WOA7017: Security Risk Analysis and Evaluation - Expanded Study Notes

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

Week 3: Project Definition (In Depth)

- **Focus:** This week dives deeper into the critical first phase – defining the project – emphasizing factors for success, scoping challenges, and the importance of a clear Statement of Work (SOW).

1. Ensuring Project Success: Success isn't just finishing; it's about delivering value. * **Success Definition Components:** * **Customer Satisfaction:** * *Identify the Customer(s):* Who requested the SRA? Who are the key stakeholders? (Security team, business managers, compliance, legal, IT ops). Understanding their needs and expectations is vital. * *Meet Expectations:* Deliver what was promised, communicate effectively, and provide actionable results relevant to their roles. * **Quality of Work:** * *General Report Expectations:* Clear, concise, well-organized, grammatically correct. * *Technical Report Expectations:* Accurate technical details, reproducible findings (where applicable), clear explanations. * *SRA Report Expectations:* Objective analysis, evidence-based findings, justifiable risk ratings, practical and prioritized recommendations, clear link between findings and business impact. * **Completion within Budget:** Adhere to the agreed-upon cost and timeframe through good planning and project management.

2. Setting the Budget: Accurately estimating cost and time is key. Factors include: * **Organisation Size:** Larger organizations usually mean more systems, users, locations = more effort. * **Geographic Separation:** Assessing multiple sites requires travel time and cost, potentially different environments. * **Complexity:** Highly interconnected, custom, or legacy systems require more time to understand and assess. * **Threat Environment:** Organizations facing sophisticated threats may require deeper, more rigorous testing. * **Culture:** An open, cooperative culture facilitates faster data gathering; a closed or resistant culture can slow things down.

3. Determining the Objective: * Reiterate the core goal: "Accurate analysis of the effectiveness of current security controls that protect organization’s assets." * The chosen **Risk Assessment Methodology** (e.g., NIST SP 800-30, ISO 27005, OCTAVE, FAIR) will guide the specific steps and analysis techniques used to achieve this objective.

4. Limiting the Scope & Identifying System Boundaries: Defining what's *in* and *out* is crucial. * **Dangers:** * **Underscoping:** Assessing too little, potentially missing critical risks in excluded areas. * **Overscoping:** Trying to assess too much, leading to delays, budget overruns, and potentially superficial analysis across the board. * **Logical Boundaries:** Justifiable reasons to exclude something from the scope: * *Not Security-Relevant:* The function has no bearing on information security (rare for IT systems, but possible for some processes). * *Covered Elsewhere:* Another assessment (e.g., a specific PCI DSS audit) is already addressing that function. Avoid duplication of effort. * *Beyond Team Skills:* The assessment team lacks the specialized expertise needed for a particular technology or system. * *Compensating Controls:* Strong physical or environmental controls might make certain technical threats non-relevant in a specific context (e.g., a system is fully air-gapped).

5. Specifying the Rigor: How deep should the analysis go? * **Definition:** Rigor refers to the depth, intensity, and level of detail in the assessment. * **Factors Determining Rigor:** * **Perceived Strength of Controls:** If controls are believed to be weak or untested, higher rigor might be needed. * **Maturity of Security Program:** Mature programs might require deeper dives; less mature ones might start with

broader, less intensive assessments. * **Criticality of Assets/Systems:** More critical systems warrant more rigorous assessment. * **Budget/Time Constraints:** Rigor is often constrained by available resources.

6. Sample Scope Statements: * *(Refer to textbook Table 3.1, page 61)* Good scope statements are specific, measurable, achievable, relevant, and time-bound (SMART). They clearly define inclusions, exclusions, and the depth of review.

7. Project Description: Formalizing the agreement, often via a Statement of Work (SOW). * **Project Variables:** Scope and rigor are the main variables influencing the price and timeline. * **Statement of Work (SOW):** A formal document outlining the agreement between the assessment team and the customer. Key elements: * **Service Description:** Clearly state what service is being provided (e.g., the definition of SRA: "A probability determination of asset losses..."). * **Scope of Security Controls:** Explicitly list the control categories covered (Administrative, Physical, Technical). * **Specifying Deliverables:** Detail *exactly* what will be produced (e.g., final report, executive presentation, vulnerability list). Be specific about recommendations – "add firewalls and DMZ" is better than "improve perimeter security." * **Contract Type:** * *Time and Materials (T&M):* Customer pays for hours worked and expenses. Flexible, but budget can be uncertain. * *Firm-Fixed Price (FFP):* A set price for the agreed scope. Budget certainty for the customer, but requires a very well-defined scope upfront. * **Contract Terms:** * *Needs Determination:* How customer needs were identified. * *Alternatives Considered:* Mentioning familiarity, specific methodology expertise (OCTAVE, CRAMM, FRAP etc.) can justify the chosen approach/team. * **Negotiating Project Membership:** Specifying the required skills or even named individuals for the assessment team can help ensure quality.

