Governance and Compliance

Objectives:

- 5.1 - Summarize elements of effective security governance
- 5.4 - Summarize elements of effective security compliance

- **Governance and Compliance**
    - *Governance*
        - Overall management of IT infrastructure, policies, procedures, and operations
        - Framework
            - Aligns with organizational objectives and regulatory requirements
        - Crucial Aspects
            - Risk Management
                - Identify, assess, and manage potential risks
            - Strategic Alignment
                - Ensure IT strategy aligns with business objectives
            - Resource Management
                - Efficient and effective use of IT resources
            - Performance Measurement
                - Mechanisms for measuring and monitoring the performance of IT processes
    - *Compliance*
        - Adherence to laws, regulations, standards, and policies

- Importance
  - Legal Obligations
    - Non-compliance leads to penalties (fines, sanctions)
  - Trust and Reputation
    - Compliance enhances reputation and fosters trust
  - Data Protection
    - Prevents breaches and protects privacy
  - Business Continuity
    - Ensures operation in disasters or disruptions
- Governance Structures
  - Boards, Committees
    - Key elements in organizational structure
  - Government Entities
    - External entities influencing governance
  - Centralized vs Decentralized
    - Explanation of organizational structures
- *Policies*
  - High-level guidelines indicating organizational commitments
  - Topics Covered
    - Acceptable Use Policies
    - Information Security Policies
    - Business Continuity
    - Disaster Recovery
    - Incident Response
    - Change Management
    - Software Development Lifecycle (SDLC)

- *Standards*
  - Specific, mandatory actions or rules adhering to policies
  - Covered Standards
    - Password Standards
    - Access Control Standards
    - Physical Security Standards
    - Encryption Standards
- *Procedures*
  - Step-by-step instructions ensure consistency and compliance
  - Covered Procedures
    - Change Management Procedures
    - Onboarding and Offboarding Procedures
    - Playbooks
- Compliance Coverage
  - Monitoring and Reporting
    - Concepts like due diligence, due care, attestation, and acknowledgment
  - Internal and External Compliance
    - Differentiating factors
  - Automation in Compliance
    - Utilizing automation in the compliance process
- Consequences of Non-compliance
  - Fines, Sanctions
    - Legal penalties
  - Reputational Damage
    - Impact on trust and reputation

        - Loss of License, Contractual Impacts
            - Severe consequences

- **Governance**
    - *Governance*
        - Part of the GRC triad (Governance, Risk, and Compliance)
        - Strategic leadership, structures, and processes ensuring IT aligns with business objectives
        - Involves risk management, resource allocation, and performance measurement
    - Purpose of Governance
        - Establishes a strategic framework aligning with objectives and regulations
        - Defines rules, responsibilities, and practices for achieving goals and managing IT resources
    - Influence on IT Components
        - Shapes guidelines for recommended approaches in handling situations
        - Drives policy development, outlining organizational commitments (e.g., data protection)
        - Impacts standards, defining mandatory rules for policy adherence
        - Ensures procedures align with objectives, providing task-specific guidance
    - Adaptation and Revision
        - Governance must adapt to technological advancements, regulatory changes, and industry culture shifts
        - Monitoring evaluates governance effectiveness and identifies gaps
        - Revision updates governance framework

- **Governance Structures**
  - *Organizational Governance*
    - Complex, multifaceted concept essential for successful organization operation
    - Comprises various components, each with unique functions
  - Governance Structures
    - *Boards*
      - Elected by shareholders to oversee organization management
      - Responsible for setting strategic direction, policies, and major decisions
    - *Committees*
      - Subgroups of boards with specific focuses
      - Allows detailed attention to complex areas
    - Government Entities
      - Play roles in governance, especially for public and regulated organizations
      - Establish laws and regulations for compliance
    - Centralized and Decentralized Structures
      - *Centralized*
        - Decision-making authority at top management levels
        - Ensures consistent decisions and clear authority
        - Slower response to local/departmental needs
      - *Decentralized*
        - Decision-making authority distributed throughout the organization
        - Enables quicker decisions and local responsiveness
        - Potential for inconsistencies

- **Policies**
  - *Acceptable Use Policy (AUP)*
    - Document that outlines the do's and don'ts for users when interacting with an organization's IT systems and resources
    - Defines appropriate and prohibited use of IT systems/resources
    - Aims to protect organizations from legal issues and security threats
  - *Information Security Policies*
    - Cornerstone of an organization's security
    - Outlines how an organization protects its information assets from threats, both internal and external
    - These policies cover a range of areas
      - Data Classification
      - Access Control
      - Encryption
      - Physical Security
    - Ensures confidentiality, integrity, and availability of data
  - *Business Continuity Policy*
    - Ensures operations continue during and after disruptions
    - Focuses on critical operation continuation and quick recovery
    - Includes strategies for power outages, hardware failures, and disasters
  - *Disaster Recovery Policy*
    - Focuses on IT systems and data recovery after disasters
    - Outlines data backup, restoration, hardware/software recovery, and alternative locations
  - *Incident Response Policy*
    - Addresses detection, reporting, assessment, response, and learning from

security incidents
        - Specifies incident notification, containment, investigation, and prevention steps
        - Minimizes damage and downtime during incidents
    - *Software Development Lifecycle (SDLC) Policy*
        - Guides software development stages from requirements to maintenance
        - Includes secure coding practices, code reviews, and testing standards
        - Ensures high-quality, secure software meeting user needs
    - *Change Management Policy*
        - Governs handling of IT system/process changes
        - Ensures controlled, coordinated change implementation to minimize disruptions
        - Covers change request, approval, implementation, and review processes

