Risk Management

Objective 5.2: Explain elements of the risk management process

- **Risk Management**
  - *Risk Management*
    - Fundamental process involving identification, analysis, treatment, monitoring, and reporting of risks
  - Risk Management Lifecycle
    - *Risk Identification*
      - Proactive process recognizing potential risks
      - Goal
        - Create a comprehensive list based on events hindering objectives
    - *Risk Analysis*
      - Evaluate likelihood and potential impact
      - Qualitative or quantitative methods
      - Outcome
        - Prioritized list for guiding risk treatment
    - *Risk Treatment*
      - Develop strategies
        - Avoidance
        - Reduction
        - Sharing
        - Acceptance

- Strategy choice based on potential impact and risk tolerance
- Goal
  - Reduce potential impact to an acceptable level

■ *Risk Monitoring*

- Ongoing process tracking identified risks
- Monitor residual risks, identify new risks, and review risk management effectiveness
- Ensures dynamic responsiveness to organizational changes

■ *Risk Reporting*

- Communicate risk information and effectiveness of risk management to stakeholders
- Various forms
  - Dashboards
  - Heat Maps
  - Detailed Reports
- Crucial for accountability and informed decision-making

○ Risk Assessment Frequency

■ Types

- Ad-hoc
- Recurring
- One-time
- Continuous

■ Varies

- Based on organization nature and types of risks involved

- Risk Identification
  - Process
    - Identify potential risks; perform business impact analysis.
  - Concepts
    - Recovery Time Objective
    - Recovery Point Objective
    - Mean Time to Repair
    - Mean Time Before Failure
- *Qualitative Risk Analysis*
  - Assess and prioritize risks based on likelihood and impact
- *Quantitative Risk Analysis*
  - Numerically estimate probability and potential impact
- Risk Management Strategies
  - Types
    - Risk Transfer
    - Risk Acceptance
    - Risk Avoidance
    - Risk Mitigation
- Risk Monitoring and Reporting
  - Crucial Steps
    - Continuous tracking and regular reporting
  - Long-Term Impact
    - Significant for the effectiveness of the risk management process

- **Risk Assessment Frequency**
  - *Risk Assessment Frequency*
    - Regularity with which risk assessments are conducted within an organization
  - Four main types of risk assessment frequencies
    - *Ad-Hoc Risk Assessments*
      - Conducted as needed, often in response to specific events or situations
      - Address potential new risks or changes in existing risks
    - *Recurring Risk Assessments*
      - Conducted at regular intervals (e.g., annually, quarterly, monthly)
      - Part of standard operating procedures for continual risk identification and management
    - *One-Time Risk Assessments*
      - Conducted for specific projects or initiatives
      - Not repeated, associated with a particular purpose
    - *Continuous Risk Assessments*
      - Ongoing monitoring and evaluation of risks
      - Enabled by technology, involving real-time data collection and analysis
      - Used for proactive threat and vulnerability monitoring, facilitating quick responses

- **Risk Identification**
  - *Risk Identification*
    - Crucial first step in risk management
    - Involves recognizing potential risks that could impact an organization
    - Risks can vary from financial and operational to strategic and reputational

- Techniques
  - Brainstorming
  - Checklists
  - Interviews
  - Scenario Analysis
- Organization should consider a wide range of risks, including operational, financial, strategic, and reputational risks
- Document and analyze risks based on impact and likelihood

- *Business Impact Analysis (BIA)*
  - Evaluates effects of disruptions on business functions
  - Identifies and prioritizes critical functions
  - Assesses impact of risks on functions
  - Determines required recovery time for functions
  - Key Metrics in BIA
    - *Recovery Time Objective (RTO)*
      - Maximum acceptable time before severe impact
      - Target time for restoring a business process
    - *Recovery Point Objective (RPO)*
      - Maximum acceptable data loss measured in time
      - Point in time data must be restored to
    - *Mean Time to Repair (MTTR)*
      - Average time to repair a failed component or system
      - Indicator of repair speed and downtime minimization
    - *Mean Time Between Failures (MTBF)*
      - Average time between system or component failures
      - Measure of reliability

