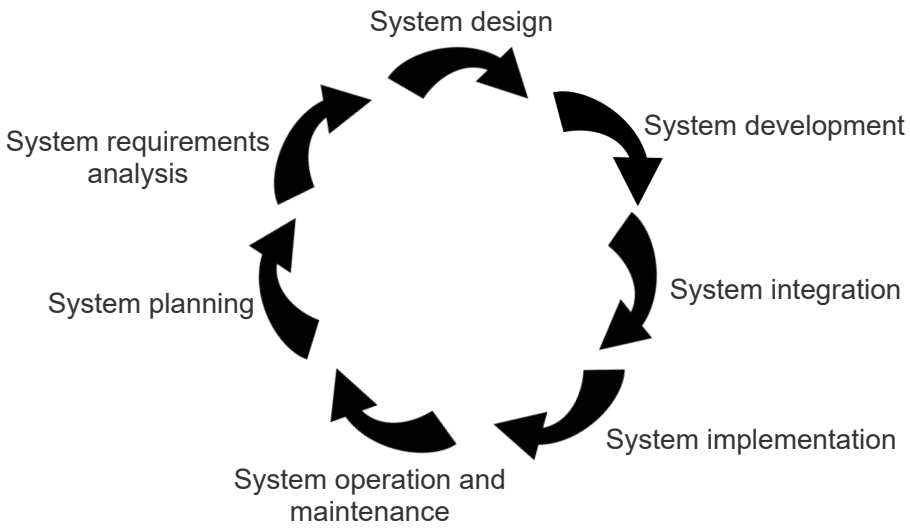
1. System planning
2. System requirements analysis
3. System design
4. System development
5. System integration
6. System implementation
7. System operation and maintenance

The software development life cycle (software SDLC)

The software development lifecycle (software SDLC) is similar to the system development lifecycle (system SDLC), but focuses specifically on software development. Ex: The software SDLC is used to build a database application installed on a database server, while the system SDLC covers the setup and configuration of the database server and other necessary system components. Both lifecycles generally

include phases such as planning, analysis, design, development, testing, deployment, and maintenance.

PARTICIPATION ACTIVITY 14.7.1: System SDLC phases.



Animation content:

Static figure: Seven arrows representing the system SDLC's seven stages are arranged in a circle.
Step 1: System development begins with a planning or initiation phase to plan a project intended to solve a problem or pursue an opportunity. The arrow representing system planning appears.
Step 2: The second system SDLC phase involves system and requirements analysis to ensure the proposed system will satisfy business and/or user requirements. The arrow representing system requirements analysis appears.
Step 3: System design produces a configuration for system development. A developed system is integrated into the desired environment for testing purposes. The arrows representing system development and system integration appear.
Step 4: System implementation deploys the system into the desired environment for all users. The new system may replace an old system during system implementation. The arrow representing system implementation appears.
Step 5: The system is used, maintained, and monitored during the operations and maintenance phase. The system will eventually be retired during a future system SDLC process. The arrow representing system operation and maintenance appears.

Animation captions:

1. System development begins with a planning or initiation phase to plan a project intended to solve a problem or pursue an opportunity.
2. The second system SDLC phase involves system and requirements analysis to ensure the proposed system will satisfy business and/or user requirements.
3. System design produces a configuration for system development. A developed system is integrated into the desired environment for testing purposes.
4. System implementation deploys the system into the desired environment for all users. The new system may replace an old system during system implementation.
5. The system is used, maintained, and monitored during the operations and maintenance phase. The system will eventually be retired during a future system SDLC process.

PARTICIPATION ACTIVITY 14.7.2: System lifecycle.

1) Which conceptual model describes system development phases?
   - DoD
   - OSI
   - System SDLC

2) Which system SDLC phase produces a system users can test prior to system integration?
   - System design
   - System development
   - System requirements analysis

3) Which system SDLC phase does performance monitoring belong to?
   - System integration
   - System operation and maintenance
   - System planning

Business continuity

Business continuity (BC) is an organization's ability to remain functional during a disaster or an incident. Two events impact BC:

- A ***disaster*** is an environmental, accidental, or intentional catastrophic event.
- An ***incident*** is an accidental or intentional security-related event.

