CH7:

How to Secure the Site?

- Evaluating location-based threats:
  1. Political stability
  2. Susceptibility to terrorism
  3. Crime rate in the area
  4. Roadways and flight paths
  5. Utility stability
  6. Vulnerability to natural disasters
- The physical perimeter can be protected using:
  1. Obstacles: Berms, Fences, Gates, and Bollards
  2. Detection systems: Cameras, closed-circuit TV, alarms, motion sensors, and security guards
  3. Response system: Locking gates and doors, personnel notification and direct communication with police

The design of a secure site starts with the location

How Is Physical Access Controlled? Physical entry and exit controls:

Depending on the site and level of security required, available access controls (camera, locks, etc.) can be selected from

- ❑ Authorizing Entry (building access)
- ❑ Securing Offices, Rooms, and Facilities (within the building)
- ❑ Working in Secure Areas
- ❑ Ensuring clear desks and screens

Access control rules should be designed for:

- ❑ Employees
- ❑ Third-party (contractors/partners/vendors)
- ❑ Visitors

Physical entry/access controls (rules):

- ❑ Authorized users should be authorized prior to gaining access to protected area
- ❑ Visitors should be identified, labeled, and authorized prior to gaining access to protected area
- ❑ Visitors should be required to wear identification that can be evaluated from a distance, such as a badge
- ❑ Identification should start as soon as a person attempts to gain entry

Classification system should address

- personnel security
- Information system security
- Documents security

Hardware assets (Equipment) must be protected from:

1. Power surges: Prolonged increase in voltage
2. Power spikes: momentary increase in voltage
3. Blackouts: Prolonged periods of power loss
4. Fault: momentary loss if power
5. Sag: Momentary periods of low voltage
6. Brownout: Prolonged period of low voltage

No power, no processing: Reduce power consumption, for example by purchasing Energy Star certified devices

Elements of fire protection:

1. Fire prevention controls: Hazard assessments, inspections, and following construction codes
2. Fire detection: Smoke, heat, and flame activated (detection devices)
3. Fire containment and suppression

Fire based Classification:

1. Class A (materials: wood, paper)
2. Class B (liquids: oils, gas)
3. Class C (electrical equipment)
4. Class D (metals)

What About Disposal?

- Removing data from drives: Formatting a hard drive or deleting files does not mean that the data located on that drive cannot be retrieved
- Destroying materials: Making devices/media unreadable and unusable through destruction (crushing, shredding or drilling through devices)

methods for permanently removing data from drives before their disposal:

- ❑ Disk wiping (overwriting the hard drive with 0 and 1)
- ❑ Degaussing (exposing the hard drive to high magnetic field)

CH8:

Communication and operations security focus on functions:

- ❑ Standard operating procedures
- ❑ Change management
- ❑ Malware protection
- ❑ Data replication
- ❑ Secure management
- ❑ Activity monitoring

Standard Operating Procedures (SOPs): are detailed explanations of how to perform a task

Standard Operating Procedures (SOPs) provide: standardized direction, improved communication, reduced training time and improved work consistency

Effective SOPS include:

1. Who performs the task
2. What materials are necessary
3. Where the task takes place
4. When the task should be performed
5. How the person is to execute the task

SOPs Documentation: should be written in detail by someone with enough experience of the targeted process.

Authorizing SOP Documentation ,

Documented procedure must be:

1. Reviewed: The reviewer should check the SOP for clarity and reliability
2. Verified: The verifier should test the procedure and ensure they are correct and not missing any steps
3. Authorized (before publication): The process owner is responsible for authorization, publication and distribution of the document

The integrity of the SOP document should be protected through:

1. Access controls: Should be applied to protect the procedure document from any tampering
2. Version controls: Employees should use the latest revision of the procedure

Developing SOPs should be:

- ❑ Concise & clear
- ❑ Logical step-by-step order
- ❑ Plain language format
- ❑ Exceptions are noted and explained
- ❑ Warnings are clear and standout

common SOP formats:

