Bootcamp PPT#6

Session 2.3 Governance, Risk, and Compliance III

Tuesday September 15, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Class Objectives

- How to use policy procedures to formalize standards or right and wrong.
- Use governance frameworks to determine which policies an organization must develop.
- Explain how audits are used to ensure compliance.
- Develop business continuity and disaster recovery plans.

Governance and Compliance (BCP/DR)

- **Governance:** Codifying proper behavior.
- **Compliance:** Enforcing policies.

Codifying Rules and Policy Procedures

- **Policy:** rule that defines the right behavior.
    - Policies inform standards for behavior and operations.
- **Governance Framework:** defines the policies an organization must follow.
    - Federal or government standards.
- **GDPR:** General Data Protection Regulation
- Training plan, rules as examples of policies, and goal of defining and implementing new policy.
- **Internal/Volitional** vs **External/Imposed** goals.
    - Alphanumeric password policy.

Using Governance Frameworks to Guide Policy Desicions

- **External Objective** and **Policy**
    - Businesses often have to follow external rules in addition to those they set for themselves.
- **Governance Frameworks:** rules and policies that must be followed by an entire organization opr industry.

- **Securities and Exchange Commission** (SEC): regulators for security, policy enforcement, incident reporting enforcement, and auditing.
    - **GDPR:** General Data Protection Regulation
    - **HIPAA:** Health Insurance Portability and Accountability Act
    - **PCI-DSS:** Payment Card Industry Data Security Standard

Business Continuity and Disaster Recovery

- **Mild/moderate:** business has been impacted but can still handle day to day operations.
- **Serious/catastrophic breach:** impact so severe that operations are halted.
- Cyber attacks, human error, and enviromental disasters.
- **Business Continuity Plan** vs **Disaster Recovery**
    - Contingency planning:
        - Responsibility of emergency response.
        - Resource requirements.
        - Training requirements.
        - Scheduling maintenance.
    - Strategies for high-impact loss
    - **NIST** Impact Levels: **Low**, **Moderate**, **High**
- **Business Impact Analysis and Risk Assesment**
    - **Identify** key processes.
    - **Establish** a detailed list of requirement.
    - **Determine** resource requirements.
    - **Evaluate impact** on daily operation.
    - **Develop priorities** and classifications of functions.
    - **Develop** recovery time requirements.
    - **Determine disruption** of financial operations and legal operations.
- **BIA Metrics**
    - **Recovery Point Objective:** amount of time that a business can afford to lose.
    - **Maximum Tolerable Downtime:** total amount of time a system can afford to be unavailable to users.
        - **RTO:** *Recovery Time Objective*
        - **WRT:** *Work Recovery Time*