- **Risk Register**
  - *Risk Management*
    - Crucial for projects and business, it involves the identification and assessment of uncertainties that may impact objectives
  - *Risk Register*
    - Records identified risks, descriptions, impacts, likelihoods, and mitigation actions
    - Key tool in risk management
    - May resemble a heat map risk matrix
    - Facilitates communication and risk tracking
    - Key component of project and business operations
  - Components of Risk Register
    - *Risk Description*
      - Identifies and describes the risk
      - Clear and concise description
    - *Risk Impact*
      - Potential consequences of risk occurrence
      - Rated on a scale (e.g., low, medium, high)
    - *Risk Likelihood*
      - Probability of risk occurrence
      - Rated on a scale (e.g., numerical or descriptive)
    - *Risk Outcome*
      - Result of the risk if it occurs
      - Related to impact and likelihood
    - *Risk Level or Threshold*
      - Determined by combining the impact and likelihood

- Prioritizes risks (e.g., high, medium, low)

- *Cost*
  - Financial impact on the project
  - includes potential expenses if it occurs or the cost of risk mitigation

- Risk Tolerance and Risk Appetite
  - *Risk Tolerance/Risk Acceptance*
    - An organization or individual's willingness to deal with uncertainty in pursuit of their goals
    - Maximum amount of risk they are willing to accept
    - Acceptance without countermeasures
  - *Risk Appetite*
    - Willingness to pursue or retain risk
    - Types
      - Expansionary
      - Conservative
      - Neutral

- *Key Risk Indicators (KRIs)*
  - Predictive metrics signaling increasing risk exposure
  - Provide early warning of potential risks
  - Tied to the organization's objectives
  - Used to monitor risk changes and take proactive steps

- *Risk Owner*
  - Responsible for managing the risk
  - Monitors, implements mitigation actions, and updates Risk Register
  - Accountable for risk management

- **Qualitative Risk Analysis**
  - *Qualitative Risk Analysis*
    - Primary method in risk management
    - Assesses risks based on potential impact and likelihood
    - Categorizes risks as high, medium, or low
    - Subjective and relies on expertise and experience
    - Avoids quantitative complexity
  - Key Components
    - *Likelihood/Probability*
      - Chance of risk occurrence
      - Qualitatively expressed as low, medium, or high
      - Based on past experience, statistical analysis, or expert judgment
    - *Impact*
      - Potential consequences if risk occurs
      - Qualitatively rated as low, medium, or high
      - Assess damage to project or business objectives
      - Impact Levels
        - *Low Impact*
          - Minor damage, essential functions operational
        - *Medium Impact*
          - Significant damage, loss to assets
        - *High Impact*
          - Major damage, essential functions impaired

- **Quantitative Risk Analysis**
  - *Quantitative Risk Analysis*
    - Provides objective and numerical evaluation of risks
    - Used for financial, safety, and scheduling decisions
    - Utilizes key components
      - Single Loss Expectancy (SLE)
      - Exposure Factor (EF)
      - Annualized Rate of Occurrence (ARO)
      - Annualized Loss Expectancy (ALE)
  - Key Components
    - *Exposure Factor (EF)*
      - Proportion of asset lost in an event (0% to 100%)
      - Indicates asset loss severity
    - *Single Loss Expectancy (SLE)*
      - Monetary value expected to be lost in a single event
      - Calculated as Asset Value x Exposure Factor (EF)
    - *Annualized Rate of Occurrence (ARO)*
      - Estimated frequency of threat occurrence within a year
      - Provides a yearly probability
    - *Annualized Loss Expectancy (ALE)*
      - Expected annual loss from a risk
      - Calculated as SLE x ARO

- **Risk Management Strategies**
    - Four primary risk management strategies
        - *Risk Transference*
            - Shifts risk to another party
            - Common methods
                - Insurance
                - *Contract indemnity clauses*
                    - A contractual agreement where one party agrees to cover the other's harm, liability, or loss stemming from the contract
            - Doesn't remove the risk
                - Shifts the responsibility for handling the risk's financial consequences
        - *Risk Acceptance*
            - Acknowledge and deal with risk if it occurs
            - Used when cost of managing the risk outweighs potential loss or risk is unlikely to have a significant impact
            - No actions to mitigate the risk are taken
            - Methods
                - Exemption (excludes party from a rule)
                    - The organization doesn't have to obey a specific rule or requirement
                    - There is no risk of not complying with the rule or requirement
                    - There may be a benefit or mitigation offered by the rule or requirement which exempted organizations won't receive

because they are exempt

- Exception (allows party to avoid rule under specific conditions)

- In both Exemption and Exception, the organization assumes risk either by operating without the safeguards or mitigations offered by a rule (exemption), or by operating in a way that lets them evade the risk (exception).

