* Security Program Management and Oversight

**5.1 Security Governance**

* **Guidelines**
* **Policies** 
  + Acceptable use policy (AUP)
  + Information security policies
  + Business continuity
  + Disaster recovery
  + Incident response
  + Software development lifecycle (SDLC)
  + Change management
* **Standards** 
  + Password
  + Access control
  + Physical security
  + Encryption
* **Procedures** 
  + Change management
  + Onboarding/offboarding
  + Playbooks
* **External considerations** 
  + Regulatory
  + Legal
  + Industry
  + Local/regional
  + National
  + Global
* **Monitoring and revision**
* **Types of governance structures** 
  + Boards
  + Committees
  + Government entities
  + Centralized/decentralized
* **Roles and responsibilities for systems and data** 
  + Owners
  + Controllers
  + Processors
  + Custodians/stewards

What is an Organization?

* It is an entity formed for a specific purpose and composed of people who work together to achieve common goals.
* Government agencies, businesses, non-profit groups, educational institutions, etc.
* They are structured entities with defined roles, responsibilities, and a hierarchical framework.

Organizational Structure And Hierarchy

* Structure and hierarchy vary. However, there are common elements found in many structures.
* The **CEO** is the top executive responsible for overall management and decision-making.
* The **Executive Team** consists of top executives who manage specific functional areas within the organization: CFO, CISO, COO, etc.
* **Middle Management** includes managers who oversee specific departments within the organization.
* **Employees/Staff**: The operational level where employees perform their specific roles and contribute to daily tasks.

Governance Structures

* **Boards**
  + Provide direction and oversight for security initiatives. )%. Governing bodies responsible for security policies and strategic decisions.
* **Committees**
  + Groups formed to focus on specific areas of security.
* **Government Entities**
  + Enforce compliance with laws and regulations.
* **Centralized/Decentralized** 
  + **Centralized**: Decisions and policies are controlled by a central authority.
  + **Decentralized:** Responsibilities are distributed across multiple departments.

Roles & Responsibilities

**CEO**

* Chief Executive Officer
* Leader of the organization
* Defines the strategic goals
* Engages with the board of directors on initiatives

**Data Owner**

* Ownership and accountability of data
* Define security policies
* Business executives, Department heads

**Data Controller**

* Determine the purposes and means of processing data
* Control how data is processed
* IT Managers, Compliance Officers

**Data Processor**

* Process data on behalf of controllers
* Third-party vendors, internal IT staff

**Data Custodian**

* Protest data from unauthorized access
* Ensure backups and recovery

Security Policies

* Security policies provide a foundation for implementing security practices in an organization.
* They are documents that outline an organization's approach to security.
* They serve as a guide for decision-making.
* Acceptable Use Policies, Change Management, Access control policies, etc.

Acceptable Use Policies (AUP)

* An AUP is a document that outlines the acceptable ways in which an organization's resources may be utilized by employees, contractors, and others.
* It serves as guidelines to ensure secure use of resources within an organization.
* Examples:
  + Use of company email for personal communication should be limited.
  + Only authorized software should be installed on company devices.
  + Employees should exercise caution when representing the company on social media.

Information Security Policies

* Outline how an organization protects its IT assets.
* Covers data protection and access control.

Incident Response Policies

* Policies for detecting, responding to, and recovering from security incidents.
* Ensures effective response to minimize impact.

Bussiness Continuity

* Ensure the organization can continue operations during and after a disruption.
* Planning for critical business functions and resources.
* The events can be a power outage, loss of network connectivity, cyberattacks, earthquakes, etc

Disaster Recovery

* Restoring systems and data after a catastrophic event.
* Includes procedures, roles, contact information, communication plan, recovery strategies, testing.

Software Development Lifecycle

* Integrating security into the software development process.
* Planning —> Requirements —> Design —> Coding —> Testing —> Deployment & Maintenance.
* Integrate security early.

Change Management

* Change management is a policy that organizations follow to control changes to their IT systems.
* The goal is to ensure that any modifications are done in a controlled manner, encouraging accountability.
* It requires a formal and approval process.

