Class Notes: WOA7017 Security Risk Analysis & Evaluation

Week 2 Summary

Lecturer: Prof. Omar Zakaria **Date:** Thursday, 27 March 2025 **Time:** 18:00 Malaysia Time

---

Why and When to Conduct Risk Assessment

- Risk assessment isn't a one-time event; it needs to be conducted or revisited based on specific **triggers**:
  - **New System Implementation:** Introducing new technology brings new, unknown risks.
  - **Major Hardware Upgrades:** Changes in infrastructure can alter the risk landscape.
  - **Major Software Version Upgrades:** New software versions might have different vulnerabilities or features affecting risk.
  - **Changes in the Threat Environment:** External factors can introduce new threats.
    - *Example:* If a jungle next to a building is replaced by a petrol pump, the fire risk and potential security threats change, necessitating a revised risk assessment.
- **Revising Risk Assessment:** When these triggers occur, the organization must re-evaluate potential threats and vulnerabilities through a formal risk assessment process.

Scoping the Risk Assessment

- **Impracticality of Full-Scope Assessment:** Conducting a risk assessment for the *entire* organization simultaneously is often infeasible due to significant requirements for:
  - **Time:** Can take a very long time to cover all departments and assets.
  - **Manpower:** Requires substantial personnel resources (assessors, interviewees).
  - **Cost:** Involves significant expense.
- **Targeted Scoping:** Therefore, risk assessments are typically **scoped** to specific, manageable units:
  - Specific departments (e.g., Finance Department only).
  - A combination of related departments (e.g., IT Department + Finance Department).
  - Specific critical systems or processes.
- **Risk Assessment as a Project:** Because it has defined objectives, scope, resources, and timelines, a risk assessment is treated as a **project**.
  - A **project** inherently has a defined **beginning** and **end**.
  - *Examples:* Final Year Project (FYP), Financial Project – all have start and end dates (e.g., 14 weeks for a semester, sometimes 28 weeks over two semesters).

Project Definition Elements for Risk Assessment

- Establishing a clear project definition is crucial before starting the assessment. Key components include:
  - **1. Project Scope Agreement:**

        - A formal agreement defining the **boundaries** (what's included/excluded) and the **content of deliverables** (what the assessment will produce).
        - Needs clear definition of the areas under assessment (e.g., IT Department, Finance Department).
        - *Example (Gamuda Audit):* The scope explicitly stated "Operation and Management of Group IT Services for Gamuda Berhad" and listed specific ISO 27001 clauses to be audited (e.g., 4.1, 4.2, 4.3, 6.1, 6.2).
        - **Sharing the Plan:** The scope and detailed plan (like an **audit plan** or **risk assessment plan**) must be communicated to the **auditees** (the departments/teams being assessed) well in advance (e.g., two weeks).
            - **Purpose:** Allows auditees to prepare relevant documents, personnel, and evidence. It is *not* a surprise "spot check" aimed at finding fault, but a collaborative process to assess risk based on prepared information. Avoids wasting time searching for documents during the assessment.
    - **2. Project Budget:**
        - Risk assessments incur costs, even if performed internally (staff time, resources).
        - External assessments have direct costs based on effort.
        - **Cost Calculation:** Often based on standardized tables/formulas considering:
            - Number of employees within the scope.
            - Complexity of the tasks/systems being assessed.
            - Required effort, measured in **mandays** (or persondays).
        - *Example (Gamuda Audit based on ISO Audit Time Table B.1):*
            - Audit time (mandays) depends on the number of personnel involved in the scope (e.g., 1-10 staff might require 0.5-2 mandays).
            - The Gamuda audit involved 3 auditors working for 2 days = **6 mandays**. (3 auditors * 1 day = 3 mandays/day; 3 mandays * 2 days = 6 mandays total).
            - This suggests the scope covered a part of Gamuda involving roughly 66-85 relevant staff (based on the example table shown, focusing only on staff involved in the security scope, not the entire company).
            - Different certification bodies (BSI, Sirim QAS, CyberSecurity Malaysia) might use the same base tables but offer different quotes based on discounts (**additive/subtractive factors**).
    - **3. Time Frame:**
        - A defined schedule with start and end dates, and milestones.
        - *Example (Gamuda Audit):* The plan detailed activities for Day 1 and Day 2, with specific time slots allocated (e.g., 9:30 Opening Meeting, 10:00 Clause X assessment, 1:00 Lunch, etc.).
    - **4. Manageable Tasks & Resource Allocation:**
        - The overall assessment work is broken down into smaller, manageable tasks.
        - Resources (assessors/auditors) are allocated to specific tasks.
        - *Example (Gamuda Audit):* The plan showed specific auditors (NY, JT, YL) assigned to audit specific ISO clauses/topics at specific times. Sometimes tasks were split, with auditors working concurrently on different areas (e.g., at 10:00, NY covers Topic A, JT covers Topic B, YL covers Topic C).
    - **5. Assessment Boundaries:**
        - Clearly defining what is *in scope* also clarifies what is *out of scope*.