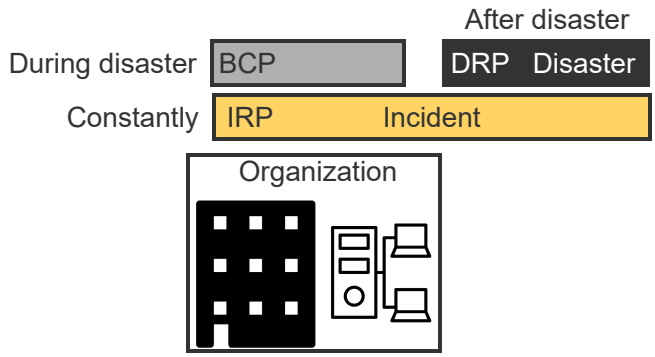
BC relies on two abilities:

- ***Disaster recovery (DR)*** is an organization's ability to return to normal operations after a disaster.
- ***Incident response (IR)*** is an organization's ability to recognize and respond to an incident.

Three plans enable an organization to respond to a disaster or an incident:

- A ***business continuity plan (BCP)***, or ***continuity of operations planning (COOP)***, is a set of processes an organization follows to maintain BC during a disaster or incident.
- A ***disaster recovery plan (DRP)*** is a set of processes an organization follows to return to normal operations after a disaster.
- An ***incident response plan (IRP)*** is a set of processes an organization follows to recognize, respond, and recover from an incident.

PARTICIPATION ACTIVITY 14.7.3: BC.



Animation content:

Static figure: An organization's building and computing resources are displayed. A BCP, an IRP, and a DRP are displayed with different labels: constantly, during disaster, and after disaster.
Step 1: A disaster forces the use of a BCP. An incident forces the use of an IRP. A disaster and an incident impact the organization. A BCP is used for the disaster while the disaster is occurring. The IRP is used for the incident.
Step 2: A BCP remains in effect until a disaster subsides. A DRP is used after a disaster subsides. The disaster subsides and the DRP assumes control over the BCP.
Step 3: An IRP is used before, during, and after an incident since incident recognition is a constant process. The IRP is applied to the incident throughout the incident's lifecycle.

Animation captions:

1. A disaster forces the use of a BCP. An incident forces the use of an IRP.
2. A BCP remains in effect until a disaster subsides. A DRP is used after a disaster subsides.

3. An IRP is used before, during, and after an incident since incident recognition is a constant process.

PARTICIPATION ACTIVITY 14.7.4: BC.

1) Which ability does an organization strive to maintain during a disaster?
   - Disaster recovery
   - Business continuity
   - Performance monitoring

2) Which ability does an organization strive to demonstrate after a disaster?
   - Disaster recovery
   - Redundancy
   - Speed

3) Which network plan is used during a disaster?
   - BCP
   - DRP
   - Change management

4) Which network plan is used after a disaster?
   - BCP
   - DRP
   - SDLC

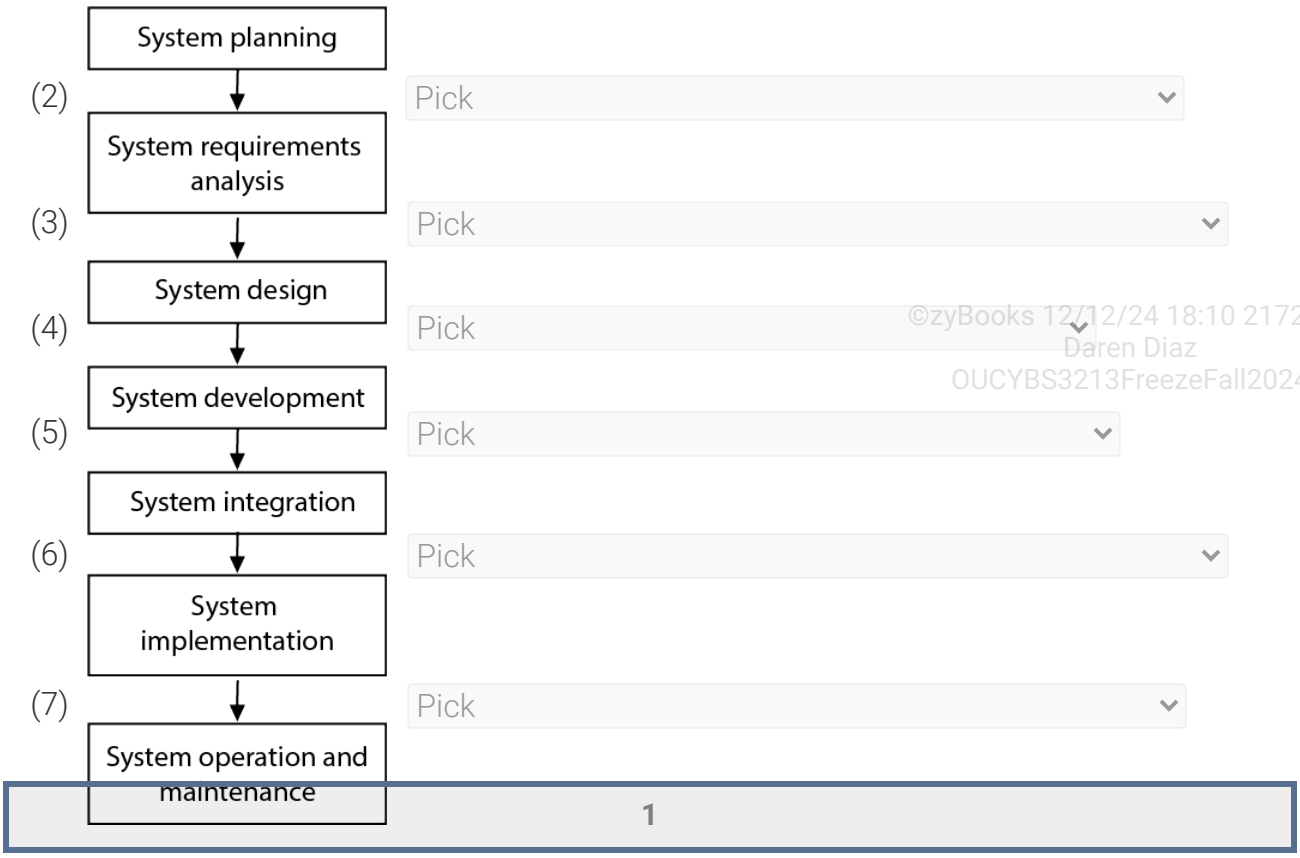
CHALLENGE ACTIVITY 14.7.1: Plans.