Standards

* Security standards are practices that organizations follow to ensure the security of systems.
* They are developed by various organizations to provide a widely accepted set of principles for securing information.
* **Password**
* Requirements for password complexity and management.
* Ensures strong and secure password practices.
* Minimum age, characters, history, lockout policies, etc.
* **Access Control**
* Standards for managing user access to systems and data.
* Includes principles like least privilege and role-based access control.
* **Physical Security**
* Standards for securing physical access to facilities and equipment.
* Building access controls and surveillance.
* **Encryption**
* Encrypting sensitive data (at rest and in transit).
* Use of HTTPS, VPNs, AES, and secure protocols.
* Ensures data confidentiality.

Procedures

* Procedures are **step-by-step instructions** for implementing the requirements outlined in policies.
* **Change Management Procedures** are steps for requesting, reviewing, approving, and implementing changes.
* **Playbooks** are step-by-step guides for responding to specific security events.

Onboarding/Offboarding

* Granting individuals access to an organization's computing resources after being hired.
* Removing user access when they leave the company.

Guidelines

* Recommendations to support security policies and procedures.
* They are not mandatory.
* For example, social media guidelines might advise employees to use common sense when posting, while a social media policy might prohibit employees from sharing confidential company information.

External Considerations

* **Regulatory** — Compliance with regulations relevant to the organization's industry.
* **Legal** — Obligations for privacy. Contracts, agreements, and liability.
* **Local/Regional** — Compliance with regional laws.
* **National** — National-level guidelines for cybersecurity (e.g. NIST in USA).
* **Global** — Regulations for organizations operating globally (e.g. GDPR in Europe).

**5.2 Risk Management**

* **Risk identification**
* **Risk assessment** 
  + Ad hoc
  + Recurring
  + One-time
  + Continuous
* **Risk analysis** 
  + Qualitative
  + Quantitative
  + Single loss expectancy (SLE)
  + Annualized loss expectancy (ALE)
  + Annualized rate of occurrence (ARO)
  + Probability
  + Likelihood
  + Exposure factor
  + Impact
* **Risk register** 
  + Key risk indicators
  + Risk owners
  + Risk threshold
* **Risk tolerance**
* **Risk appetite** 
  + Expansionary
  + Conservative
  + Neutral
* **Risk management strategies** 
  + Transfer
  + Accept
  + Exemption
  + Exception
  + Avoid
  + Mitigate
* **Risk reporting**
* **Business impact analysis** 
  + Recovery time objective (RTO)
  + Recovery point objective (RPO)
  + Mean time to repair (MTTR)
  + Mean time between failures (MTBF)

What is Risk?

* A **vulnerability** is a weakness, a **threat** is a harmful thing that can exploit (take advantage of) a vulnerability.
* **Risk** in the context of security is the probability of a threat exploiting a weakness.
* These threats could be cybercriminals, malware, mistakes, or even natural disasters.
* **GRC** helps organizations align their governance, risk management, and compliance to achieve business goals.

Risk Management

* Risk management is the process of identifying, assessing, and reducing risks to an organization.
* Risk management typically includes:
  + **Identify risks**: Identifying risks to the organization.
  + **Assess risks**: Once the risks are identified, determin the probability and impact of each risk.
  + **Mitigate risks**: Take steps to reduce the probability or impact of the risks.
  + **Monitor risks** on a regular basis.

1. Risk Identification

* Recognizing potential risks before applying measures to mitigate them.
* Identified risks should be documented, detailing their nature, impact, and causes.
* A risk matrix is a tabular representation of the risks an organization face, helping to assess the likelihood of each risk and the severity of its impact.

1. Risk Assessment (Analysis)

* Risks are assessed quantitatively (using numerical data) and qualitatively (using expert judgment) to understand their probability and impact.
* Impact could be financial, operational, reputational, or related to compliance. Quantify the impact whenever possible.
* **Ad hoc** - Conducted on an as-needed basis, often in response to incidents.
* Less structured and may not follow a predefined schedule.
* **Recurring** - Regularly scheduled to continuously manage risks.
* **One-time** - Conducted for specific projects, providing a snapshot of risk at a particular point in time.
* **Continuous** - Ongoing risk assessment integrated into daily operations.
* **Automated tools** and real-time monitoring.