        - Ensures focus and prevents scope creep.
        - *Example:* Assessing a bank – the scope might be limited to the 'Saving Account' application system initially, explicitly excluding 'Loans' or 'Current Account' systems for that specific project phase.

Identifying and Valuing Assets

- **Information Assets:** Any resource or data of value to the organization that requires protection.
    - **Definition:** Includes hardware, software, networks, personnel (staff), documentation (physical or digital), buildings/facilities, organizational reputation, business documents, and other tangible/intangible items.
    - **Crucial Step:** Identifying assets is fundamental to knowing what needs to be protected.
- **Tangible vs. Intangible Assets:**
    - **Tangible Assets:** Physical items that can be seen and touched.
        - *Examples:* Buildings, equipment (servers, desktops), physical documents.
    - **Intangible Assets:** Non-physical items, often related to reputation or information value.
        - *Examples:* Organization's reputation/image, customer trust, intellectual property, data.
        - Protecting these is often a key driver for security (e.g., ensuring fast, secure banking services maintains customer trust and reputation).
- **Asset Enumeration:**
    - The process of listing and grouping the assets that fall within the assessment's scope.
    - Helps to precisely define *what* is being assessed.
    - *Analogy:* Similar to **metadata** for an image (which describes the image: date captured, size, location), asset enumeration describes the components of the system/area being assessed.
    - *Example:* For a 'Saving Account' application assessment, enumeration would list:
        - Specific servers (hardware) involved.
        - Application software and database versions (software).
        - Network segments used (network).
        - Key personnel managing/using the system (people).
        - Physical location of servers (building).
        - Relevant policy/procedure documents (documentation).
- **Asset Valuation and Relation to Controls:**
    - The perceived value or criticality of an asset often dictates the level and strength of security controls applied.
    - Higher value/criticality assets typically warrant stronger controls.
    - *Example (Lab Security):*
        - A **network switch** in a lab rack is critical; if it fails, the whole lab network goes down. Control: Locked rack, special key access.
        - A single **desktop PC** is less critical; if it fails, only one user is affected. Control: Simple cable lock for CPU/monitor.
    - Risk assessment must consider this relationship – are controls appropriate for the asset's value?

Phase 2: Project Preparation

- This phase involves setting up the groundwork for the assessment execution.