- ❑ Simple step
- ❑ Hierarchical
- ❑ Flowchart
- ❑ Graphic

Change control: An internal procedure in which authorized changes are made

The change control process:

- ❑ Submitting a Request For Change (RFC)
- ❑ Developing a change control plan
- ❑ Communicating change
- ❑ Implementing & monitoring change

The RFC should include:

- ❑ Description of the proposed change
- ❑ Justification why the change should be implemented
- ❑ Impact of not implementing the change
- ❑ Alternatives
- ❑ Cost
- ❑ Resource requirements and timeframe

The change control plan should include:

- ❑ Security reviews to ensure no new vulnerabilities are introduced
- ❑ Implementation instructions
- ❑ Rollback and/or recovery options
- ❑ Post implementation monitoring

Communicating Change

- **There are two main categories of messages that are communicated:**
  1. Messages about the change, which should include:
     - Current situation
     - The need for change
     - What the change is, how it will change and when
  2. Messages how the change will impact employees
     - Impact on day-to-day activities of the employees
     - Implication on job security

Patch management: is the process of scheduling, testing, approving, and applying security patches

Malware (malicious software) is designed to:

- disrupt computer operation
- gather sensitive information
- or gain unauthorized access to computer systems and mobile devices

Types of Malware:

- Viruses: malicious code that attaches to become part of another program
- Worm: a piece of code that spreads from one computer to another without requiring a host file
- Trojans: malicious code that masks itself as an application
- Bots: Snippets of code designed to automate tasks and respond to instructions
- Ransomware: a type of malware that take computer or its data as hostage
- Rootkits: a set of software tools that hides its presence on the computer, using some of the lower layers of the operating system
- Spyware/adware: general term describing software that tracks internet activity and searches without user knowledge

How Is Malware Controlled?

- Prevention controls
  - Stop an attack before it occurs
    - Disable remote desktop connection
    - Configure the firewall to restrict access
    - Disallow users to install software on company device
- Detection controls
  - Identify the presence of malware, alert the user, and prevent the malware from carrying out its mission
    - Real-time firewall detection of suspicious files download and of suspicious network connections

What Is Antivirus Software? Antivirus software is used to detect, contain, and in some cases eliminate malicious software

two techniques Of Antivirus Software:

- Signature-based recognition
- Behavior-based (heuristic) recognition

Antivirus software is not 100% effective due to three factors:

- The volume of new malware
- Single-instance malware
- Blended threats (malware put together)

Reduced The impact of malware, hardware failure, accidental deletion by effective:

- Data Replication: is the process of copying data to a second location that is available for immediate use
- Data backup: is the process of copying/storing data that can be restored to its original location

Recommended Backup/Replication Strategy:

- Decision to backup/replicate and how often should be based on the impact of not being able to access the data
- Several factors should be considered when the strategy is designed:
  - Reliability, Speed and efficiency, Simplicity and ease of use,Cost
- Backed-up or replicated data should be stored in a off-site location, secure from theft, the elements, and natural disasters

Encryption protects the privacy of the message by converting it from readable plain text to ciphers text

Malware is spread in emails through:

- Attachments
- Hyperlinks
- Email hoax: Email containing false information (like virus) asking user to perform actions that can be damaging.

Common e-mail-related mistakes are:

- Hitting the wrong button: using “reply all” as instead of “reply” or “forward” instead of “reply”
- Sending an e-mail to the wrong e-mail address
- Forwarding an email with the entire string

Log management activities include:

- Configure log sources, log generations, storage & security
- Perform analysis of log data
- Initiate appropriate responses to identified events
- Manage the long-term storage of log data

Log analysis techniques include:

- Correlation: ties individual log entries together based on related information
- Sequencing: examines activity based on patterns
- Signature: compares log data to "known bad" activity
- Trend analysis: identifies activity overtime that alone might seem normal