581480.4344582.qx3zqy7

Start

Company E needs to track employee work time. Select the activity performed in each step of system SDLC.

(1) Pick



14.8 Policies

Data classification

Data classification is a process for categorizing data based on the adverse effect of unauthorized disclosure. ***NIST special publication (SP) 800-53*** is a collection of security control standards and guidelines developed by the U.S. Department of Commerce and the NIST. Many organizations classify data using the three impact levels defined in NIST SP 800-53B, a companion publication to NIST SP 800-53:

- A ***low impact level*** is a data classification level indicating unauthorized disclosure causes a limited adverse effect.
- A ***moderate impact level*** is a data classification level indicating unauthorized disclosure causes a serious adverse effect.
- A ***high impact level*** is a data classification level indicating unauthorized disclosure causes a catastrophic adverse effect.

Data classification determines data governance and retention processes:

- ***Data governance*** is a collection of processes detailing how data is collected and accessed during the data's life cycle.
- ***Data retention*** is a collection of processes detailing how data is stored for a specified amount of time.

PARTICIPATION ACTIVITY 14.8.1: Data classification.

Data classification

Low impact	Moderate impact	High impact
Public job postings Public-facing website content Public contact information Press releases	Employment applications Non-public contact information Non-public policies and reports Non-public financial data	Patient or employee health data Social security numbers Payment card numbers Financial account numbers

Animation content:

The three data classification levels are low, moderate, and high impact.

Animation captions:

1. The impact of unauthorized disclosure of data is used to categorize data as low, moderate, or high impact.
2. A low impact classification indicates unauthorized disclosure causes a limited adverse effect. Low impact data includes public domain information.
3. A moderate impact classification indicates unauthorized disclosure causes a serious adverse effect. Moderate impact data includes internal organizational information.
4. A high impact classification indicates unauthorized disclosure causes a catastrophic adverse effect. High impact data includes sensitive internal organizational and personal information.

PARTICIPATION ACTIVITY 14.8.2: Data classification.

Select the data classification level for each data example.

1) An organization's customer service telephone number.
   - ○ Low impact

- Moderate impact
- High impact

2) A press release for a new smartphone.
   - Low impact
   - Moderate impact
   - High impact

3) The human resources manager's personal cellular phone number.
   - Low impact
   - Moderate impact
   - High impact

4) An organization's business checking account number.
   - Low impact
   - Moderate impact
   - High impact

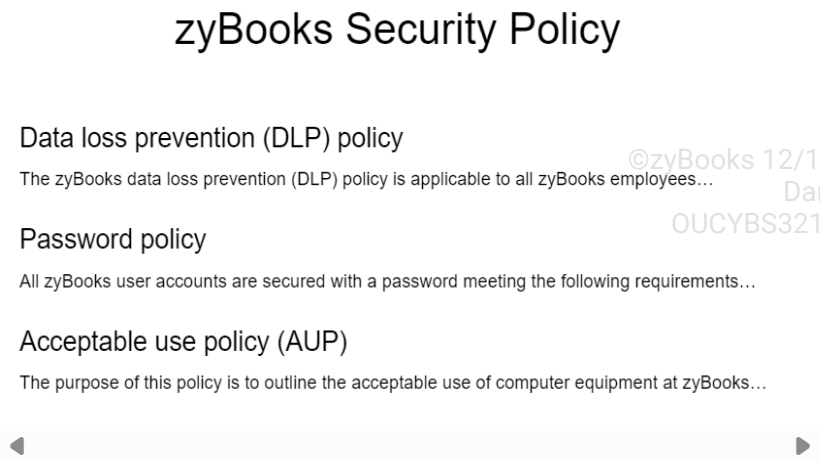
Security policies

Security focuses on the unauthorized disclosure of sensitive data, or ***data loss prevention (DLP)***. Several security-related policies support DLP:

- A ***DLP policy*** is a policy detailing DLP efforts.
- A ***password policy*** is a policy detailing password complexity and password expiration requirements known as password aging.
- An ***acceptable use policy (AUP)*** is a policy detailing the valid, or acceptable, use of network resources.
- A ***BYOD policy*** is a policy detailing if and how BYOD connects to network resources.
- A ***remote access policy (RAP)*** is a policy detailing if and how network resources are remotely accessed.
- An ***onboarding policy*** is a policy detailing how a new employee accesses network resources.
- An ***offboarding policy*** is a policy detailing the removal of network resource access for a resigning or resigned employee.
- A ***retention policy*** is a policy detailing archiving processes for data and sensitive documentation.
- A ***credential policy*** is a policy detailing processes for identity and authentication, or ***credentials***, management.

An organization's collection of security-related policies is collectively referred to as a ***security policy***.

Figure 14.8.1: A security policy is a collection of security-related policies.



PARTICIPATION ACTIVITY 14.8.3: Security policies.

Select the security-related policy described.

1) A policy stating a password must include at least one number and one special character.
   - DLP policy
   - Password policy
   - Onboarding policy

2) A policy stating an organization's computer cannot be used for online gaming.
   - RAP
   - BYOD policy
   - AUP

3) Details for providing access to network resources for newly hired employees.
   - Onboarding policy
   - Offboarding policy
   - DLP policy

4) Details for removing access to network resources for former employees.

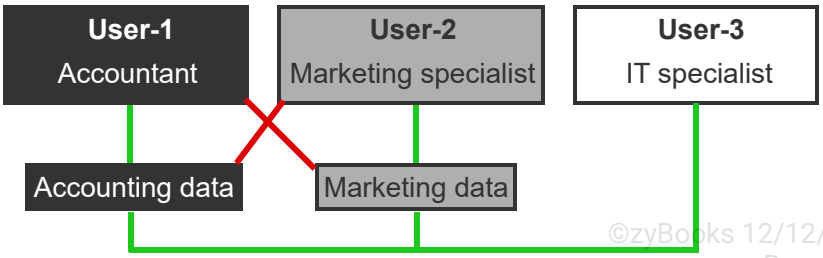
- Onboarding policy
- Offboarding policy
- BYOD policy

Personnel policies

A personnel policy details various security-related procedures and employee expectations. Personnel policy examples:

- A ***background check policy*** is a policy detailing the use of applicant or employee background checks.
- A ***job rotation policy*** is a policy detailing the temporary or permanent reassignment of an employee to expose security or procedural issues.
- A ***mandatory vacation policy*** is a policy detailing mandatory use of paid time off to expose security or procedural issues.
- A ***separation of duties policy*** is a policy detailing how critical functions are divided among multiple personnel to maintain procedural integrity.
- A ***least privilege policy*** is a policy detailing how an organization implements the principle of least privilege.
- A ***clean desk policy*** is a policy detailing how an employee must maintain a clean working area to prevent unauthorized disclosure of sensitive documentation.
- A ***social media policy*** is a policy detailing the authorized use of social media for business-related purposes.

PARTICIPATION ACTIVITY 14.8.4: Least privilege policy.



Animation content:

Static figure: Three boxes represent three users within an organization. Each user works in a different department and receives different access rights based on the organization's least privilege policy.
Step 1: Three users work in different departments within the same organization. Least privilege

determines each user's data access rights. Three boxes for user 1, 2, and 3 appear. Two boxes for accounting data and marketing data appear.
Step 2: User-1 is an accountant and requires access rights to accounting data. A green line connects user-1 to the accounting data.
Step 3: User-2 is a marketing specialist and requires access rights to marketing data. A green line connects user-2 to the marketing data.
Step 4: Least privilege determines user-1's job does not require access to marketing data and user-2's job does not require access to accounting data. A red line appears between user-1 and the marketing data to show user-1 is not authorized to access the marketing data. A red line appears between user-2 and the accounting data to show user-2 is not authorized to access the accounting data.
Step 5: User-3 is an IT specialist and requires access rights to all data. However, additional security controls limit how the IT specialist can use data access rights. A green line connects user-3 to both the accounting and marketing data.