- **Standards**
    - *Standards*
        - Provides a framework for implementing security measures, ensuring that all aspects of an organization's security posture are addressed
    - Password Standards
        - Define password complexity and management
        - Include length, character types, regular changes, and password reuse rules
        - Emphasize password hashing and salting for security
    - Access Control Standards
        - Determine who has access to resources within an organization
        - Include access control models like
            - Discretionary Access Control (DAC)
            - Mandatory Access Control (MAC)
            - Role Based Access Control (RBAC)

        - Enforce principles of least privilege and separation of duties
    - Physical Security Standards
        - Cover physical measures to protect assets and information
        - Include controls like perimeter security, surveillance systems, and access control mechanisms
        - Address environmental controls and secure areas for sensitive information
    - Encryption Standards
        - Ensure data remains secure and unreadable even if accessed without authorization
        - Include encryption algorithms like AES or RSA
        - Depends on the use case and balance between security and performance

- **Procedures**
    - *Procedures*
        - Systematic sequences of actions or steps taken to achieve a specific outcome in an organization
        - Ensures consistency, efficiency, and compliance with standards
    - *Change Management*
        - Systematic approach to handling organizational changes
        - It aims to implement changes smoothly and successfully with minimal disruption
        - Key Stages
            - Identifying the need for change
            - Assessing impacts
            - Developing a plan
            - Implementation
            - Post-change review

- Onboarding and Offboarding Procedures
  - Onboarding integrates new employees into the organization
    - ensures productivity and engagement
    - Includes orientation, training, and integration activities
  - Offboarding manages the transition when an employee leaves
    - Tasks include property retrieval, access disabling, and exit interviews
- *Playbooks*
  - Detailed guides for specific tasks or processes
  - They provide step-by-step instructions for consistent and efficient execution
  - Used in various situations, from cybersecurity incidents to customer complaints
  - Include resource requirements, steps to be taken, and expected outcomes

- **Governance Considerations**
  - Regulatory Considerations
    - Organizations must comply with various regulations, depending on industry and location
    - Regulations cover areas such as
      - Data Protection
      - Privacy
      - Environmental Standards
      - Labor Laws
    - Non-compliance leads to penalties, sanctions, and reputational damage
  - Legal Considerations
    - Complement regulatory considerations, encompassing contract, intellectual property, and corporate law
    - Employment laws address minimum wage, overtime, safety, discrimination, and

benefits
        - Litigation risks include breach of contract, product liability, and employment disputes
        - Robust legal strategies and resources are needed to manage legal risks
    - Industry Considerations
        - Refer to industry-specific standards, practices, and ethical guidelines
        - Not legally binding but influence customer, partner, and regulator expectations
        - Non-adoption may lead to competitive disadvantages and stakeholder criticism
    - Geographical Considerations
        - Geographical regulations impact organizations at local, regional, national, and global levels
        - Local considerations include city ordinances, zoning laws, and operational restrictions
        - Regional considerations, like CCPA in California, impose state-level regulations
        - National considerations, e.g., ADA in the US, affect businesses across the entire country
        - Global considerations, like GDPR, apply extraterritorially to organizations dealing with EU citizens' data
        - Conflict of laws between jurisdictions is a significant challenge
        - Navigating these differences requires deep legal knowledge and flexibility in governance

- **Compliance**
    - *Compliance*
        - Ensures adherence to laws, regulations, guidelines, and specifications
        - Includes compliance reporting and compliance monitoring

- *Compliance Reporting*
  - Systematic process of collecting and presenting data to demonstrate adherence to compliance requirements
  - Two Types of Compliance Reporting
    - *Internal Compliance Reporting*
      - Ensures adherence to internal policies and procedures
      - Conducted by an internal audit team or compliance department
    - *External Compliance Reporting*
      - Demonstrates compliance to external entities
      - Mandatory, often by law or contract
- *Compliance Monitoring*
  - Regularly reviews and analyzes operations for compliance
  - Includes due diligence and due care, attestation and acknowledgement, and internal and external monitoring
- Due Diligence and Due Care
  - *Due Diligence*
    - Identifying compliance risks through thorough review
  - *Due Care*
    - Mitigating identified risks
- Attestation and Acknowledgement
  - *Attestation*
    - Formal declaration by a responsible party that the organization's processes and controls are compliant
  - *Acknowledgement*
    - Recognition and acceptance of compliance requirements by all relevant parties

- Internal and External Monitoring
  - *Internal Monitoring*
    - Regularly reviewing an organization's operations to ensure compliance with internal policies
  - *External Monitoring*
    - Third-party reviews for compliance with external regulations or standards
- Role of Automation in Compliance
  - Streamlines data collection, improves accuracy, and provides real-time monitoring

- **Non-compliance Consequences**
  - Compliance in IT is essential to avoid severe consequences
  - Consequences of non-compliance include
    - *Fines*
      - Monetary penalties imposed by regulatory bodies
    - *Sanctions*
      - Strict measures by regulatory bodies to enforce compliance
      - Range from restrictions to bans
    - *Reputational Damage*
      - Negative impact on a company's reputation
      - Significant and long-lasting in the age of social media
    - *Loss of License*
      - Loss of the right to operate, relevant in regulated industries
    - *Contractual Impacts*
      - Breach of contracts due to non-compliance with laws and regulations
      - Can lead to legal disputes, financial penalties, or contract termination

- To avoid these consequences, companies should prioritize compliance by
  - Understanding and adhering to relevant laws and regulations
  - Implementing robust cybersecurity measures
  - Regularly reviewing and updating compliance programs