CH9:

Access controls: Security features that govern how users and processes communicate and interact with systems and resources

Primary objective of Access controls: is to protect information and systems from unauthorized access, modification, or disruption

Common Attributes of Access Controls:

- Identification scheme: identifies unique records in the set, subject supplies identifier to the object
- Authentication method: how id is proven to be genuine
- Authorization method: to carryout certain operations

Two fundamental security postures:

- Open
  - which implements the "default allow" model
  - means that access, not explicitly forbidden, is permitted.
- Secure,
  - which implements the "default deny" model
  - means that access, not explicitly permitted, is forbidden.

Definition of Least Privilege: The least amount of permissions granted users that still allow them to perform whatever business tasks they have been assigned, and no more.

Definition of Need-to-know: Having a demonstrated and authorized reason for being granted access to information.

Authentication: Subject must supply verifiable credentials offered referred as factors

- Single-factor authentication
- Multifactor authentication
- Multilayer authentication

How Is Identity Verified? Three categories of factors

- Knowledge: Something you know (Password, PIN, Answer to a question).
- Possession: Something you have (One-time passcodes, Memory cards, Smart cards, Out-of-band communication).
- Inherence: Something you are (Biometric identification).

What Is Authorization: The process of assigning authenticated subjects permission to carry out a specific operation. The authorization model defines how access rights and permission are granted.

Primary authorization models

- Object capability: Used programmatically and based on a combination of a unforgettable reference and an operational message
- Security labels: Mandatory access controls embedded in object and subject properties
- Access Control Lists: Used to determine access based on some criteria

Categories of access control lists:

- MAC (Mandatory Access Control): Data is classified, and employees are granted access according to the sensitivity of information
- DAC (Discretionary Access Control): Data owners decide who should have access to what information
- RBAC (Role-based Access Control): Access is based on positions (roles) within an organization
- Rule-based access control: Access is based on criteria that is independent of the user or group account

Infrastructure Access Controls: Include physical and logical network design, border devices, communication mechanisms, and host security settings

Network segmentation: The process of logically grouping network assets, resources, and applications

Type of network segmentation

- Enclave network
- Trusted network
- Semi-trusted network, perimeter network, or DMZ
- Guest network
- Untrusted network

What Is Layered Border Security? Different types of security measures designed to work in tandem with a single focus

How to protect internal network from external threats:

- Firewall devices
- Intrusion detection systems (IDSs)
- Intrusion prevention systems (IPSs)
- Content filtering and whitelisting/blacklisting
- Border device administration and management

Firewalls: are devices or software that control the flow of traffic between networks.

- The rule set is used by the firewall to evaluate ingress (incoming) and egress (outgoing) network traffic.

Intrusion detection systems - (IDSs): are passive devices designed to analyze network traffic in order to detect unauthorized access or malevolent activity.

- Most IDSs use multiple methods to detect threats, including signature-based detection, anomaly-based detection, and stateful protocol analysis.

Intrusion prevention systems (IPSs): are active devices that sit inline with traffic flow and can respond to identified threats by disabling the connection, dropping the packet, or deleting the malicious content

Types of IDS/IPS technologies:

- Network-based IDS/IPS: Monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity
- Wireless IDS/IPS: Monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves
- Network behavior analysis IDS/IPS: Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.
- Host-based IDS/IPS: Monitors the characteristics of a single host and the events occurring within that host for suspicious activity

Content Filtering and Whitelisting/Blacklisting:

- Whitelists are addresses (IP and/or Internet domain names) of known "good" sites to which access should be allowed.
- blacklists are addresses (IP and/or Internet domain names) of known "bad" sites to which access should be denied. It is common practice to block entire ranges of IP addresses specific to geographic regions.
- Content-filtering applications can be used to restrict access by content category (such as violence, gaming, shopping, or pornography), time factors, application type, bandwidth use, and media.