Animation captions:

1. Three users work in different departments within the same organization. A least privilege policy determines each user's data access rights.
2. User-1 is an accountant and requires access rights to accounting data.
3. User-2 is a marketing specialist and requires access rights to marketing data.
4. A least privilege policy determines user-1's job does not require access to marketing data and user-2's job does not require access to accounting data.
5. User-3 is an IT specialist and requires access rights to all data. However, additional security controls limit how the IT specialist can use data access rights.

PARTICIPATION ACTIVITY 14.8.5: Personnel policies.

1) Which personnel policy is used to rotate employee responsibilities within the organization?
   - Background check policy
   - Job rotation policy
   - NDA

2) Which personnel policy can uncover a security issue by forcing an employee to use paid time off?
   - Job rotation policy
   - SLA
   - Mandatory vacation policy

3) Which personnel policy ensures sensitive documentation is not left unattended in a work space?

- Clean desk policy
- Data classification policy
- AUP

4) Which personnel policy controls the organizational information an employee can disclose on LinkedIn?

- Data classification policy
- Social media policy
- Background check policy

Policy governance, monitoring, and revision

An organization's policies are created and governed by authoritative bodies. A private, non-governmental organization may create specific committees that report to high-level boards. The boards dictate overall directives, and the committees create policy based on those directives. In contrast, a governmental organization is often dictated by legislation and politics.

An organization may employ centralized or decentralized governance. In a centralized governance structure, ultimate decision-making authority resides with a central body. A decentralized governance structure spreads decision-making across the organization, with decisions often being made by employees close to the related work.

Policies are created to support the goal of information security: ensuring the confidentiality, integrity, and availability of an organization's data. Those policies must be monitored and revised in response to emerging technologies, new threats, or additional legal requirements. Ex: Requiring two-factor authentication when the technology was integrated into Microsoft Active Directory.

CHALLENGE ACTIVITY 14.8.1: Policies.

Start

Select all statements that could be included in an acceptable use policy.

- [ ] Retain daily backups for 7 days
- [ ] Minimum password length is 8 characters
- [ ] Passwords must contain at least 3 special characters
- [ ] Company phones are only to be used for business-related communications

1

Check Try again

14.9 Personnel training

Training for non-IT personnel

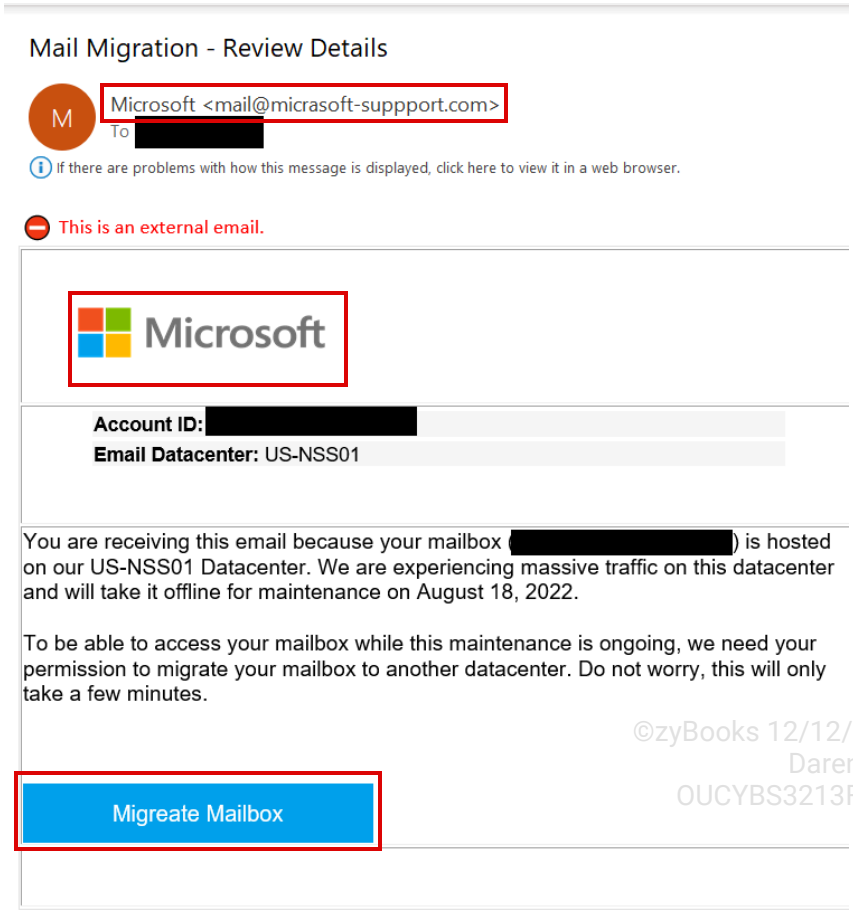
Personnel training is a vital security procedure because personnel are both security's first line of defense and security's most exploitable component. Personnel are broadly categorized as IT personnel or non-IT personnel. Personnel can be further classified by job function and department. Ex: A non-IT human resources manager.