Quantitative & Qualitative Analysis

These are 2 distinct methods of assessing risks in an organization.

* Quantitative risk analysis involves assigning **numerical values** to aspects of risks, such as the probability of occurrence, potential impact, and **monetary loss**.
* Qualitative risk analysis involves a **subjective assessment** of risks based on judgment or experience. It doesn't assign numerical values to risks but uses descriptive terms to categorize risks.

Quantitative Analysis

* Single Loss Expectancy (**SLE**) is the expected monetary loss for one
* It is a **monetary value** assigned to an event that represents the potential loss amount if a negative event occurred.
* Annual Rate of Occurrence (**ARO**) measures how often an event can happen in a year.
* How many times is a negative event expected to happen in a year?
* Annual Loss Expectancy (**ALE**) represents the financial impact of a risk over the course of a year.
* **ALE = ARO x SLE**
* Suppose you expect a ransomware attack on your organization **2 times** per year, and each attack costs **$75,000** to repair servers and recover data. Your ALE is: **$150,000**

Quantitative Risk Analysis

* Suppose a fire in a warehouse causes **$37,500** in damages.
* The frequency of a fire taking place is once every 10 years (= ARO value of 0.1)
* What is the ALE?
* **$3,750** ($37,500 x 0.1 = $3,750)
* The ALE value tells the organization that if it wants to put in controls to protect the asset (warehouse) from this threat (fire), it can spend $3,750 or less per ear tn nrnwirio tho nrzroccary level of protection.

Risk Assessment (Analysis)

* **Likelihood** - The chance of a risk event happening (low, medium, high).
* Influences risk prioritization and mitigation strategies.
* **Exposure Factor (EF)** - The percentage of asset value at risk due to a specific threat.
* Helps in calculating potential losses.
* SLE = EF (Exposure Factor) x AV (Asset Value)
* **Impact** - The potential consequences of a risk event, considering financial, operational, reputational, and regulatory effects.
* Critical for understanding the severity of risks and prioritizing response actions.

Risk Register

* A documented repository used to record information about identified .
* Risks affecting an organization are documented and managed.
* **Key Risk Indicators** 
  + Metrics used to monitor and signal changes in risk levels.
  + Helps in identification and management of risks.
* **Risk Owners** 
  + Individuals or teams responsible for managing specific risks (ensures accountability).
* **Risk Threshold** 
  + The level of risk that an organization is willing to accept before action is required.

Risk Appetite

* The level of risk that an organization is willing to accept.
* A balance between pursuing opportunities and the adverse effects of risks.
* **Risk Tolerance**: A company might specify that it can tolerate up to a 25% market downturn before taking action.
* Risk appetite can be:
* **Expansionary**- Willing to take on higher risks to pursue opportunities.
* **Conservative** - Minimize risk exposure, prioritizing stability and security.
* **Neutral** - Maintaining a moderate approach, adopting flexible strategies that can adjust to changing conditions.

1. Responding to Risks

* Risk can be dealt with in four ways: **transfer it, avoid it, mitigate it, or accept it**.
* If an organization decides the risk is too high to gamble with, it can purchase insurance, which would **transfer the risk** to the insurance company.
* **Risk Avoidance**: Completely avoid an activity that poses risks.
  + **Example**: A company wants to allow employees to use WhatsApp at work but realizes that there are many risks on this app. The company could decide to forbid all WhatsApp communications in the office and on office equipment.
* **Risk mitigation** is an approach where the risk is reduced to a level considered acceptable enough to continue conducting business.
  + **Example**: Installing firewalls and anti-viruses on computers.
* **Accepting the risk** means that the organization understands the level of risk it is faced with, as well as the cost of damage, and decides to just live with it and not implement a countermeasure.