Remote Access: Users who have a demonstrated business-need to access the corporate network remotely and are authorized to do so must be given that privilege

Remote access technologies:

- Virtual Private Networks (VPNs): Secure tunnel for transmitting data over unsecure network, such as the Internet
- Remote access portals: Offers access to one or more applications through a single centralized interface

Network access control (NAC): systems can be used to "check" a remote access device based on defined criteria such as operating system version, security patches, antivirus software version, and wireless and firewall configurations before it is allowed to connect to the infrastructure.

Teleworking Access Controls: teleworking allows employees to work offsite, often from their home.

User Access Controls: Used to ensure authorized users can access information and resources.

Types of Access Should Be Monitored?

- Successful access: record of user activity, Reporting should include date, time, and action
- Failed access: indicative of either unauthorized attempts or authorized user issues
- Privileged operations: Compromise or misuse of administrator accounts can have disastrous consequences.

Is Monitoring Legal?

Employees should have no expectation of privacy while on company time or when using company resources

CH10:

Systems development lifecycle (SDLC): provides a standard process for any system development.

five phases in the SDLC according to NIST:

- Initiation phase: Establishes the need for a system and documents its purpose
- Development /acquisition phase: The system is designed, purchased, programmed, or developed
- Implementation phase: The system is tested and retested, and any modifications are applied until it is accepted
- Operational phase: The system in put into production-should include monitoring, auditing, testing
- Disposal phase: Ensure the orderly termination of the system

Software Releases life cycle:

- Alpha phase: Initial release of software for testing, Can be unstable
- Beta phase: Software is complete and ready for usability testing
- Release candidate (RC): Hybrid of beta and final release version, Has the potential of being final release unless significant issues are identified
- General availability or go live: Software has been made commercially available

Two types of code

- Insecure code (referred as "sloppy code")
- Secure code: Deploying secure code is responsibility of the systems' owner

Input validation: is the process of validating all the input to an application before using it. This includes correct syntax, length, characters, and ranges.

Dynamic data verification: data that changes as updates become available—for example, an e-commerce application that automatically calculates sales tax based on the ZIP Code entered.

Output validation: is the process of validating (and in some cases, masking) the output of a process before it is provided to the recipient.

Cryptography: The process that takes plain text and turns it into ciphertext

Encryption is the conversion of plain text into what is known as cipher text using an algorithm called a cipher.

Decryption, the inverse of encryption, is the process of turning cipher text back into readable plain text.

Ciphertext: Text that cannot be read unless you apply the correct algorithm and predetermined value

Hashing: The process of creating a numeric value that represents the original text, It is a one-way process, Provides integrity

Digital signature: A hash value that has been encrypted with the sender's private key

Symmetric key: Uses a single secret key that must be shared in advance and kept private

Asymmetric key: Also known as public key, Uses two different but mathematically related keys, One is called public and the other one private

Public Key Infrastructure (PKI): Framework and services used to create, distribute, manage, and revoke public keys

Public Key Infrastructure Components:

- Certification Authority (CA): issues and maintains Digital certificates
- Registration Authority (RA): performs the administrative functions, including verifying the identity of users and organizations requesting a digital certificate, renewing certificates, and revoking certificates
- Client nodes: interfaces to users
- Digital certificate: contains public key of certificate holder, serial number, name, validity period, name of certificate issuer, digital signature, algorithm id.

CH11:

incident management: is defined as a predictable response to damaging situations.

The benefits of having a practiced incident response capability include the following:

- Calm and systematic response
- Minimization of loss or damage
- Protection of affected parties
- Compliance with laws and regulations
- Preservation of evidence
- Integration of lessons learned
- Lower future risk and exposure

Information security incident: is an adverse event that threatens business security and/or disrupts service

Core group of attacks:

- Intentional unauthorized access or use: Occurs when an insider or an intruder gains logical or physical access without permission
- Denial of service (DoS) attacks: Prevents or impairs the normal authorized functionality of the organization's networks, systems, or applications
- Malware: Code that is covertly inserted into another program with the intent of gaining authorized access or causing harm
- Inappropriate usage: Occurs when authorized user performs actions that violate company policy, agreement, law, or regulation

Incident Severity Levels:

- Level 1: Incidents that could cause significant harm
- Level 2: Compromise of or unauthorized access to noncritical systems or information
- Level 3: Situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel

How Are Incidents Reported?