All personnel require training. However, non-IT personnel usually require more security awareness training than IT personnel. Gamified computer-based training is a commonly used non-IT personnel training delivery method. ***Gamification*** is a training delivery technique where game-like elements like points and badges are used to encourage engagement. ***Computer-based training (CBT)*** is any type of pre-recorded self-paced training delivered remotely via a computer or similar device. CBT is an efficient training delivery method for an entire organization.

Instructor-led training is another non-IT personnel training delivery method. ***Instructor-led training (ILT)*** is any type of live training delivered remotely or in-person by an instructor. ILT is an effective training delivery method for a small personnel group.

A phishing campaign is a common training scenario. A ***phishing campaign***, or ***phishing simulation***, is a simulated phishing attack an organization conducts where the results are used to improve personnel training. A gamified phishing campaign can award points or badges to the department with the least amount of phishing victims.

PARTICIPATION ACTIVITY 14.9.1: Phishing campaign.



A phishing campaign is intended to be formative rather than punitive. Campaign results identify a need for more or more effective non-IT personnel training.

Animation content:

Static figure: A phishing email example is shown with various sections highlighted.
Step 1: The destination antenna rarely receives all the electrical power. The Microsoft logo is included near the beginning of the phishing email. The logo is highlighted to show how a phishing email appears to be legitimate.
Step 2: The sender address is from the micrasoft-support.com domain instead of microsoft-support.com or the organization's domain. The email's sender information is highlighted to show the sender's name is Microsoft. However, the sender's email address is mail at micrasoft-support.com. The micrasoft-support.com contains a misspelling and is also not the official microsoft.com domain.
Step 3: Phishing attempts often include misspelled words and links to unsafe websites. The clickable box within the phishing email misspelled migrate and directs a user to a malicious domain.

Animation captions:

1. A phishing email appears to be from the organization itself or a service the organization uses. Ex: An email from Microsoft Office 365.
2. The sender address is from the micrasoft-support.com domain instead of microsoft-support.com or the organization's domain.
3. Phishing attempts often include misspelled words and links to unsafe websites.

PARTICIPATION ACTIVITY 14.9.2: Training for non-IT personnel.

1) Who in an organization requires security awareness training?
   - Non-IT personnel
   - IT personnel
   - All personnel

2) Which training delivery technique adds a competitive element to the training content?
   - Gamification
   - ILT
   - CBT

3) Which training delivery method can efficiently train an entire organization?
   - Gamification
   - ILT
   - CBT

4) Which training scenario attempts to obtain sensitive information from an entire organization?

- Spear phishing campaign
- Whaling campaign
- Phishing campaign

Training for IT personnel

Training for IT personnel is usually more technical than training for non-IT personnel. An organization's use of diverse training techniques improves training effectiveness. Common IT personnel training examples include role-based training and capture the flag training.

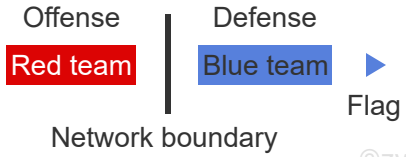
Role-based training (RBT) is a training exercise where individuals assume different organizational roles and each individual performs each role's responsibilities. An individual may assume their actual role or rotate among different roles to gain experience with different responsibilities.

Capture the flag (CTF) is a training exercise where a digital resource represents a flag that must be captured by some competitors and protected by other competitors. A common CTF example is known as red team versus blue team.

- Red team represents the offensive attackers in a cyber security exercise.
- Blue team represents the defensive security team in a cyber security exercise.

Some CTF exercises include a purple team. A purple team consists of red and blue team members to improve a blue team's defense.

PARTICIPATION ACTIVITY | 14.9.3: CTF.



Animation content:

Static figure: Red and blue text boxes represent the offense (red team) and the defense (blue team) during a CTF training exercise. The two teams are separated by a network boundary and a blue triangle represents the blue team's flag.
Step 1: An offense (red team) attempts to capture a defense's (blue team) during a CTF training exercise. The red team, blue team, and blue team's flag appear.

