Class Notes: WOA7017 Security Risk Analysis & Evaluation

Week 3 Summary

Lecturer: Prof. Omar Zakaria **Date:** Thursday, 3 April 2025 **Time:** 18:00 Malaysia Time

Customers of Security Risk Assessment

- A security risk assessment serves various stakeholders ("customers") within an organisation. Understanding their needs is crucial for a successful assessment.
- **Key Customer Types:**
    - **End Users:** (Briefly mentioned in relation to control usability) Security controls proposed (like access controls) must be practical and not overly burdensome.
        - Example: Requiring key card access at *every* single door might lead users to bypass controls (e.g., propping doors open) due to inconvenience. Balance security needs with user workflow.
    - **Compliance Officer / Legal Department:**
        - Risk assessments are often **legal or regulatory requirements** for specific industries (e.g., healthcare, financial institutions, government agencies).
        - These departments ensure the organisation complies with relevant laws, regulations, and contractual obligations.
        - Example (Financial Institutions): **Bank Negara Malaysia (BNM)** mandates specific regulations, such as conducting **Disaster Recovery Planning (DRP) testing twice a year**. Any security improvements must align with these requirements.
        - Example (Software): Ensuring compliance with **software licensing** (e.g., obtaining site licenses for proprietary software installed on multiple machines) falls under legal/compliance purview.
    - **Technicians, Operators, and Administrators:**
        - These are the individuals responsible for **maintaining and operating** security controls daily.
        - Their involvement is vital because they perform **troubleshooting**, manage **system availability** (often working in shifts, e.g., 24/7 ATM operation), and handle critical operational tasks.
        - Example (Backup Tapes): Assessing the process for handling backup tapes involves understanding:
            - **Staff rotation:** Who handles the tapes? Is there a clear schedule (**duty roster**)?
            - **Tracking:** Can you trace who took which tape, when, and where (from HQ to backup site)?
            - **Accountability:** Clear roles and responsibilities are needed for audit trails and incident investigation.
        - Need to monitor their adherence to **Standard Operating Procedures (SOPs)** for tasks like backups, virus checks, configurations.

        - The assessment should evaluate if current SOPs are effective and aligned with security standards, or if they need improvement.

Quality of Work in Risk Assessment Projects

- The success of a risk assessment project is heavily judged by the **quality of its deliverables**, primarily the technical reports.
- **Structured Approach:** A good assessment follows a structured plan (e.g., an audit plan) covering content, process, scope (areas, functions, departments).
- **Flexibility & Adaptability:**
    - Real-world assessments require flexibility. Schedules might need adjustment.
    - Example: If a top management interview is scheduled but the manager becomes unavailable, the assessment team should **reorganise the agenda** (e.g., swap with a later activity) rather than losing time.
    - Example: If a planned visit to a backup site (e.g., in Cyberjaya) needs rescheduling by the site, the team must adjust the day's plan to fill the time productively.
- **Focus on Results:** Customers ultimately judge the project's success based on tangible outcomes and the effectiveness of proposed solutions.
    - Example: If proposing **biometrics** for staff attendance to prevent buddy-punching, the *result* (reduced unauthorized clock-ins, effective control) is the measure of success. Proposed controls should be **effective** and justifiable.

Quality Aspects of Assessment Reports

- Reports (technical or otherwise) must meet general quality standards.
- **General Quality Aspects:**
    - **Grammar:** Clear, correct, and professional language.
    - **Visual Presentation:** Consistent formatting (fonts, headings, bullets), appropriate use of tables/figures, clear spacing, headers/footers. A well-formatted report is easier to read and understand.
    - **Audience:** Tailor the language and level of detail to the intended reader.
    - **Understanding the Topics:** The report must demonstrate the assessment team's grasp of the relevant technical and business context.
- **Specific Report Components:**
    - **Executive Summary:** High-level overview for management.
    - **Technical Appendices:** Detailed findings, supporting data.
    - **Supporting Evidence:** Audit logs, vulnerability scan results, configuration details.
    - **References:** Citations, links to policies.
    - **Resolution Description:** Recommended actions.
    - **Calculations:** Risk calculations, cost-benefit analysis.
- **Assessment Team's Role:**
    - The team isn't there to "find mistakes" like police, but to **verify compliance** with established policies, procedures, and instructions.
    - The goal is to identify gaps and recommend improvements to reduce security incidents by ensuring procedures are followed.

  - Requires understanding the assessed systems/processes (e.g., knowing the student lifecycle from admission to alumni for a student information system assessment).

The Critical Role of Objective Evidence (O.E.)