- Employees should be required to report all actual and suspected incidents
- The employee who discovers an incident may not be trained or an IT technician
- The culture of the company needs to incorporate this point so that employees don't feel like they may be ridiculed if they are wrong

What Is an Incident Response Program? Composed of policies, plans, procedures, and people

An incident response plan (IRP): is a roadmap of reporting, responding, and recovery actions

Incident response procedures: are detailed steps needed to implement the plan

Key Incident Management Personnel:

- Incident response coordinator (IRC)
  - ❑ Central point of contact for all incidents
  - ❑ Verifies and logs the incident
- Designated incident handlers (DIHs)
  - ❑ Senior-level personnel who have crisis management and communication skills, experience, and knowledge to handle an incident
- Incident response team (IRT)
  - ❑ Trained team of professionals that provide services through the incident lifecycle

Incident Severity Level Matrix:

Severity Level = 1	
Explanation	Level I incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.
Required Response Time	Immediate.
Required Internal Notification	Chief Executive Officer. Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Compromise or suspected compromise of protected customer information. Theft or loss of any device or media on any device that contains legally protected information. A denial of service attack. Identified connection to "command and control" sites. Compromise or suspected compromise of any company website or web presence. Notification by a business partner or vendor of a compromise or potential compromise of a customer or customer-related information. Any act that is in direct violation of local, state, or federal law or regulation.
Severity Level = 2	
Explanation	Level 2 incidents are defined as compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation.
Required Response Time	Within four hours.
Required Internal Notification	Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Inappropriate access to legally protected or proprietary information. Malware detected on multiple systems. Warning signs and/or reconnaissance detected related to a potential exploit. Notification from a third party of an imminent attack.
Severity Level = 3	
Explanation	Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services.

Required Response Time	Within 24 hours.
Required Internal Notification	Chief Information Security Officer. Designated incident handler.
Examples	Malware detected and/or suspected on a workstation or device, with no external connections identified. User access to content or sites restricted by policy.

Activities in the incident response plan (IRP):

- Preparation includes developing internal incident response capabilities, establishing external contracts and relationships, defining legal and regulatory requirements, training personnel, and testing plans and procedures.
- Detection and investigation include establishing processes and a knowledge base to accurately detect and assess precursors and indicators.
- Initial response include incident declaration, internal notification, activation of an incident response team, and/or designated incident handlers, and prioritization of response activities.
- Containment includes taking the steps necessary to prevent the incident from spreading, and as much as possible limit the potential for further damage.
- Eradication and recovery include the elimination of the components of the incident.
- Notification includes the steps taken to notify state and federal agencies, affected parties, victims, and the public-at-large.
- Closure and post-incident activity include incident recap, information sharing, documentation of "lessons learned," plan and procedure updates, and policy updates and risk reviews, as applicable.
- Documentation and evidence-handling requirements include the recording of facts, observations, participants, actions taken, forensic analysis, and evidence chain of custody.

Communicating Incidents: Throughout the incident lifecycle, there is frequently the need to communicate with outside parties, including law enforcement, insurance companies, legal counsel, forensic specialists, vendors, external victims, and other IRTs.

Incident Response Training and Exercises:

- Establishing a robust response capability ensures that the organization is prepared to respond to an incident swiftly and effectively.
- Responders should receive training specific to their individual and collective responsibilities. Recurring tests, drills, and challenging incident response exercises can make a huge difference in responder ability.

