CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 4
Security Architectures

Frameworks, Policies, Controls, and Procedures

Chapter 11

Outline

- Security Frameworks
- Policies and Procedures
- Controls
- Regulatory Compliance
- Verification and Quality Control
- Quiz

Security Frameworks

- **Security framework**
  - **a series of documented, agreed and understood policies, procedures, and processes that define how information is managed to lower risk and vulnerability**
  - **Common frameworks:**
    - **NIST**
    - **ISO**
    - **COBIT**
    - **SABSA**
    - **TOGAF**
    - **ITIL**

Security Frameworks

- National Institute for Standards and Technology (NIST)
  - Develops and publishes standards and guidelines at improving practices
  - 2 important publications:
    - SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)
      - provides specific guidance on how to select security controls
    - Cyber Security Framework (CSF)
      - a voluntary cybersecurity framework for organizations that are part of the critical infrastructure
      - CSF Core has 5 functions
        - » Identify
        - » Protect
        - » Detect
        - » Respond
        - » Recover

Security Frameworks

- **International Organization for Standardization (ISO)**
  - **The world's largest developer of and publisher of international standards**
  - **Worked with the International Electrotechnical Commission (IEC) to build a family of Information Security Management System (ISMS) standards known as the ISO/IEC 27000 series**
    - **These standards serve as industry best practices for the management of security controls**
    - **It is common for organizations to seek a ISO/IEC 27001 certification**

ISO/IEC 27000 series

- ISO/IEC 27000 Overview and vocabulary
- ISO/IEC 27001 ISMS requirements
- ISO/IEC 27002 Security management
- ISO/IEC 27003 ISMS implementation
- ISO/IEC 27004 ISMS measurement
- ISO/IEC 27005 Risk management
- ISO/IEC 27006 Certification requirements
- ISO/IEC 27007 ISMS auditing
- ISO/IEC 27008 Guidance for auditors
- ISO/IEC 27031 Business continuity
- ISO/IEC 27033 Network security
- ISO/IEC 27034 Application security
- ISO/IEC 27035 Incident management
- ISO/IEC 27037 Digital evidence collection and preservation

Security Frameworks

- **Control Objectives for Information and Related Technology (COBIT)**
  - **Defines goals for managing IT, integrating these with business needs**
  - **Bridges the gap between a high-level framework and the selection and implementation of effective procedures and controls**
  - **four specific domains:**
    - **Planning & Organization**
    - **Acquiring & Implementation**
    - **Delivering and Support**
    - **Monitoring & Evaluating**

Security Frameworks

- **Sherwood Applied Business Security Architecture (SABSA)**
  - **A layered model in which each layer is less abstract and improves in detail to provide a chain of traceability from policy to practical implementation including all steps in between.**
  - **Provides a structure and processes upon which individual architectures may be built and maintained**
- **The Open Group Architecture Framework (TOGAF)**
  - **An enterprise architecture framework originating with the US Department of Defense**
  - **Provides an approach for designing, implementing, and governing architectures**

Security Frameworks

- **Information Technology Infrastructure Library (ITIL)**
  - **A series of best practices for IT service management**
  - **Seeks to create a better blending of IT and business objectives**
  - **Operates though a customizable framework that provides goals and general activities necessary to achieve those goals**
  - **Focuses on internal service level agreements between IT and a business's internal departments**

Interactive Exercise: 1

What is a Security Framework?	
What are the six common Security frameworks?	
Which security framework The world's largest developer of and publisher of international standards?	