1. Risk Monitoring & Reporting

* Assess the effectiveness of our work by continuously monitoring.
* Develop metrics that act as warning signs and monitor these indicators.
* Regular communication of risk status to stakeholders.
* Detailed reports and dashboards to ensure decision-making

Buiness Impact Analysis

* BIA is a process that helps organizations understand the critical functions within their operations.
* Determining which processes/assets are crucial for the organization's operations.
* Evaluating the impact of disruptions on critical functions.

**5.3 Third Party Risk Management**

* **Vendor assessment** 
  + Penetration testing
  + Right-to-audit clause
  + Evidence of internal audits
  + Independent assessments
  + Supply chain analysis
* **Vendor selection** 
  + Due diligence
  + Conflict of interest
* **Agreement types** 
  + Service-level agreement (SLA)
  + Memorandum of agreement (MOA)
  + Memorandum of understanding (MOU)
  + Master service agreement (MSA)
  + Work order (WO)/statement of work (SOW)
  + Non-disclosure agreement (NDA)
  + Business partners agreement (BPA)
* **Vendor monitoring**
* **Questionnaires**
* **Rules of engagement**

Vendors / 3rd Parties

* Vendors refer to 3rd party companies that provide products or services to an organization.
* Vendor assessment involves evaluating the security practices and risks associated with vendors.
* Vendors can be potential entry points for cyber threats.
* Software vendors, hardware vendors, cloud service providers, consulting firms, telecom providers, datacenters, human resources, etc.

Vendor Assessment

* **Penetration Testing**
  + Conduct security testing on vendor systems to identify vulnerabilities.
  + Ensure that vendors meet security requirements and can protect data.
* **Right-to-Audit Clause**
  + Include clauses in contracts that grant the right to audit vendor practices.
  + Periodic reviews and assessments of vendors with security policies.
* **Evidence of Internal Audits** 
  + Require vendors to provide evidence of their internal security audits.
* **Independent Assessments**
* Use 3rd party assessments to verify vendor security practices.
* Unbiased evaluation.
* **Supply Chain Analysis**
* Assess the security of the vendor's supply chain.
* Identify risks from 3rd party services used by the vendor.

Vendor Selection

* **Due Diligence**
* Perform investigations of potential vendors before engagement.
* Ensures that they meet security and legal requirements.
* **Conflict of Interest**
* Identify any conflicts of interest that may affect vendor relationships.

Agreement Types

* **A Memorandum of Agreement (MOA)** is a formal agreement between parties outlining the terms of cooperation.
* It establishes roles, responsibilities, and expectations.
* **A Memorandum of Understanding (MOU)** is a non-binding (informal) agreement that both sides agree to. Not necessarily a signed contract.
* It is a precursor to a formal agreement.
* **A Master Service Agreement (MSA)** is a contract that outlines the overall terms of engagement for multiple services.

Service Level Agreement **(SLAs)**

* **A Service Level Agreement (SLA)** is a contract that states that a service provider guarantees a certain level of service.
* SLAS define the expected performance metrics, and responsibilities of the provider and the customer.
* If the service is not delivered at the agreed-upon level, then there are consequences (typically financial) for the service provider.
* Example: An Internet service provider may sign an SLA of 99.999% (commonly called "five nines") uptime of Internet. That means that they guarantee less than 26 seconds of downtime per month.

Non-Disclosure Agreements **Nas**

* Legal contract between parties that outlines the confidential information they will share and the obligations of to protect the confidentiality.
* NDAS help foster trust between parties.
* Protect sensitive and confidential information.

Agreement Types

* **A Business Partner Agreement (BPA)** is an agreement between business partners indicating the conditions of their relationship.
* **A Work Order (WO)/Statement of Work (SOW)** is a detailed document that specifies the work to be performed, timelines, and deliverables.
* Clarity and alignment on project scope and expectations.

3rd Party Risk Assessment

* Continuously monitor vendor performance with security requirements to ensures that they maintain security standards.
* Use questionnaires to gather detailed information about vendor security practices.
* Establish Engagement Rules, define the terms and conditions, ensures clear communication and alignment on expectations and responsibilities.