Documenting Incidents

- The initial documentation should create an incident profile. The profile should include the following:
- How was the incident detected?
- What is the scenario for the incident?
- What time did the incident occur?
- Who or what reported the incident?
- Who are the contacts for involved personnel?
- A brief description of the incident.
- Snapshots of all on-scene conditions.

The process of digital forensic includes

- Collection
- Examination
- Analysis
- Reporting

Data Breach Notification Requirements: A data breach is widely defined as an incident that results in compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or unauthorized use or loss of control of legally protected PII (Personally identifiable information).

CH12:

Disaster: Any event that results in damage or destruction, loss of life, or drastic change to the environment, the cause can be environmental, operational, accidental, or willful.

Resilient organization: Has the capability to quickly adapt and recover from known or unknown change to the environment

Continuity planning: The business practice of ensuring the execution of essential functions

Risk management for continuity of operations requires the organizations to:

- Identify the threats that can disrupt operations
- Determine the risk
- Assess the impact on the company

Business continuity threat assessment:

- Identify viable threats and predict the likelihood of occurrence
- Threat modeling takes into account historical and predictive geographic, technological, physical, environmental, third-party, and industry **factors such as the following:**

■ What type of disasters have occurred in the community or at this location?
■ What can happen due to the geographic location?
■ What could cause processes or information systems to fail?
■ What threats are related to service provider dependency?
■ What disasters could result from the design or construction of the facility or campus?
■ What hazards are particular to the industry sector?

Business continuity risk assessment: Evaluates the sufficiency of controls to prevent a threat from occurring or to minimize its impact, the outcome is the residual risk associated with each threat.

Business Impact Analysis: Identify essential services/processes and recovery timeframes

A business impact analysis step:

- Step 1: Identify essential business services and processes.
- Step 1A: Determine the maximum tolerable downtime for each service.
- Step 2: Identify supporting infrastructure, information systems, and dependencies.
- Step 2A: Determine recovery time objectives and recovery point objectives
- Step 3: Compare to current recovery capability. Step 3A: Document the gap between desired and current capabilities.
- Step 4: Have stakeholders review the report for accuracy.
- Step 5: Present the BIA to management for approval.

A business impact analysis (BIA) incorporates three metrics:

- The maximum tolerable downtime (MTD) is the total length of time an essential business function can be unavailable without causing significant harm to the business.
- The recovery time objective (RTO) is the maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business processes.
- The recovery point objective (RPO) represents the point in time, prior to a disruption or system outage, that data can be recovered (in other words, the acceptable data loss).

The objective of Business Continuity Plan: to ensure the organization has the capability to respond and recover from a disaster.

Business Continuity Plan Component:

- Response plans
- Contingency plans
- Recovery plans
- Resumption plans

Business Continuity Team (BCT): has the authority to make decisions related to disaster preparation, response, and recovery

Occupant emergency Plan (OEP): Describes evacuation and shelter-in-place procedures in the event of a threat or incident to the health and safety of personnel

Disaster Response Plans

Addresses what should be done immediately following a significant incident

- Defines who has the authority to declare a disaster
- Defines who has the authority to contact external entities
- Defines evacuation procedures
- Defines emergency communication & notification procedures

Relocation strategies:

- Hot site
  - Fully operational location with redundant equipment.
  - The data has been streamed to the site on a real-time basis or close to real time
- Warm site
  - Configured to support operations including communications capabilities, peripheral devices, power.
  - Spare computers may be located there that then would need to be configured in the event of a disaster
  - Data must be restored
- Cold site
  - Available alternative location
  - Equipped with power, HVAC, and secure access
- Mobile site
  - Self-contained unit
  - Equipped with the required hardware, software, and peripherals
  - Data needs to be restored

Operational Contingency Plans: Addresses how an organization's essential business processes will be delivered during the recovery process

Recovery strategies: The path to bringing the company back to a normal business environment

daunting recovery process:

- Mainframe
- Network
- Communications
- Infrastructure
- Facilities

The objective of the Resumption Phase: is to transition to normal operations.