Step 2: The red team's goal is to penetrate the blue team's defenses to capture the blue team's flag. A text box labels the red team as the offense in a CTF training exercise. A thick line representing a network boundary appears in between the red and blue teams.
Step 3: The blue team's goal is to prevent the red team from penetrating the blue team's defenses and capturing the flag. A text box labels the blue team as the defense in a CTF training exercise.

Animation captions:

1. An offense (red team) attempts to capture a defense's (blue team) flag during a CTF training exercise.
2. The red team's goal is to penetrate the blue team's defenses to capture the blue team's flag.
3. The blue team's goal is to prevent the red team from penetrating the blue team's defenses and capturing the flag.

PARTICIPATION ACTIVITY 14.9.4: Training for IT personnel.

1) Which training type requires an employee to assume a role and perform a role's responsibilities?
   - ILT
   - CBT
   - RBT

2) Which training type consists of teams attempting to capture the other team's flag?
   - CTF
   - RSF
   - CSF

3) Which team portrays the attackers in a CTF training exercise?
   - Red team
   - Blue team
   - Purple team

4) Which team portrays the defenders in a CTF training exercise?
   - Red team
   - Blue team

- Purple team

14.10 Security awareness practices

Security awareness

Security awareness practices refer to the systematic efforts undertaken by organizations to educate and empower employees to recognize, understand, and appropriately respond to various security threats. Security awareness practices encompass a range of educational initiatives, training programs, policies, and procedures designed to cultivate a culture of security awareness among employees. The goal of security awareness practices is to teach individuals the knowledge, skills, and behaviors necessary to effectively mitigate risks, protect sensitive information, and contribute to the organization's overall security posture. Ex: A monthly security awareness newsletter that highlights recent security incidents, provides safety tips, and reminds employees of the organization's security policies.

Phishing involves manipulating individuals into sharing sensitive information through fraudulent emails or messages. A ***phishing campaign*** is an organized attempt to distribute fraudulent communications on a large scale, typically impersonating reputable entities to trick individuals into revealing sensitive credentials. Given the significant threat phishing campaigns pose to organizations, training on recognizing and responding to phishing is a central component of most security awareness programs. Ex: After undergoing awareness training on phishing, an employee identifies a suspicious email requesting bank verification, avoids clicking the embedded link, and promptly notifies the security team.

Table 14.10.1: Security awareness program components.

Component	Description	Examples
Educational initiatives	Programs designed to teach employees about recognizing and mitigating security threats	Workshops, e-Learning courses
Training programs	Targeted programs that develop specific security skills	Phishing simulation exercises
Policies and procedures	Established guidelines for managing and securing information	Data protection policies, incident response plans

Awareness culture	Efforts to integrate security awareness within the organizational culture	Monthly security newsletters, security awareness days

PARTICIPATION ACTIVITY 14.10.1: Security awareness.

1) What is the primary goal of security awareness practices?
   - To increase the organization's sales
   - To limit employee access to the internet
   - To improve employee skills in threat mitigation

2) What is a characteristic of a phishing campaign?
   - Always targets specific, high-profile individuals only
   - Large-scale distribution of deceptive communications
   - A spontaneous, unorganized effort with minimal impact

3) Why are phishing simulations important in security awareness practices?
   - Assist IT staff in recognizing threats
   - Serve as a punishment for employees who fail to detect phishing attempts
   - Offer employees hands-on experience in identifying and responding to phishing

©zyBooks 12/12/24 18:10 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

4) Which outcome indicates the success of a security awareness program?

- Decreased incident response times
- Increased number of security breaches
- Less frequent updates to security policies

5) In the context of cloud computing, what role does security awareness play in protecting against data breaches?
   - Only relevant for IT staff, not for regular users of cloud services
   - Minimal, since cloud providers are solely responsible for data security
   - Significant, as educated users are better prepared to use cloud services securely

Anomalous behavior recognition

Security awareness practices aim to improve employees' ability to identify and respond to anomalous behavior. Anomalous behavior exists in various forms:

- Risky - Recognizing actions or patterns that pose a potential risk to the security of the network or systems. Ex: Accessing sensitive information without proper authorization or attempting to bypass security measures.
- Unexpected - Detecting actions or events that deviate from normal operations. Ex: Unusual login times, access from unfamiliar locations, or exhibiting abnormal user behavior.
- Unintentional - Identifying unintentional actions or mistakes made by legitimate users. Ex: Accidental deletion of critical files or misconfiguration of security settings.

An integral part of security awareness practices is situational awareness, which prepares employees with the knowledge and alertness needed to detect and react to anomalous behavior that may indicate a security threat. By improving employees' ability to recognize anomalous behavior, employees can help mitigate potential security threats and improve the organization's security posture.

