Module-4

Incident Management

Risk Assessment

- Risk Assessment
  - Risk Overview
  - Risk Identification
  - Risk Analysis
  - Risk Treatment
  - Risk Management Feedback Loops
  - Risk Monitoring
- Security incident management
- Third party security management
- Incident Components, Roles

Risk Overview

- **Risk:**
  - A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.

Risk Overview

- **Risk assessments:**
  - whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk.

Risk Overview

- **Risk assessments:**
  - All risk assessments generally include the following elements.
    - Identifying threats that could harm and, thus, adversely affect critical operations and assets.
    - Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.

Risk Overview

- **Risk assessments Steps:**
  - **Step** 1: Identify the hazards.
  - **Step** 2: Decide who might be harmed and how.
  - **Step** 3: Evaluate the **risks** and decide on precautions.
  - **Step** 4: Record your findings and implement them.
  - **Step 5**: Review your **assessment** and update if necessary.

Risk Overview

- **Risk assessments:**
  - Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
  - Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.

Risk Overview

- **Risk assessments:**
  - Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs. Identifying cost-effective actions to mitigate or reduce the risk.
  - These actions can include implementing new organizational policies and procedures as well as technical or physical controls.

Risk Overview

- **Risk assessments:**
  - Documenting the results and developing an action plan.
  - There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors.
  - In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified.

Risk Overview

- **Risk assessments:**
  - A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on
    1. the likelihood that a damaging event will occur,
    2. the costs of potential losses, and
    3. the costs of mitigating actions that could be taken.

Risk Overview

- **Risk assessments:**
  - When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low.
  - In this regard, qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment.
  - It is also possible to use a combination of quantitative and qualitative methods.

Risk Identification

- It is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.
- It includes documenting and communicating the concern.
- The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on the project's ability to achieve performance or capability outcome goals.
- They may come from within the project or from external sources.

Risk Identification

- There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty.
- Risk identification needs to match the type of assessment required to support risk- informed decision making.

Risk Identification

- For an acquisition program, the first step is to identify the program goals and objectives, thus fostering a common understanding across the team of what is needed for program success.
- This gives context and bounds the scope by which risks are identified and assessed.

Risk Identification

- There are multiple sources of risk.
- For risk identification, the project team should review the program scope, cost estimates, schedule (to include evaluation of the critical path), technical maturity, key performance parameters, performance challenges, stakeholder expectations vs. current plan, external and internal dependencies, implementation challenges, integration, interoperability, supportability, supply-chain vulnerabilities, ability to handle threats, cost deviations, test event expectations, safety, security, and more.
- In addition, historical data from similar projects, stakeholder interviews, and risk lists provide valuable insight into areas for consideration of risk.

Risk Identification

- Risk identification is an iterative process. As the program progresses, more information will be gained about the program (e.g., specific design), and the risk statement will be adjusted to reflect the current understanding.
- New risks will be identified as the project progresses through the life cycle.

Risk Analysis

- This is the next step in the risk assessment program, Risk Analysis, requires an entity to, conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected information held by the entity.
- In other words, Risk analysis, which is a tool for risk management, is a method of identifying vulnerabilities and threats, and assessing the possible damage to determine where to implement security safeguards.

Risk Analysis

- **Risk Analysis steps:**
  1. Identify the scope of the analysis.
  2. Gather data.
  3. Identify and document potential threats and vulnerabilities.
  4. Assess current security measures.
  5. Determine the likelihood of threat occurrence.
  6. Determine the potential impact of threat occurrence.
  7. Determine the level of risk.
  8. Identify security measures and finalize documentation.

Risk Analysis

- **A risk analysis has four main goals:**
  1. Identify assets and their values
  2. Identify vulnerabilities and threats
  3. Quantify the probability and business impact of these potential threats
  4. Provide an economic balance between the impact of the threat and the cost of the countermeasure

Risk Analysis

- **Risk Evaluation**
  - The risk evaluation process receives as input the output of risk analysis process.
  - It compares each risk level against the risk acceptance criteria and prioritize the risk list with risk treatment indications.