- *Risk Avoidance*
  - Change plans or strategies to eliminate a specific risk
  - Chosen when the risk is too great to accept or transfer
- *Risk Mitigation*
  - Take steps to reduce likelihood or impact of risk
  - Common strategy involving various actions

- **Risk Monitoring and Reporting**
  - *Risk Monitoring*
    - Process of
      - Tracking identified risks
      - Monitoring residual risks
      - Identifying new risks
      - Evaluating risk response plans
    - Involves ongoing tracking of risks and their response actions
    - Helps determine Residual Risk and Control Risk
      - *Residual Risk*
        - The likelihood and impact of the risk after mitigation, transference, or acceptance measures have been taken on the initial risk

- *Control Risk*
    - Assessment of how a security measure has lost effectiveness over time

- *Risk Reporting*
    - Communicating information about risk management activities to stakeholders
    - Includes results of risk identification, assessment, response, and monitoring
    - Often presented in the form of a risk report
- Risk Monitoring and Reporting are essential for
    - Informed decision making
        - Offer insights for informed decisions on resource allocation, project timelines, and strategic planning
    - Risk mitigation
        - Recognize when a risk is escalating so it can be mitigated before becoming an issue
    - Stakeholder communication
        - Assist in setting expectations and showing effective risk management
    - Regulatory compliance
        - Demonstrate compliance with these regulations

Third-party Vendor Risks

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 2.3 - Explain various types of vulnerabilities
- 5.3 - Explain the processes associated with third-party risk assessment and management

- **Third-party Vendor Risks**
    - *Third-party Vendor Risks*
        - Potential security and operational challenges from external collaborators
        - Scope
            - Encompasses vendors, suppliers, or service providers
        - Risks
            - Impact on integrity, data security, and overall business continuity
    - Common Threat Vectors and Attack Surfaces
        - *Threat Vectors*
            - Paths attackers use to gain access
        - *Attack Surfaces*
            - Points where an unauthorized user can try to enter
    - Various Types of Vulnerabilities
        - *Hardware Vulnerabilities*
            - Components with vulnerabilities
        - *Software Vulnerabilities*
            - Applications with hidden backdoors
        - *Operational Vulnerabilities*
            - Lack of cybersecurity protocols

- Vendor Assessments
  - Evaluation
    - Pre-partnership assessment
  - Penetration Testing
    - Testing vendor security
  - Audit Rights
    - Right to audit vendors
  - Evidence Collection
    - Internal and external audit evidence
- Vendor Selection and Monitoring
  - Importance
    - Meticulous selection process
  - Vigilance
    - Ongoing monitoring of vendor performance
- Contracts and Agreements
  - Basic Contracts
    - Forming relationships
  - Nuanced Agreements
    - SLAs, MOUs, NDAs for specific safeguards

- **Supply Chain Risks**
  - Hardware Manufacturers
    - Products like routers and switches are composed of many components from various suppliers
    - Component tampering or untrustworthy vendors can introduce vulnerabilities
    - Rigorous supply chain assessments needed to trace origins and component

integrity

- Trusted foundry programs ensure secure manufacturing

- Secondary/Aftermarket Sources
  - Risk of acquiring counterfeit or tampered devices
  - Devices may contain malware or vulnerabilities
  - Budget-friendly but high-risk option
- Software Developers/Providers
  - Software developers and software providers are integral cogs in the supply chain
    - However, software can introduce vulnerabilities
  - Check for proper licensing, authenticity, known vulnerabilities, and malware
  - Open-source software allows source code review
  - Proprietary software can be scanned for vulnerabilities
- Service Providers/MSPs
  - *Managed Service Providers*
    - Organizations that provide a range of technology services and support to businesses and other clients
  - Security challenges with Software-as-a-Service (SaaS) providers
    - Data confidentiality and integrity concerns
    - Assess provider's cybersecurity protocols and support for security incidents
    - Vendor selection should consider due diligence, historical performance, and commitment to security
  - Considerations
    - Evaluate data security measures
    - Ensure confidentiality and integrity
    - Assess cybersecurity protocols