- **Objective Evidence** is paramount for credible and actionable assessment findings. It is factual, specific, and verifiable.
- **Subjective vs. Objective:**
  - **Subjective (Weak):** "Some staff are not practising lock screen on their monitors." (General, vague, easily disputed).
  - **Objective (Strong):** "Staff member **Ali** from the **IT department** did not implement lock screen on his monitor at [Time/Date]. This violates **Security Policy Clause 8.1.1**, which requires lock screens when leaving the workplace." (Specific person, department, action, policy violation, clause number).
- **Importance of O.E.:**
  - Provides **clear, undeniable proof** of a finding.
  - Makes findings **difficult to argue against** during closing meetings.
  - Leads to **acceptance** of findings and commitment to remediation.
  - Satisfies stakeholders (managers, security officers) who need concrete details.
  - Forms the basis for effective **resolutions** and recommendations.
- **Gathering O.E.:** Involves observation, reviewing logs, checking configurations, referencing specific policy clauses.

Project Management: Completion Within Budget

- Risk assessment projects operate under **time and budget constraints**.
- **Effective Management:** The project leader must manage resources carefully to complete the assessment **on time** and **within the allocated budget**.
- **Consequences of Overruns:**
  - Projects significantly exceeding time or budget may be **cancelled** or completed too late to be impactful.
  - Significant overruns often indicate **project team inexperience** or poor planning.
- **Audit Plans & Scheduling:**
  - Detailed plans (like the BSI audit plan example shown) allocate specific time slots for activities across multiple auditors.
  - Auditors are expected to adhere to the schedule, demonstrating professionalism and efficiency. Requires careful time management and potential adjustments within the overall timeframe.
  - Example: Completing a 2-day audit requires finishing all planned activities within those two days.
- **Man-Day Calculation:**
  - Audit costs are often calculated based on **man-days** (or person-days).
  - Example Calculation: 3 auditors working for 1 full day = 3 man-days. 3 auditors working for a half-day = 1.5 man-days. Total for 1.5 days = 4.5 man-days.
  - Clients are billed based on this, so the planned work must align with the calculated man-days.

Setting the Budget: Factors Influencing Cost

- Several factors determine the cost (and required effort/man-days) of a security risk assessment:
  - **Organisation Size:** Crucially, this refers to the number of employees **within the scope** of the assessment, not necessarily the total number of employees in the entire organisation.
  - **Geographical Separation:** Assessing multiple locations (e.g., HQ in Damansara and a backup site in Cyberjaya) increases complexity and cost (travel, time).
  - **Complexity:**
    - The intricacy of the systems, processes, and network infrastructure being assessed.
    - More interconnected systems, multiple dependencies, or non-standard setups increase complexity and cost.
  - **Threat Environment:** The types and severity of threats the organisation faces. Assessing against more sophisticated or unusual threats (e.g., terrorism vs. common malware) may require more effort.
  - **Culture:** The organisation's internal culture can impact security implementation and assessment.
    - Example (UPNM): Having distinct military and civilian security personnel creates unique cultural and operational considerations for physical security compared to an organisation with only civilian guards.
    - Example (Banking): Different banks (Maybank, CIMB) have slightly different cultures, approaches to mobile banking security, and operational nuances.

Determining Assessment Benefits and Objectives

- A security risk assessment provides several benefits:
  - A basis for **risk-based security spending**.
  - A mechanism for **periodic review** of the security program's effectiveness.
  - A system of **checks and balances** for protecting sensitive data.
- **Clear Objectives:** Both the assessment team and the client (auditee) must understand the specific objectives of the assessment.
- **Example Objectives (from Audit Plan):**
  - **Determine Conformity:** Verify that the Information Security Management System (ISMS) meets the requirements of the audit criteria (e.g., ISO 27001 standard), potentially leading to certification.
  - **Meet Requirements:** Ensure the organisation's ability to meet applicable legal, regulatory, and contractual requirements.
  - **Determine Effectiveness:** Evaluate if the ISMS effectively achieves the organisation's stated security objectives, often linked to the **Statement of Applicability (SOA)** which lists the implemented security controls.

Assessment Methodology and Verification

- Risk assessments employ various methods to gather information:
  - **Document Review:** Examining policies, procedures, logs, reports, licenses.
  - **Interviews:** Talking to management, staff, technicians.

  - **Observation:** Watching processes in action, physically inspecting controls (e.g., checking lock screens, fire extinguishers).
- **Verification is Key:** Claims made during interviews or found in documents must be verified through other means.
  - Example: If staff claim they always use lock screens, **observe** their actual behaviour.
  - Example: If an organisation claims software is licensed, ask to **see the licenses**.
  - Example: If fire extinguishers are claimed to be maintained, **physically check** the inspection tags/dates on the extinguishers.
- Combining multiple methods provides a more **accurate analysis** of control effectiveness.