Interactive Exercise Answer: 1

What is a Security Framework?	a series of documented, agreed and understood policies, procedures, and processes that define how information is managed to lower risk and vulnerability
What are the six common Security frameworks?	- NIST - ISO - COBIT - SABSA - TOGAF - ITIL
Which security framework The world's largest developer of and publisher of international standards?	International Organization for Standardization or ISO

Policies and Procedures

- **Security Policies**
  - **defined regulations for maintaining security within an organization**
  - **Data Classification**
    - **Organizing data based on its level of sensitivity and the impact should that data be disclosed, altered, or destroyed without authorization**
  - **Data Ownership**
    - **Defines who is responsible for both the responsibilities and use of specific information**
  - **Data Retention**
    - **organization's established protocol for retaining information for operational or regulatory compliance needs**

Policies and Procedures

- **Passwords**
  - Regulations on employing strong passwords
- **Acceptable Use**
  - what the organization considers an acceptable use of the information systems that are made available to the employee
- **Account Management**
  - Procedures established for the creation, monitoring, control and removal of user accounts
    - Accounts with more privilege than necessary or accounts for former users that should no longer be on the system are potentially dangerous security risks

Policies and Procedures

- **Procedures**
  - **Detailed, step-by-step tasks that should be performed in order to achieve a certain goal**
  - **Procedures spell out exactly how policies, standards, and guidelines will be implemented in an operating environment**
  - **Effective procedures must be:**
    - **Detailed**
    - **Understandable**
    - **Useful / Practical**

Policies and Procedures

- **Continuous Monitoring Procedures**
  - **Defined by NIST as "Maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions"**
  - **The process by which an organization collects and analyzes information in order to maintain awareness of threats, vulnerabilities, compliance, and effectiveness of security controls.**
  - **Should be enact remediation plans if a situation is discovered wherein the security of the system is compromised or a new threat or vulnerability is revealed**

Policies and Procedures

- **Evidence Production Procedures**
  - Evidence production is a legal request for information having a bearing on a legal procedure
  - In court the way evidence is produced is nearly as important as the evidence itself
    - A well documented and enforced procedure becomes is critically important
  - The Electronic Discovery Reference Model identifies 8 steps
    - Identification
    - Preservation
    - Collection
    - Review
    - Analysis
    - Production
    - Presentation

Policies and Procedures

- **Patching Procedures**
  - **Security patches identify, test, apply, validate and document fixes for software vulnerability**
  - **Patching procedures are the processes by which it is decided which patches are needed, whether there are likely to be any unintended effects and if so whether to apply the patches anyway**
  - **After patches are installed, they should be documented and validated to ensure that their intended purpose is being served**

Policies and Procedures

- **Compensation Control Development Procedures**
  - **Security controls that compensate for when leaders knowingly choose not to take actions and leave vulnerabilities in their information systems**
    - **Valid reasons for leaving vulnerabilities include when patches would break critical processes or when a vulnerability cannot be directly fixed**

Policies and Procedures

- **Control-Testing Procedures**
  - All controls implemented to protect an organization's information system should be verified and validated
    - Verify that the control is in place and installed correctly
    - Validate that the control does in fact protect the system from the intended threat
- **Exception Management Procedures**
  - Sometimes an organization will choose to violate its own policies or procedures
  - A detailed procedure of who should make which decisions and the process by which these decisions are implemented should be in place before this decision-making process is initiated

Interactive Exercise: 2

What are the six Security Policies?	
What is Data Classification?	
What makes a procedure effective?	
What does Patching Procedures do?	
How does Control-Testing Procedures help protect an organization's information system?	

Interactive Exercise Answer: 2

What are the six Security Policies?	- Data Classification - Data Ownership - Data Retention - Passwords - Acceptable Use - Account Management
What is Data Classification?	is organizing data based on its level of sensitivity and the impact should that data be disclosed, altered, or destroyed without authorization
What makes a procedure effective?	A effective procedure must be - Detailed - Understandable - Useful / Practical
What does Patching Procedures do?	Patching procedures are the processes by which it is decided which patches are needed, whether there are likely to be any unintended effects and if so whether to apply the patches anyway
How does Control-Testing Procedures help protect an organization's information system?	–Verify that the control is in place and installed correctly –Validate that the control does in fact protect the system from the intended threat