Week 4: Security Risk Assessment Preparation (In Depth)

- **Focus:** Expanding on Phase 2 (Preparation), detailing the practical steps needed before data gathering can effectively begin. This involves introductions, understanding the business context, and identifying key elements like systems, assets, threats, and expected controls.

1. Introduce The Team: First impressions matter. * **Purpose:** Build trust, establish communication channels, manage expectations, and ensure smooth cooperation. * **Methods:** * **Introductory Letter:** Formal communication including: Point of Contact (POC) for both sides, reference to the SOW/agreement, planned start/end dates, initial data requests (org charts, policies, network diagrams), access needs (physical access, system accounts), on-site requirements (workspace, network access). * **Pre-Assessment Briefing (Kick-off Meeting):** * *Introductions:* Team members introduce themselves and their roles. * *What to Expect:* Explain the assessment process, timeline, types of activities (interviews, scans, reviews), and potential disruptions (keep minimal). * *Not Always Quick:* Manage expectations about the time and effort required from the customer's staff. * *Team Needs:* Clearly state what information and access the team requires from the customer. * **Obtain Proper Permission:** Absolutely essential, especially for any active testing. * *Policies Required:* Adhere to the customer's security and access policies. * *Permission Required:* Get written sign-off authorizing the assessment activities. * *Scope of Permission:* The authorization must clearly state what systems can be tested, what methods are allowed (e.g., vulnerability scan vs. penetration test), and the timeframe. * *Accounts Required:* Specify necessary user accounts (e.g., read-only access, temporary admin rights if needed and approved). *(Refer to textbook Table 4.1, page 78 for examples)*.

2. Review Business Mission: Context is everything. * **What is it?** The organization's purpose, goals, primary activities, customers, and competitive advantages. * **Why Review?** Security controls should *enable* and *protect* the mission, not hinder it unnecessarily. Understanding the mission helps prioritize assets and

risks based on their impact on core business objectives. * **Obtaining Information:** Review websites, annual reports, strategic plans; interview key business managers. Understand the sensitivity/confidentiality of this mission information itself. * **Elements & Needs:** Link specific business activities (e.g., online sales, patient care, manufacturing) to required security properties (Confidentiality, Integrity, Availability - CIA). *(Refer to textbook Table 4.2, page 80 for detailed examples)*.

3. Identify Critical Systems: Focus the assessment effort where it matters most. * **Why Independent Consideration?** Each system supporting a critical function likely has unique data, dependencies, users, and associated risks. They can't always be lumped together. *(Refer to textbook Table 4.3, page 82)*. * **Determining Criticality Approaches:** * **Approach 1: Find Information Elsewhere:** Leverage existing Business Continuity Plans (BCP) or Disaster Recovery Plans (DRP), as these usually contain prioritized lists of critical systems based on business impact analysis (BIA). *Efficiency gain if available and current*. * **Approach 2: Create High-Level Information:** If no BCP/DRP exists, conduct a rapid, high-level BIA during preparation to identify the most critical systems based on input from business managers. *Less detailed but better than nothing*. * **Approach 3: Classify Critical Systems (Structured Method):** * *Determine Protection Requirements (CIA Needs):* Rate each system based on the impact of losing Confidentiality, Integrity, or Availability. Use a scale (e.g., High, Medium, Low) tied to potential impact (financial loss, operational disruption, reputational damage, legal issues). Example thresholds: High > RM1M loss, Medium RM100k-RM1M, Low < RM100k. * *Determine Mission Criticality:* Categorize systems based on their role in the business mission: * *Mission Critical:* Directly supports a core function; loss causes immediate, significant disruption; single source of vital data. * *Important:* Supports critical functions indirectly; backup data source; loss impacts business over time. * *Supportive:* Provides convenience or efficiency; loss is inconvenient but doesn't stop core operations. * *Define Critical Systems:* Combine protection requirements and mission criticality to formally designate systems as critical (e.g., systems rated High for Availability and Mission Critical). Categorize system types (Major applications, General support systems).

