Class Notes: WOA7017 Security Risk Analysis & Evaluation

Week 1 Summary

Lecturer: Prof. Omar Zakaria **Date:** Thursday, 20 March 2025 **Time:** 18:00 Malaysia Time

---

Course Introduction & Logistics

- **Lecturer Affiliation:** Universiti Pertahanan Nasional Malaysia (**UPNM**) / National Defence University of Malaysia (**NDUM**).
- **Lecturer Background:** Extensive experience (UM, UPNM), PhD from **Royal Holloway**, University of London. Specializes in Information Security Management (**ISMS** - **ISO 27001**, **BCMS** - **ISO 22301**).
- **Class Schedule (Ramadan/Shawwal):**
  - 18:00 Start, 19:15-20:00 Break (Iftar), 20:00 Resume.
  - First 3 weeks will be **online**.
  - Subsequent weeks will be **physical** at FSKTM.
- **Assessment Breakdown (50% Continuous Assessment, 50% Final Exam):**
  - **Continuous Assessment:** 2 Quizzes, 1 Individual Assignment, 1 Group Assignment.
  - **Final Exam:** Physical, **Open Book** (Lecture notes allowed, no laptops).
- **Learning Approach:** Focus on **understanding** and critical thinking, not memorization.

Rationale for Security Risk Analysis & Evaluation

- It is a fundamental part of **Risk Management**.
- **Primary Goal:** To implement **cost-effective** security controls.
- **Consequences of Neglecting Risk Analysis:**
  - **Overspending:** Implementing unnecessary controls based on assumptions.
  - **Under-protection:** Failing to address actual significant threats.
- **Key Concept:** Focus on identifying and managing **significant threats** (higher frequency or impact).
- **Control Philosophy:** Aim for **"Good"** (appropriate, cost-effective) controls, not necessarily the absolute **"Best"** (potentially excessive).
- **Illustrative Examples:**
  - **Home Security:** Budget constraints force prioritization based on likely risks.
  - **UK vs. Malaysia:** Different threat landscapes (e.g., **Terrorism** significance) necessitate different controls; blind copying is wasteful.
  - **Transparent Garbage Bags (UK):** A specific control derived from bomb threat analysis.
  - **Oklahoma City Bombing:** Led to controls like prohibiting parking near critical federal buildings.

Fundamental Security Principles (CIA + AAA)

- **CIA Triad:**

    - **Confidentiality:** Preventing unauthorized disclosure of information.
    - **Integrity:** Ensuring data accuracy, authenticity, and preventing unauthorized modification.
    - **Availability:** Ensuring systems and data are accessible to authorized users when needed.
- **Triple A (AAA):**
    - **Authentication:** Verifying *who* a user is.
        - Methods: Something you **know** (password), **have** (token), **are** (biometrics).
        - Context is key: Higher risk demands stronger authentication (e.g., immigration biometrics).
    - **Authorization:** Determining *what* an authenticated user is allowed to do/access.
    - **Accountability:** Tracking actions (**Who, What, When, Where, Why, How** - 5W1H). Crucial for audits, billing, incident investigation (e.g., **audit logs**).

Overview: Role of the Information Security Manager

- Prevent loss, fraud, and sensitive data breaches.
- Ensure **Regulatory Compliance** (e.g., software licenses).
- Manage and update **Security Policies**.
- Ensure **Business Continuity Planning (BCP)**.
- Plan for **Incident & Disaster Response**.
- **Prioritize** Security Initiatives and resource allocation.

Drivers for Security Initiatives

- **Audit Findings:** Non-compliance identified in audits drives corrective actions.
- **Technology:** New technologies can address existing weaknesses (e.g., biometrics vs. swipe cards).
- **Compliance:** Laws, regulations, or internal policies mandate specific controls.
- **Security Risk (Assessment):** The systematic process of identifying needs based on risk levels to achieve cost-effectiveness.

Introduction to Security Risk Assessment (SRA)

- **Importance of Quality:** A poor SRA leads to faulty conclusions, bias, planning errors, and potentially *increased* risk due to ineffective controls.
- **Core Components (Introduced):**
    - **Asset Valuation:** Understanding the value/criticality of what's being protected.
    - **Threat Analysis:** Identifying potential sources of harm.
    - **Vulnerability Evaluation:** Identifying weaknesses exploitable by threats.
    - **Control Effectiveness Review:** Objectively assessing how well current controls work.
- **Goal: Risk Reduction** to an acceptable level (not elimination). Identify **appropriate**, cost-effective controls.

Overview: Related Security Activities

- **Gap Analysis:** Comparing current state against a standard/requirement to find deficiencies.
- **Compliance Audit:** Verifying adherence to *required* controls (laws, standards).

- **Security Audit:** Verifying specific security controls are in place and effective.
- **Vulnerability Scanning:** Identifying known weaknesses in systems/networks.
- **Penetration Testing:** Authorized, simulated attacks to find exploitable flaws.
- **Ad Hoc Testing:** Expert-driven testing for less obvious vulnerabilities.
- **Social Engineering:** Non-technical attacks manipulating people; also used to test awareness.

Announcements & Key Logistics

- First 3 weeks of class are **online**.
- Subsequent classes will be **physical** at FSKTM.
- **Assessment:** 50% **Continuous Assessment** (2 Quizzes, 1 Indiv. Assignment, 1 Group Assignment), 50% **Final Exam**.
- Final Exam is **physical** and **Open Book** (lecture notes only).
- Course emphasizes **understanding** concepts over rote memorization.

Key Takeaways from Week 1

- Security Risk Analysis is essential for implementing **cost-effective** security, preventing waste and exposure.
- Understanding the **CIA Triad** and **Triple A (AAA)** principles is foundational.
- SRA involves analyzing **assets, threats, vulnerabilities, and controls** to appropriately reduce risk.
- The course blends online/physical sessions and uses varied assessments, culminating in an open-book final exam focused on application.