Controls

- **Physical Controls**
  - **Safeguards that deter, delay, prevent, detect, or respond to threats against physical property**
  - **Examples:**
    - **ID cards to enter buildings**
    - **Fob controlled gates**
- **Logical/Technical controls**
  - **software tools used to restrict access to system resources**
  - **Examples:**
    - **User authentication**
    - **Encryption**
    - **Firewalls**

Controls

- **Administrative controls**
  - **Security policies and procedures conducted by management**
  - **Examples:**
    - **Management can give or revoke access to resources**
    - **Management must determine what actions to take if an employee is terminated to maintain resource security**
- **Control Selection**
  - **Organizationally Defined Parameters**
    - **define parts of specific controls in order to meet organizational or operational needs**
  - **Selection Criteria**
    - **consists of the baseline security levels for each system combined with any additional requirements imposed by laws, regulations, or policies**
    - **Risk assessment helps determine if the baseline is adequate**

Regulatory Compliance

- **Regulatory Compliance**
  - **adherence to established laws and regulations**
  - **Examples:**
    - **Sarbanes-Oxley Act (SOX) - integrity protection**
    - **Payment Card Industry Data Security Standard (PCI DSS) – vulnerability scanning**
    - **The Gramm-Leach-Bliley Act (GLBA) - requires financial institutions to maintain safeguards to protect the confidentiality and integrity of personal consumer information**
    - **Federal Information Security Management Act (FISMA) - minimum frequency of risk assessments, security awareness training, incident response, and continuity of operations requirements**
    - **Health Insurance Portability and Accountability Act (HIPAA) – place specific requirements on protecting the confidentiality, integrity, availability, and privacy of patient data**

Verification and Quality Control

- **Verification**
  - **defined policies and procedures are being followed**
- **Quality control**
  - **Follow defined policies and procedures to ensure baseline security standards are met**
- **Audit**
  - **provides a fair and measurable way to examine how secure an organization is**
  - **Conducted by a third party (an external evaluation)**

Verification and Quality Control

- **Assessments**
  - **A means of evaluating the adequacy of an organization's security policies and procedures**
  - **Examples:**
    - **Vulnerability assessment**
    - **Penetration test**
    - **Red team assessment**
    - **Risk assessment**
    - **Threat modeling**
    - **Tabletop exercises**

Verification and Quality Control

- **Certification**
  - **A comprehensive evaluation of the security components of a system**
  - **ensures that security weaknesses are identified and plans for mitigation strategies are in place**
- **Accreditation**
  - **the process of accepting the residual risks associated with the continued operation of a system and granting approval to operate for a specified time period**

Verification and Quality Control

- **Maturity Models**
  - **Provides a formal method of improving security within an organization**
  - **a proactive, disciplined approach rather than reactive, high-risk approach**
  - **Example: Capability Maturity Model Integration (CMMI) has 5 maturity levels**
    - **Initial – ineffective procedures, inconsistency, unpredictability**
    - **Repeatable – processes are established, defined, and documented, using repeatable project management techniques**
    - **Defined – greater attention to documentation, standardization, and maintenance support**
    - **Managed – formal processes in place to collect and analyze data**
    - **Optimizing – continuous process improvement**

Interactive Exercise: 3

What are some examples of Physical Controls?	
What is Regulatory Compliance?	
What do assessments accomplish?	
What is Accreditation?	

Interactive Exercise Answer: 3

What are some examples of Physical Controls?	- ID cards - Guards - Cameras - Parameter fence
What is Regulatory Compliance?	It is to abide by established laws and regulations
What do assessments accomplish?	Assessments is a way to evaluate if an organization's security policies and procedures are adequate
What is Accreditation?	the process of accepting the residual risks associated with the continued operation of a system and granting approval to operate for a specified time period

Quiz

Chapter 11

Question #1

- **Which of the following is not a category for access controls and their implementation?**
  - **A. Administrative**
  - **B. Physical**
  - **C. Virtual**
  - **D. Logical**

Answer #1

- **C**
  - **Access controls are the mechanisms put into place to protect the confidentiality, integrity, and availability of systems, and are categorized as administrative, logical, or physical.**