Limiting the Scope: Boundaries and Exclusions

- Clearly defining the scope is essential to avoid **underscoping** (doing too little work for the agreed fee/effort) or **overscoping** (doing more work than planned/budgeted).
- **Audit/Assessment Plan:** The plan defines the agreed-upon scope in advance, ensuring alignment between the assessment team and the client.
- **Types of Boundaries:**
  - **Physical Boundaries:** The geographical or physical areas included in the assessment (e.g., specific buildings, data centres). Often depicted in diagrams.
  - **Logical Boundaries:** The systems, applications, networks, or data flows included in the assessment.
- **Reasons for Excluding Functions/Systems from Scope:**
  - **Not Security Relevant:** The function has no significant security implications (e.g., a basic word processing application).
  - **Subject of Another Assessment:** The function is already being assessed under a separate, dedicated review (e.g., relying on a data centre's separate audit for its internal controls).
  - **Beyond Assessor Skills:** (Less common) The specific technology requires expertise the current team lacks (should ideally be addressed during planning).
  - **Physical Controls Obviate Need:** Strong physical or environmental controls might make detailed logical analysis of a function unnecessary (e.g., data on a physically secured internal LAN might not need additional encryption analysis *for internal transit*).

Determining the Rigor (Depth) of Analysis

- The required depth or rigor of the assessment depends on several factors:
  - **Perceived Strength of Existing Controls:** If controls seem strong initially, deeper analysis might be needed to confirm their actual effectiveness. This involves "digging" using multiple methods (docs, interviews, observation).
  - **Maturity of the Organisation's Security Program:** How long has the program been established? Is it well-integrated? Maturity can be indicated by factors like:
    - Lower frequency of security incidents.
    - Evidence of continuous improvement based on previous findings.
  - **Results from Previous Findings:** Reviewing past assessments helps focus the current analysis on recurring issues or areas needing verification.

Project Description, SOW, and Recommendations

- **Project Variables:** Factors like size, complexity, location, culture influence the project's price and deliverables.
- **Statement of Work (SOW):** A document detailing the services to be provided, including:
  - Service description.
  - Probability/likelihood determination methods.
  - Acceptable loss criteria.
  - Threat analysis scope.
  - Review of existing controls' effectiveness.
- **Scope of Controls:** Assessments typically cover:
  - **Administrative Controls:** Policies, procedures, standards, guidelines, training. (Detailed in later lectures)
  - **Physical Controls:** Locks, guards, CCTV, environmental controls. (Detailed in later lectures)
  - **Technical Controls:** Firewalls, IDS/IPS, encryption, access control systems. (Detailed in later lectures)
- **Providing the "Remedy" (Recommendations):**
  - Based on findings, the assessment provides recommendations for improvement.
  - Example: Suggesting the addition of firewalls or enhanced logical parameter security. Justification for recommendations is crucial.
- **Contract Types:** Can be Time & Materials (pay for actual time spent) or Fixed Price (agreed cost upfront).

Designating the Project Team

- The quality of the personnel assigned to the assessment directly impacts the quality of the project outcome.
- **Selection Criteria:**
  - **Experience:** Lead auditors typically have more experience.
  - **Expertise:** Team members possess relevant technical or domain knowledge.
  - **Familiarity:** Assigning personnel who have previously assessed the client can be beneficial, as they are already familiar with the environment (ensuring continuity and efficiency).
- Matching the right skills and experience to the specific assessment scope ensures a high-quality project.

Tasks & Next Steps

- Review the **Tutorial** questions related to this week's material.
- **Revision Tip:** Create your own summary notes after lectures (like the lecturer did during studies) to reinforce understanding and prepare for exams. Use tutorials to test comprehension and identify areas needing clarification.

Announcements

- Next week's class (Week 4) will be held **physically** at UM.

- Online classes may occasionally occur if specific circumstances arise (e.g., urgent matters), but the default is physical unless otherwise notified.

Key Takeaways

- Risk assessments serve multiple **customers** (Compliance, Legal, Techs, Ops, Admins) whose needs must be considered.
- **Quality** (in work and reports) and **Objective Evidence** are critical for credible findings and acceptance. Avoid subjective statements.
- Assessments must be managed within **scope** and **budget**, requiring careful planning and potentially flexible execution.
- Understanding **cost factors** (size, complexity, geography, culture, threat) is important for setting budgets.
- Clearly defined **objectives** and **scope** (physical/logical boundaries) are essential.
- **Methodology** involves multiple techniques (docs, interviews, observation), and **verification** of claims is crucial.
- The **rigor** of analysis depends on control strength and program maturity.
- The **project team's** quality and familiarity influence success.