- Response to a security breach

- **Supply Chain Attacks**
  - *Supply Chain Attacks*
    - An attack that targets a weaker link in the supply chain to gain access to a primary target
    - Exploit vulnerabilities in suppliers or service providers to access more secure systems
  - *CHIPS Act of 2022*
    - U.S. federal statute providing funding to boost semiconductor research and manufacturing in the U.S.
    - Aims to reduce reliance on foreign-made semiconductors, strengthen the domestic supply chain, and enhance security
    - *Semiconductors*
      - Essential components in a wide range of products, from smartphones and cars to medical devices and defense systems
  - Safeguarding Against Supply Chain Attacks
    - Vendor Due Diligence
      - Rigorous evaluation of vendor cybersecurity and supply chain practices
    - Regular Monitoring & Audits
      - Continuous monitoring and periodic audits of supply chains to detect suspicious activities
    - Education and Collaboration
      - Sharing threat information and best practices within the industry
      - Collaborating with organizations and industry groups for joint defense

        - Incorporating Contractual Safeguards
            - Embedding cybersecurity clauses in contracts with suppliers or service providers
            - Ensuring adherence to security standards with legal repercussions for non-compliance

- **Vendor Assessment**
    - *Vendor Assessments*
        - Process to evaluate the security, reliability, and performance of external entities
        - Crucial due to interconnectivity and potential impact on multiple businesses
    - Entities in Vendor Assessment
        - *Vendors*
            - Provide goods or services to organizations
        - *Suppliers*
            - Involved in production and delivery of products or parts
        - *Managed Service Providers (MSPs)*
            - Manage IT services on behalf of organizations
    - Penetration Testing of Suppliers
        - *Penetration Testing*
            - Simulated cyberattacks to identify vulnerabilities in supplier systems
        - Validates supplier's cybersecurity practices and potential risks to your organization
    - *Right-to-Audit Clause*
        - Contract provision allowing organizations to evaluate vendor's internal processes for compliance
        - Ensures transparency and adherence to standards

- *Internal Audits*
  - Vendor's self-assessment of practices against industry or organizational requirements
  - Demonstrates commitment to security and quality
- *Independent Assessments*
  - Evaluations conducted by third-party entities without a stake in the organization or vendor
  - Provides a neutral perspective on adherence to security or performance standards
- *Supply Chain Analysis*
  - Assessment of an entire vendor supply chain for security and reliability
  - Ensures integrity of the vendor's entire supply chain, including sources of parts or products

- **Vendor Selection and Monitoring**
  - Vendor Selection Process
    - Similar to hiring a team member
    - Due diligence
      - A rigorous evaluation that goes beyond surface-level credentials
      - Includes the following
        - Evaluating financial stability
        - Operational history
        - Client testimonials
        - On-the-ground practices to ensure cultural alignment
    - Check for conflicts of interest that could bias the selection process

- *Vendor Questionnaires*
  - Comprehensive documents filled out by potential vendors
  - Vendor questionnaires provide insights into operations, capabilities, and compliance
  - Standardized criteria for fair and informed decision-making
- *Rules of Engagement*
  - Guidelines for interaction between organization and vendors
  - Cover communication protocols, data sharing, and negotiation boundaries
  - Ensure productive and compliant interactions
- *Vendor Monitoring*
  - Mechanism used to ensure that the chosen vendor still aligns with organizational needs and standards
  - Performance reviews assess deliverables against agreed-upon standards and objectives
  - *Feedback loops*
    - Involve a two-way communication channel where both the organization and the vendor share feedback

- **Contracts and Agreements**
  - Types of Contracts and Agreements
    - *Basic Contract*
      - Versatile tool that formally establishes a relationship between two parties
      - Defines roles, responsibilities, and consequences for non-compliance
      - Specifies terms like payment structure, delivery timelines, and product specifications

- *Service Level Agreement (SLA)*
  - Defines the standard of service a client can expect from a provider
  - Includes performance benchmarks and penalties for deviations
- Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU)
  - *MOA*
    - Formal, outlines specific responsibilities and roles
  - *MOU*
    - Less binding, expresses mutual intent without detailed specifics
- *Master Service Agreement (MSA)*
  - Covers general terms of engagement across multiple transactions
  - Used for recurring client relationships, supplemented by Statements of Work
- *Statement of Work (SOW)*
  - Specifies project details, deliverables, timelines, and milestones
  - Provides in-depth project-related information
- *Non-Disclosure Agreement (NDA)*
  - Ensures confidentiality of sensitive information shared during negotiations
  - Commitment to privacy, protecting proprietary data
- *Business Partnership Agreement (BPA) or Joint Venture Agreement (JV)*
  - Goes beyond basic contracts when two entities collaborate
  - Outlines partnership nature, profit-sharing, decision-making, and exit strategies
  - Defines ownership of intellectual property and revenue distribution