**5.4 Security Compliance**

* **Compliance reporting**
  + Internal
  + External
* **Consequences of noncompliance** 
  + Fines
  + Sanctions
  + Reputational damage
  + Loss of license
  + Contractual impacts
* **Compliance monitoring** 
  + Due diligence/care
  + Attestation and acknowledgement
  + Internal and external
  + Automation
* **Privacy** 
  + Legal implications
  + Local/regional
  + National
  + Global
  + Data subject
  + Controller vs. processor
  + Ownership
  + Data inventory and retention
  + Right to be forgotten

Compliance Reporting

* Documenting and communicating adherence to security standards.
* **INTERNAL REPORTING**
  + Regular audits and assessments.
  + Reporting findings to management.
  + Documenting compliance status and incidents.
* **EXTERNAL REPORTING**
  + Submitting reports to regulatory bodies, LTING & TRAINING
  + Providing compliance documentation to clients and partners. Sharing audit results with external stakeholders.

Non-Compliance

* Failing to comply with security regulations can lead to negative outcomes:
* Financial penalties (fines) imposed by regulatory bodies.
* Restrictions or prohibitions (sanctions) on certain business activities.
* Reputational Damage, loss of trust and credibility with customers.
* Revocation of licenses required to operate in certain industries.
* Breaches of contract leading to lawsuits or termination of agreements.

Compliance Monitoring

* Compliance monitoring ensures ongoing adherence to requirements.
* **Due Diligence/Care**
  + Regularly reviewing and updating security policies.
  + Implementing and maintaining appropriate security measures.
* **Attestation and Acknowledgement**
  + Formal statements by employees or third parties confirming compliance.
  + Regular training and awareness programs.
* **Internal and External Monitoring**
  + Conducting internal audits and assessments.
  + Engaging third-party auditors for external evaluations.
* **Automation**
  + Using automated tools to track compliance metrics.
  + Real-time monitoring and reporting of compliance status.
  + Tenable (Nessus), Qualys, Burp Suite, etc.

Privary

* Adhering to laws and regulations that protect personal data.
* **Data Subject** - Individuals whose personal data is being collected and stored.
* **Controller vs. Processor**
* **Controller:** Entity that determines the purposes and means of processing personal data (e.g. Amazon with customer data).
* **Processor:** Entity that processes personal data on behalf of the controller (e.g. card payment processor).
* **Legal Implications**
  + **Local/Regional**: Adhering to state or regional data protection laws (CCPA).
  + **National**: Compliance with national regulations like the GDPR (EU).
  + **Global**: Ensuring compliance with international protection standards (APEC).
* **Ownership** - Who owns the data and the rights associated with it.
* **Data Inventory and Retention** - Maintaining an inventory of personal data.
* Establishing and enforcing data retention policies.
* **Right to Be Forgotten** - Allowing data subjects to request the deletion of their personal data.

**5.5 Audits & Assessments**

* **Attestation**
* **Internal** 
  + Compliance
  + Audit committee
  + Self-assessments
* **External** 
  + Regulatory
  + Examinations
  + Assessment
  + Independent third-party audit
* **Penetration testing** 
  + Physical
  + Offensive
  + Defensive
  + Integrated
  + Known environment
  + Partially known environment
  + Unknown environment
  + Reconnaissance
    - Passive
    - Active

Audits & Assessments

* Systematic evaluations aimed at ensuring the security of an organization.
* An **audit** is a formal examination of an organization's policies and controls to ensure compliance with regulations.
* An **assessment** focuses on identifying vulnerabilities and the overall security posture of an IT systems. It is often more technical.
* Importance of audits & assessments:
* Identifying vulnerabilities
* Compliance requirements
* Incident response readiness
* Continuous improvement
* **Attestation** involves certifications from an organization confirming compliance with regulations and internal policies.

Internal

* **Self-Assessments** - Internal reviews conducted to evaluate compliance and security.
* Helps identify gaps and areas for improvement before external audits
* **Audit Committee** - A group responsible for overseeing the internal audit process.
* Reviews findings and ensures appropriate actions are taken.