Major activities of Resumption Phase:

- Validation: Verifying recovered systems are operating correctly
- Deactivation: The official notification that the organization is no longer operating in emergency or disaster mode

Test methodologies:

- Tabletop exercise: Structured review, Simulation
- Functional exercises
- Full-scale testing

Business continuity plan audit: Evaluation of how the business continuity program in its entirety is being managed, Auditors must be independent

Plan Maintenance: The plan should be reviewed and edited regularly to match the changes that occur in the company and/or the industry in which the company is involved

CH13:

Who regulates banking and financial services in Saudi Arabia?

- Saudi Arabian Monetary Agency (SAMA)
- Capital Market Authority (CMA)

Capital Market Authority (CMA) Duties:

- Regulate and develop the capital market and promote appropriate standards and techniques for all sections and entities involved in Securities Trade Operations.
- Protect investors and the public from unfair and unsound practices involving fraud, deceit, cheating, manipulation, and inside information trading.
- Maintain fairness, efficiency, and transparency in transactions of securities.
- Develop appropriate measures to reduce risks pertaining to transactions of securities.
- Develop, regulate, and monitor the issuance of securities and under-trading transactions.
- Regulate and monitor the activities of entities working under CMA.
- Regulate and monitor full disclosure of information related to securities and issuers.

The objective of Cyber Security framework: is to create an effective approach for addressing cyber security and managing cyber security risks within the Financial Sector.

Components of cyber security framework:

- Cyber security leadership and Governance
- Cyber security risk management and compliance
- Cyber security operations and technology
- Third party cyber security

Cyber security governance: A governance structure should be established and endorsed by the board of directors.

Cyber security strategy: A strategy should be setup related to cyber security, which aligns with the organization's strategic objectives.

Cyber security policy: A policy should be defined, approved and communicated to all stakeholders.

Cyber security roles and responsibilities: Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization.

Cyber Security in Project Management: ensure that the all the Member Organization's projects meet cyber security requirements.

Cyber Security Awareness: A cyber security awareness program should be defined and conducted for staff, third parties and customers of the Member Organization.

Cyber Security Training: Staff of the Member Organization should be provided with training regarding how to operate the Member Organization's systems securely and to address and apply cyber security controls.

Risk management: is the ongoing process of identifying, analyzing, responding and monitoring and reviewing risks.

The SAMA regulates the following entities:

- Conventional banks (deposit takers)
- Insurance companies that engage in any insurance and re-insurance activities, including general insurance, health insurance and protection and savings insurance
- Finance companies that engage in real estate finance, production asset finance, small and medium enterprise finance, finance lease, credit card finance, consumer finance, micro finance and any other finance activity approved by the SAMA

CH14:

Saudi Health Information Exchange (HIE) is a collection of polices that regulate and protect, the flow of the health information.

- Ministry of Health (MOH) enforces and monitors the HIE policies.

Saudi Health Information Exchange policies apply to:

- Participating Healthcare Subscriber (PHCSs),
- PHCS Business Associates,
- Any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI,
- Any Saudi Health Information Exchange Infrastructure Service Provider
- Any other subcontractors of the Saudi Health Information Exchange.

Permissible uses of Saudi Health Information Exchange (HIE) include:

- Patient Care and Treatment
- Public Health
- Healthcare Operations
- Education.
- Payment

Purpose of security policy:

- protects PHI
- supports: Availability, Confidentiality, integrity, Accountability

Saudi Health Information Exchange (HIE) Infrastructure security requires:

- Physical Security
- Access Control
- Classification of data
- Supervision of those with access

Data retention requirement:

- PHI is retained indefinitely
- Data may allow amendment or replacement for corrections
- Data SHALL NOT be deleted at any time

Purpose of Authentication Policy: Ensure that systems and individuals interacting with HIE are known through the process of reliable security identification of subjects.

