WOA7017: Security Risk Analysis and Evaluation - Expanded Study Notes

Instructor: Prof. Ts. Dr. Omar Zakaria *(Contact: 012-9180186, manafzack@gmail.com)*

Week 2: Information Security Risk Assessment Basics - The Process

- **Focus:** This week outlines the typical phases involved in conducting an SRA, providing a structured approach from initiation to reporting.

Phase 1: Project Definition

- **Goal:** To establish clear expectations, boundaries, and resources for the assessment *before* it begins. Prevents misunderstandings and scope creep.
    - **Project Scope:** Define precisely what systems, locations, assets, and processes are *included* and *excluded*. Document this agreement.
    - **Budget:** Allocate sufficient funds and estimate the timeframe. This influences the depth (rigor) and breadth of the assessment.
    - **Tasks:** Break the assessment into manageable steps (e.g., data gathering, analysis, reporting) and assign resources (people, tools).
    - **Objective:** Reiterate the primary goal – usually analyzing control effectiveness against threats to specific assets.
    - **Assessment Boundaries:** Clearly define the limits – e.g., "Assess the customer database server and its network segment, but not the connected marketing portal."

Phase 2: Project Preparation

- **Goal:** To gather necessary context, permissions, and preliminary information to enable efficient data collection and analysis.
    - **Team Preparation:** Select individuals with appropriate skills (technical, policy, business context) and formally introduce them to the organization being assessed (builds rapport).
    - **Project Preparation:**
        - **Obtain Permission:** Crucial! Get explicit, written authorization defining the scope of testing (especially for technical tests) and access granted.
        - **Review Business Mission:** Understand what the organization does, its critical functions, and strategic goals. Security exists to support the mission.
        - **Identify Critical Systems:** Focus efforts on the systems most vital to the business mission. (More detail in Week 4).
        - **Map Assets:** Create an initial inventory of key information assets associated with the critical systems.
        - **Identify Threats:** Brainstorm potential threats relevant to the organization and scope (e.g., malware, insider threat, natural disaster).
        - **Determine Expected Controls:** Based on best practices, regulations, and the organization's context, list the types of controls you would *expect* to find protecting the assets. This forms a baseline for comparison.

Phase 3: Data Gathering

- **Goal:** To collect detailed information about the existing security posture across administrative, technical, and physical domains. This is the evidence-gathering phase.
    - **Administrative:** Focuses on policies, procedures, and people-related controls.
        - *Methods:* Reviewing documents (security policy, BCP, incident response plan, training materials), interviewing staff (managers, users, HR), observing practices (e.g., onboarding/offboarding).
    - **Technical:** Focuses on technology-based controls.
        - *Methods:* Reviewing system configurations (firewalls, servers, databases), network architecture diagrams, security tool logs (IDS/IPS, SIEM), conducting security testing (vulnerability scans, limited penetration tests as agreed in scope).
    - **Physical:** Focuses on the security of the physical environment.
        - *Methods:* Reviewing physical access policies/procedures, observing access controls (doors, locks, guards), inspecting facilities (server rooms, wiring closets, fire suppression).

Phase 4: Risk Analysis

- **Goal:** To analyze the gathered data to identify vulnerabilities, link them to threats and assets, and determine the level of risk. This is where information becomes insight.
    - **Determine Risk Components:**
        - **Asset Valuation:** Assign value (qualitative or quantitative) to the identified assets based on their importance to the business (confidentiality, integrity, availability needs). Grouping similar assets can simplify this.
        - **Threat and Vulnerability Mapping:** Identify specific vulnerabilities (weaknesses found in Phase 3) and map them to relevant threats (identified in Phase 2) that could exploit them against specific assets. *Example: Threat (Malware) exploits Vulnerability (Unpatched OS) on Asset (Customer Database)*.
    - **Calculate Risk:** Estimate the likelihood (probability) of a threat exploiting a vulnerability and the potential impact (damage) if it occurs. Risk can be expressed qualitatively (High, Medium, Low) or quantitatively (e.g., Annual Loss Expectancy - ALE).
        - *Conceptual Formula:* Risk = Likelihood x Impact
    - **Create Risk Statements:** Clearly document each identified risk, including the asset, threat, vulnerability, existing controls (if any), likelihood, impact, and overall risk level. *Example: "High Risk: External attackers (Threat) could exploit an unpatched web server vulnerability (Vulnerability) to access the customer database (Asset), resulting in significant data breach costs and reputational damage (Impact), due to inconsistent patching (Control Weakness). Likelihood: Medium, Impact: High."*
    - **Obtain Team Consensus:** The assessment team should review and agree on the identified risks and their ratings to ensure objectivity and consistency.

Phase 5: Risk Mitigation

- **Goal:** To recommend specific controls (safeguards) to reduce the identified risks to an acceptable level.
    - **Safeguards (Controls):** Propose solutions tailored to the identified risks. Controls can be categorized by function:
        - **Preventative:** Aim to stop threats from succeeding (e.g., firewalls, access control lists, encryption, security awareness training).

        - **Detective:** Aim to identify threats or intrusions when they occur (e.g., Intrusion Detection Systems (IDS), security logs and monitoring, audits).
        - **Corrective:** Aim to fix problems and restore systems after an incident (e.g., backups and recovery procedures, incident response plans).
    - **Residual Security Risks:** After proposing controls, evaluate the risk that *remains*. It's rarely possible to eliminate all risk. This residual risk level must be understood by management for the final decision.

Phase 6: Risk Reporting and Resolution

- **Goal:** To communicate the findings and recommendations clearly to stakeholders and enable management to make informed decisions on risk treatment.
    - **Reporting:**
        - Develop a formal report summarizing the scope, methodology, findings (key risks), and recommended safeguards.
        - Tailor the report presentation for different audiences:
            - *Executive Summary:* High-level overview of major risks, potential business impact, and key recommendations for senior management.
            - *Management Report:* More detail on risks, control weaknesses, and proposed solutions for departmental managers.
            - *Technical Report:* In-depth findings, vulnerability details, and specific configuration recommendations for IT/security staff.
    - **Resolution:**
        - Management reviews the identified risks and recommendations.
        - For each significant risk, management must formally decide how to resolve it:
            - **Reduce Risk (Mitigate):** Implement the recommended controls (most common).
            - **Accept Risk:** Formally acknowledge the risk and decide not to implement controls (usually for low risks or where mitigation cost exceeds potential loss). Requires documented sign-off.
            - **Delegate/Transfer/Share Risk:** Shift the risk to a third party (e.g., buy insurance, outsource the function).
        - **Documentation:** All resolution decisions must be documented for accountability, tracking, and future audits.