Table 14.10.2: Overview of anomalous behavior recognition training.

Type of behavior	Awareness topics	Behavioral change goals
Risky	Applying access controls and preventing unauthorized access	Improve data protection and ensure protocol adherence
Unexpected	Adopting security best practices for authentication and suspicious activity reporting	Enhance anomaly detection and reporting, and foster security awareness culture
Unintentional	Effective data management, precise configuration settings, and conducting regular audits	Improve data handling and system configuration accuracy

PARTICIPATION ACTIVITY 14.10.2: Anomalous behavior recognition.

Select the anomalous behavior form in each scenario.

1) Accessing company data from an unsecured public Wi-Fi network
   - Risky
   - Unexpected
   - Unintentional

2) Installing software without prior approval from the IT department
   - Risky
   - Unexpected
   - Unintentional

3) Discovering a server configuration that allows unauthorized users to access restricted data
   - Risky
   - Unexpected
   - Unintentional

4) Accidentally downloading a virus that looked like a software update

- Risky
- Unexpected
- Unintentional

5) Forgetting to log out of a shared computer in the company's public area

- Risky
- Unexpected
- Unintentional

User guidance and training

User guidance and training focus on the human element of security, aiming to turn employees from potential vulnerabilities into proactive participants in threat defense. Such an approach not only mitigates risks but also develops a culture of security awareness throughout an organization. Ex: Educating employees on how to securely manage and promptly dispose of sensitive documents once no longer necessary, actively ensuring compliance with data protection regulations.

Security training covers topics such as creating and managing strong passwords, identifying insider threats, and safely using removable media. Maintaining operational security and adapting to the unique challenges of hybrid or remote work environments are often part of targeted training programs. Such programs are designed to enhance employees' ability to operate securely from any location, focusing on secure home networking practices and the effective use of VPNs to safely handle sensitive information when working outside the company premises. Ex: Training employees on securing physical devices in remote locations, including the use of privacy screens and secure Wi-Fi connections.

Table 14.10.3: Security training categories.

Training category	Description	Examples
Insider threat	Training on identifying and mitigating internal risks	Recognizing suspicious behavior, understanding reporting protocols
Password management	Guidelines for robust password security	Creating strong passwords, avoiding password sharing, implementing regular updates

Removable media and cables	Best practices for handling and securing physical data carriers	Secure usage and storage of USB drives, ensuring safe connections for network devices
Operational security	Strategies to uphold data integrity and security	Implementing data encryption, secure document disposal, conducting regular security audits
Hybrid/remote work environments	Security measures for off-site work arrangements	Securing home networks, utilizing VPNs, protecting devices in public areas

PARTICIPATION ACTIVITY 14.10.3: User guidance and training.

1) What is the primary goal of user guidance and training in an organization's security strategy?
   - To focus solely on technical security measures
   - To turn employees into active participants in threat defense
   - To remove the human element from security considerations

2) What is emphasized in training about removable media and cables?
   - Unlimited access to USB ports
   - Encouraging the use of personal USB devices
   - Safe handling and secure storage of USB drives

3) Which of the following best practices is recommended for password management?
   - Sharing passwords with trusted colleagues

- Strong password creation and regular updates
- Using the same password for multiple accounts

4) What specific training is provided for hybrid or remote work environments?

- Open network connectivity
- Avoiding the use of any digital devices
- Home network security and effective VPN use

5) How can training about insider threats be applied to enhance incident response plans?

- Insider threat training is unrelated to incident response
- Through drills that simulate different insider threat scenarios
- By limiting access to sensitive data to senior management only

6) When considering the use of software as a service (SaaS) applications, what specific training should employees receive to handle data securely?

- Only training provided by the SaaS vendor is necessary
- Guidance on secure SaaS configuration and data sharing implications
- No additional training is needed since SaaS applications are secure by design

©zyBooks 12/12/24 18:10 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

Security awareness program development, execution, and monitoring

Security awareness programs begin by developing training modules that provide guidance on key security practices. Following development, the modules are delivered through engaging and interactive formats, consistently reinforced with regular updates to ensure ongoing employee engagement. The execution phase includes interactive sessions and continuous refreshers to enhance awareness.

Beyond the foundational training, security awareness programs also include mechanisms for reporting and monitoring effectiveness, allowing for continuous refinement and adaptation in response to emerging security challenges. Such a dynamic approach ensures the training remains relevant, effective, and aligned with the evolving security landscape.

14.11 LAB: Security policies (Walkthrough)

IT-Labs are not printable at this time.

14.12 LAB: Enhancing security through policy implementation (Scenario)

IT-Labs are not printable at this time.