External

* **Regulatory** - Audits conducted by regulatory bodies to ensure compliance.
* Can result in fines or sanctions if non-compliance is found.
* **Assessment** - Evaluations conducted to measure adherence to policies.
* **Independent 3rd Party Audit** - External audits conducted by independent firms to provide an unbiased evaluation of the organization's security posture.

Pen Testing

* Simulating an attack against the organization's System. Trying to **exploit** vulnerabilities.
* **Actively** assesses security.
* Similar to vulnerability scanning, except that we try to exploit the vulnerabilities.
* It often requires a signed authorization.
* **Physical** - Simulates attacks on physical security measures, such as surveillance systems.
* **Offensive** - Active attempts to exploit vulnerabilities.
* **Defensive** - Tests the organization's ability to detect and respond to attacks.
* Evaluates the effectiveness of monitoring and incident response measures.
* **Integrated** - Combines both offensive and defensive testing to provide a complete assessment.
* In an unknown environment (**black-box testing**), the pen tester has no idea of what the system looks like.
* In a known environment (**white-box testing**), the tester has full disclosure and knows what to test.
* In a partially known environment (**gray-box testing**), the tester has limited knowledge of the system and focuses apps.

Reconnaissance

* **Reconnaissance** is a phase where the pen tester gathers information before launching an attack.
* **Passive Reconnaissance** —- Gathering information without interacting directly with the target.
* Searching public records and using open-source intelligence (OSINT)
* **Active Reconnaissanc**e — Direct interaction with the target to gather information.
* Network scanning and social engineering.

**5.6 Security Awareness**

* **Phishing** 
  + Campaigns
  + Recognizing a phishing attempt
  + Responding to reported suspicious messages
* **Anomalous behavior recognition** 
  + Risky
  + Unexpected
  + Unintentional
* **User guidance and training** 
  + Policy/handbooks
  + Situational awareness
  + Insider threat
  + Password management
  + Removable media and cables
  + Social engineering
  + Operational security
  + Hybrid/remote work environments
* **Reporting and monitoring** 
  + Initial
* **Recurring**
* **Developmen**

Phishing

* It is a cyberattack that involves sending emails that appear to e from a legitimate source.
* The emails often contain a link that goes to a fake website that looks like the real website.
* Effects are data breach, identity theft, financial loss, reputation loss.
* Features of phishing:
  + Too good to be true
  + URLs, Attached Files
  + Urgency
  + Unsual Sender
  + Money involved

Prevent Phishing

* **Campaigns** - Conduct simulated phishing attacks to train employees on **recognizing and responding** to phishing attempts.
* Teach employees how to identify common signs of phishing
  + Suspicious email addresses
  + Spelling errors
  + Requests for personal information
  + Money involved
* Establish a clear procedure for **reporting** suspected phishing attempts.

Behavior Recognition

* **Risky Behavior** - Actions that pose a potential security risk
  + Downloading unauthorized software
  + Accessing restricted areas
* **Unexpected Behavior** - Monitoring unusual activities deviating from normal patterns.
  + Logging in from unfamiliar locations
  + Logging in at odd hours
* **Unintentional Behavior** -Accidental actions that could compromise security
  + Sending sensitive information to the wrong recipient
  + Mishandling confidential data

Prevent Phishing

* Provide **policies and handbooks** that outline security expectations.
* Train employees to be aware of their surroundings (**situational awareness**), both physical and digital.
* Educate employees about the risks posed by **insider threats** and how to detect them.
* Promote the use of **strong passwords** (complexity, length, age, etc.)
* Educate on the risks associated with using **removable media**.
* Train employees to **recognize social engineering** tactics
* Implement policies for **secure remote access** (working remotely or in hybrid settings).

Reporting & Monitoring

* **Initial Reporting** - Establish channels for employees to report suspicious activities.
* **Recurring Monitoring** - Continuously monitor for security incidents.
  + Regular reviews
  + Updates
  + Security awareness programs