4. Identify Assets: What specifically needs protection within the critical systems? * **Methods:** Use checklists (general asset types like hardware, software, data, services, personnel, reputation) and judgment based on the business mission and critical systems. *(Refer to textbook Table 4.4: General Asset List, page 87)*. * **Asset Sensitivity/Criticality Classification:** Similar to systems, classify assets to prioritize protection. * **Approach 1: Find Information Elsewhere:** Reuse existing data classification schemes, asset inventories, or previous SRA results. *Verify currency and relevance*. * **Approach 2: Create High-Level Information:** Develop a simple classification scheme if none exists. * **Approach 3: Determine Asset Criticality:** Categorize based on relationship to critical systems: * *Critical Assets:* Essential for a critical system; no easy backup/alternative (e.g., the primary customer database). * *Important Assets:* Backup data, assets supporting important (but not critical) functions (e.g., development server). * *Supportive Assets:* Used for convenience, non-essential functions (e.g., archive data rarely accessed). * **Asset Valuation:** Determine the 'worth' of assets to justify protection efforts. * **Importance:** Needed for compliance, BCP, insurance claims, budgeting, risk calculations (impact side). Links asset loss to tangible/intangible organizational impact. * **Qualitative Approaches:** * *Binary:* Asset is valuable (Yes) or not (No). Very simple. * *Classification-based:* Assign value based on category (e.g., Critical=High Value, Important=Medium, Supportive=Low). Common and practical. * *Rank-based:* Order assets from most to least valuable relative to each other. Good for prioritization. *(Refer to textbook Table 4.7, page 93)*. * *Consensus:* A group of knowledgeable stakeholders agrees on the relative value or category. Uses collective expertise. * *(Note: Quantitative valuation assigns a specific monetary value, which can be difficult but powerful if achievable)*.

5. Identify Threats: What adverse events or actors could harm the assets? * **Purpose:** Bounds the assessment by focusing on relevant potential causes of harm. Helps scope (e.g., focus on insider threats vs. nation-state actors based on context). * **Threat Components:** * *Threat Agent/Source:* The entity initiating the threat (e.g., disgruntled employee, hacker group, earthquake, software bug, hardware failure). * *Undesirable Event/Threat Action:* What the agent does (e.g., unauthorized access, data modification, denial of service, system destruction). * **Listing Possible Threats:** Brainstorm based on industry knowledge, threat intelligence, organizational history, geographic location. Use checklists. Pair agents with potential events. *(Refer to textbook Table 4.11, page 100 for pairings)*. * **Threat Statements:** Clearly articulate potential threats. *Format: [Threat Source] could cause [Undesirable Event] impacting [Asset(s)]. (Refer to textbook Figure 4.1, page 101)*. * **Validating Threat Statements:** Prioritize threats based on relevance and likelihood. Consider: * *History:* Has this happened before (internally or to similar organizations)? * *Environmental Factors:* Location (earthquakes, floods), industry (targeted attacks). * *Business Factors:* Type of data handled (financial, health), online presence. Focus on plausible, relevant threats.

6. Determine Expected Controls: What security measures *should* reasonably be in place? * **Prerequisites:** Requires understanding the business, identified assets, and relevant threats. * **Purpose:** Establishes a baseline or benchmark against which existing controls (found in Phase 3) will be compared during the analysis (Phase 4). Helps identify gaps. * **Consider Expectations Based On:** * **Security Policy:** What controls does the organization's own policy mandate? (e.g., password complexity, background checks, encryption standards). * **Security Organization:** Is there a dedicated security function? Does it have adequate authority, resources, and skilled staff to implement and manage controls effectively? * **Security Procedures:** Are there documented, adequate procedures for key security processes (e.g., change management, incident handling, access reviews, vulnerability management)?

Study Tips for Revision:

- **Understand Definitions:** Be clear on the definitions of key terms: Risk, Asset, Threat, Vulnerability, Control (Preventative, Detective, Corrective), Residual Risk, SRA, Audit, Pen Test, etc.
- **Know the Process:** Understand the purpose and key activities of each of the 6 SRA phases. How does one phase lead into the next?
- **Focus on Relationships:** How do assets, threats, vulnerabilities, and controls relate to each other in determining risk? How does asset valuation influence control selection? How does business mission drive criticality?
- **Distinguish Concepts:** Be able to clearly explain the difference between an SRA, a gap assessment, a compliance audit, and a penetration test.
- **Why is it Done?** Understand the *reasons* for performing an SRA (compliance, risk reduction, budget justification) and the *benefits* (awareness, communication, baseline).
- **Quality Matters:** Why is a *quality* SRA important, and what makes an assessment weak?
- **Use Examples:** Think of practical examples for different types of threats, vulnerabilities, assets, and controls.
- **Context is Key:** Remember that SRA is not done in isolation; it must consider the specific organization's business mission, environment, and resources.