Question #2

- **Which is the NIST publication that outlines various security controls for government agencies and information systems?**
  - **A. Special Publication 800-53**
  - **B. Special Publication 800-37**
  - **C. ISO/IEC 27000**
  - **D. ISO/IEC 27001**

Answer #2

- **A**
  - **The NIST released Special Publication 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), which aims to establish a unified information security framework for the federal government and related organizations.**

Question #3

- **Which of the following standards, composed of five core volumes, is widely accepted for service management of information technology assets?**
  - **A. Information Security Management System (ISMS)**
  - **B. Cyber Security Framework (CSF)**
  - **C. The Open Group Architecture Framework (TOGAF)**
  - **D. Information Technology Infrastructure Library (ITIL)**

Answer #3

- **D**
  - **The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management.**
  - **It provides the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals in a common language.**

Question #4

- **Which of the following NIST publications describes a voluntary cybersecurity structure for organizations that are part of the critical infrastructure?**
  - **A. Cyber Security Framework (CSF)**
  - **B. International Organization for Standardization (ISO)**
  - **C. Information Security Management System (ISMS)**
  - **D. Control Objectives for Information and related Technology (COBIT)**

Answer #4

- **A**
  - **The CSF focuses on aligning cybersecurity activities with business processes and including cybersecurity risks as part of the organization's risk management processes.**
  - **The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.**

Question #5

- **The ISO/IEC 27000 series describes which of the following?**
  - **A. Control Objectives for Information and related Technology (COBIT)**
  - **B. Information Security Management System (ISMS)**
  - **C. Architecture Development Method (ADM)**
  - **D. International Electrotechnical Commission (IEC)**

Answer #5

- **B**
  - **The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000-series, also known as the "ISMS Family of Standards," provides best practice recommendations on information security management.**

Question #6

- **Who is responsible for ensuring that data security controls are in place, defining classification requirements, and approving disclosure?**
  - **A. Systems administrators**
  - **B. Chief Security Officer**
  - **C. Data owners**
  - **D. Chief Information Officer**

Answer #6

- **C**
  - **Data owners classify data and are ultimately responsible for its protection, use, and disclosure.**

Question #7

- **What device is part of a formal process to improve a cybersecurity posture by developing comprehensive and repeatable security processes unique to the organization?**
  - **A. Verification**
  - **B. Maturity model**
  - **C. Quality control**
  - **D. Regulatory compliance**

Answer #7

- **B**
  - **Maturity models are used to create processes that are unique to the operating environment and help improve operational performance and the security posture.**

Question #8

- **Which component of the Cyber Security Framework describes the degree of sophistication of cybersecurity practices?**
  - **A. Framework Core**
  - **B. Implementation Tiers**
  - **C. NIST SP 800-53 control categories**
  - **D. ITIL processes**

Answer #8

- **B**
  - **CSF Implementation Tiers categorize the degree of rigor and sophistication of cybersecurity practices, which can be Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3), or Adaptive (tier 4).**

Question #9

- **Which are the key functions of the Framework Core of the Cyber Security Framework (CSF)?**
  - **A. Identify, Protect, Detect, Respond, Recover**
  - **B. Identify, Process, Detect, Respond, Recover**
  - **C. Identify, Process, Detect, Relay, Recover**
  - **D. Identify, Protect, Detect, Relay, Recover**

Answer #9

- **A**
  - **The Framework Core consists of five functions that can provide a high-level view of an organization's management of cybersecurity risk: Identify, Protect, Detect, Respond, Recover.**

Question #10

- **The directives that originate from senior management and govern the role of security practices in an organization are referred to by which term?**
  - **A. Administrative policy**
  - **B. Technical policy**
  - **C. Security policy**
  - **D. Physical policy**

Answer #10

- **C**
  - **A security policy is guidance produced by the senior management, policy board, or committee that dictates what role security plays within the organization.**

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.