Purpose of Identity Management Policy: Ensure that the identities of the individuals and entities interacting with HIE are assured to enable a data processing system to recognize entities.

Purpose of Consent and Access Control Policy:

- Define who and how individuals and systems can access HIE.
- Ensure that the resources of a data processing system can be accessed only by authorized users.
- Define the circumstances in which a Subject of Care can permit or withhold the use and disclosure of HIE accessible health information.

Purpose of Audit Policy: Ensure that the security and confidentiality of subject of care data transmitted through HIE is protected through privacy/security audits.

Define policy surrounding:

- identification
- investigation
- notification
- mitigation

CH15:

- Payment cards companies developed the **Payment Card Industry Data Security Standard (PCI DSS)** in order to protect cardholder information and to prevent fraud.
- **Payment Cards examples:** Visa, MasterCard, Discover, JCB International and American Express

Protecting Cardholder Data

- **PCI DSS applies to all system components where account data is stored**
  - **Account data;** Cardholder data plus sensitive authentication data
  - **System components;** Any network component, server, or application that is included in, or connected to, the cardholder data environment
  - **Cardholder data environment;** The people, processes, and technology that handle cardholder data or sensitive authentication data

Account Data Elements

TABLE 15.1 Account Data Elements

Cardholder Data Includes...	Sensitive Authentication Data Includes...
Primary account number (PAN)	Full magnetic stripe data or equivalent data on a chip
Cardholder name	CAV2/CVC2/CVV2/CID
Expiration date	PINs/PIB blocks
Service code	

What Is the PCI DSS Framework?

- The PCI DSS framework includes:
  1. Stipulations regarding storage, transmission, and processing of payment card data
  2. Six core principles
  3. Required technical and operational security controls
  4. Testing requirements
  5. Certification process

- Business-as-usual is defined as the inclusion of PCI controls as part of an overall risk-based security strategy that is managed and monitored by the organization.

The Six PCI DSS core principles

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

PCI Top Level Requirements

First Core Principle: **Build and maintain a secure network and systems** and Includes the following two requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and security parameters

Second Core Principle: **Protect Cardholder Data** , Includes the following two requirements

3. Protect stored card data
4. Encrypt transmission of cardholder data across open, public networks

Third Core Principle: **Maintain a Vulnerability Management Program**, Includes the following two requirements

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and architecture

Fourth Core Principle: **Implement Strong Access Control Measures**, Includes the following three requirements

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Fifth Core Principle: **Regulatory Monitor and Test Networks**, Includes the following two requirements

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Sixth Core Principle: **Maintain an Information Security Policy**, Includes the final requirement

12. Maintain a policy that addresses information security for all personnel
13.

Compliance Assessment

- Assessment Methodology
  1. Observe system settings
  2. Observe processes and actions that use cardholder data
  3. Review documentations
  4. Interview system users
  5. Run test data through system (Sampling)

Report on Compliance

- ROC standard template includes the following
  - ❑ Section 1: Executive Summary
  - ❑ Section 2: Description of Scope of Work and Approach Taken
  - ❑ Section 3: Details About Reviewed Environment
  - ❑ Section 4: Contact Information and Report Date
  - ❑ Section 5: Quarterly Scan Results
  - ❑ Section 6: Findings and Observations
  - ❑ Compensating Controls Worksheets (if Applicable)

What Is the SAQ?

- SAQ: Self-Assessment Questionnaire, A validation tool for merchants that are not required to submit to an onsite data security assessment

Are There Penalties for Noncompliance? Three type of fines

1. PCI noncompliance ; discretionary and can vary greatly, depending on the circumstances
2. Account Data Compromise Recovery (ADCR) ; for compromised domestic-issued cards
3. Data Compromise Recovery Solution (DCRS) ; for compromised international-issued cards

_____

تم بحمد الله..... دعواتكم