**Ch.4 summary By @MHazazi**

## Understanding Information Security Policies

- The goal of the information security policies is to protect the organization from harm
  - Policies should be written
  - Policies should be supported by management
  - Policies should help companies align security with business requirements laws & regulations
- ISO 27002:2013 provide a framework for developing security policies
- **Two approaches to information security**
  - **Parallel approach** = assigns responsibility for being secure to the IT department
  - **Integrated approach** = recognizes that security and success are intertwined
- Policies can serve as teaching documents to influence behavior
  - Acceptable Use Policy
- Companies should create vendor versions of information security policies
- Policies should be authorized by executive management
- Policies should be updated on regular basis

## Evaluating Information Security Policies

- Policies can be evaluated **internally** or **independent third parties**
- Evaluation methods:

1. **Audit**
   - Systematic, evidence-based evaluation
   - interviews, observation, tracing and review documents and data
   - Audit report containing the formal opinion and findings of the audit team
2. **Capability Maturity Model (CMM)**
   - Used to evaluate and document process maturity for a given area

## Information Security Governance

- Managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- Board of Directors responsible for overseeing the policy development.
- **Effective security requirements :**

1. Distribute governance model
2. Stakeholders, decision makers, and users involvement

## Distributed Governance Model

| | |
|---|---|
| **CISO** | Chief information security officer is the leader, teacher, and security champion across company. |
| **ISSC** | Information security steering committee consist of members from different section at the company who provides a forum to communicate, discuss, and debate on security requirements and business integration |
| **Compliance officer** | Identifying all applicable information security-related legal, regulatory, and contractual requirements. |
| **Privacy officer** | Handle and disclose of data as it relates to state, federal, and international law and customs. |
| **Internal audit** | measure compliance with Board-approved policies and to ensure that controls are functioning as intended. |
| **Incident response team** | Respond to and manage security-related incident |
| **Data owners** | - Define protection requirements for the data based on classification<br>- Review the access controls<br>- Monitor and enforce compliance with policies and standards |
| **Data Custodians** | - Implement, manage, and monitor the protection mechanisms<br>- Notify the appropriate party of any suspected policy violations |
| **Data users** | act as agents of the security program by taking reasonable and needed steps to protect the systems and data they have access to. |

## Regulatory Requirements

- ➢ Gramm-Leach Bliley (GLBA) Section 314.4
- ➢ HIPAA/HITECH Security Rule Section 164.308(a)
- ➢ Payment Card Industry Data Security Standard (PCI DDS) section 12.5
- ➢ 201 CMR 17: Standards for Protection of Personal Information of the Residents of the Commonwealth

## Information Security Risk

- **Three factors influence information security decision making and policy creation**
  1. Guiding principles
  2. Regulatory requirements
  3. Risk associated with achieving business objectives

- **Risk:** The potential of undesirable or unfavorable outcome from a given action
- **Risk tolerance:** How much undesirable outcome the risk taker is willing to accept
- **Risk appetite:** The amount of risk an entity is willing to accept in pursuit of its mission

## Risk Assessment

- Evaluate what can go wrong and the likelihood of a harmful event occurring
- **Risk assessment involves:**
  - Identifying inherent risk based on relevant threats, threat sources, and related vulnerabilities
  - Determining the impact of a threat if it occurs
  - Calculating the likelihood of occurrence
  - Determining residual risk

- **Inherent risk** = The level of risk before security measure are applied
- **Residual risk** = The level of risk after security measures are applied
- **Threat** = Natural, environmental, or human event that could cause harm
- **Vulnerability** = A weakness that could be exploited by a threat
- **Impact** = The magnitude of a harm

## Risk Assessment Methodologies

- **Components of a risk assessment methodology include**
  - Defined process
  - Assessment approach
  - Standardized analysis

- **Three well-known information security risk assessment methodologies**
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Factor Analysis of Information Risk (FAIR)
  - NIST Risk Management Framework (RMF)

**Risk Management**

- The process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level.
  - **Risk acceptance =** org accept the level of risk associated
  - **Risk mitigation =** reducing the risk by implementing one or more countermeasures
    1) Risk reduction = implement offensive or defensive controls to lower the residual risk
       - offensive control reduce or eliminate vulnerability
       - Defensive control respond to a threat source
    2) Risk transfer = shifts risk responsibility or liability to another organization.
    3) Risk sharing = shifts portion of risk responsibility or liability to another organization
    4) Risk avoidance = actions to eliminate or modify process or activities causing the risk