- **Key Activities:**
  - **1. Select Team & Introduce Team:**
    - Identify individuals who will conduct the assessment.
    - Define roles (e.g., Team Lead, Assessor, Subject Matter Expert, Observer).
    - *Example (Gamuda Audit):* Team clearly defined: Norida Yahya (Lead Auditor), U auditors (JT, YL), BSI Observer (Azizan), External Observer (Prof. Omar Zakaria).
  - **2. Obtain Permission:**
    - Formal authorization is required to conduct the assessment.
    - Sign **Non-Disclosure Agreements (NDAs)** because assessors will likely access sensitive or confidential information.
    - Obtain specific permissions needed to access physical locations (e.g., Data Center) or systems/data.
  - **3. Review Business Vision/Mission/Objectives:**
    - Understand the organization's strategic direction and goals to contextualize the assessment. *Example:* Reviewing Gamuda's ISMS objectives like "determine conformity," "determine effectiveness."
  - **4. Identify Critical Systems:**
    - Focus the assessment effort on systems most vital to the organization's operations, revenue, or mission.
    - Prioritize these systems as they often represent the highest risk if compromised.
    - *Example:* Focusing on a bank's 'Saving Account' system because it's highly profitable and customer-facing. (Does not mean non-critical systems are ignored, but critical ones are prioritized).
  - **5. Map Assets (Asset Enumeration):**
    - Detailed listing of assets associated *specifically* with the identified critical systems within the scope.
  - **6. Identify Threats:**
    - Understand the organization's existing process for identifying potential threats relevant to the scoped assets/systems. Review their threat intelligence methods.
  - **7. Determine Expected Controls:**
    - Review existing security controls relevant to the scope.
    - Evaluate if they are appropriate or if new/revised controls are needed based on potential threats and asset value. The assessment will later evaluate their effectiveness.

Phase 3: Data Gathering

- Collecting detailed information about the scoped environment using multiple methods. Essential for analysis.
- **Three Categories of Data:**
  - **1. Administrative Data Gathering:** Focuses on documentation, policies, procedures, and human aspects.
    - **Purpose:** Understand the documented rules and intended practices.
    - **Methods/Sources:**
      - **Policy Review:** Examining high-level documents stating management's intent and rules (what *can* and *cannot* be done). Policies drive actions. *Example:* Password

complexity policy, data backup policy, building access policy (main gate closed at 12 AM).
        - **Procedure Review:** Examining detailed, step-by-step instructions for performing specific tasks. Procedures implement policies. *Example:* Procedure for updating antivirus software, procedure for requesting system access, procedure for performing daily backups. Review checks if procedures are clear, correct, efficient, and align with policy.
        - **Training Review:** Assessing the organization's **SETA** (Security Education, Training, and Awareness) program content and effectiveness. Is training adequate? Does it cover relevant risks? *Example:* Reviewing training materials on the importance of locking workstations. If users ignore lock screens due to "ignorance" or thinking it's unimportant, training might be insufficient.
        - **Organization Review:** Examining the people involved – roles, responsibilities, job rotation, shift work, supervision, performance monitoring related to the scoped system/process. Is staffing adequate? Are responsibilities clear?
        - **Interviews & Observation:** Talking to personnel to understand their practices and perspectives. Directly observing workflows and security practices in action. *Crucial for cross-checking.*
    - **Cross-Checking Example (Lock Screen):**
        - *Administrative (Policy):* Policy states users MUST lock screens when leaving workstations.
        - *Physical (Observation):* Assessor observes a staff member leaving their workstation unlocked.
        - *Finding:* A violation of policy. Interviewing the staff member might reveal reasons (ignorance, inconvenience, perceived low risk), informing potential improvements to training or procedures.
- **2. Technical Data Gathering:** Focuses on the technology, systems, and configurations.
    - **Purpose:** Understand the actual technical implementation and settings.
    - **Methods/Sources:**
        - **Design Review:** Examining system architecture diagrams, network diagrams, security design documents. *Example:* Comparing the security design principles applied to the lab switch versus the lab desktop.
        - **Configuration Review:** Checking the actual settings on devices (firewalls, routers, servers, applications). *Example:* Reviewing firewall rules for spam filtering – ensuring they check both sender reputation *and* content, adapting to newer spammer techniques (impersonation).
        - **Architectural Review:** Analyzing the overall structure, including network segmentation. *Example:* Verifying that public-facing web servers are placed in a **DMZ (Demilitarized Zone)**, while sensitive internal systems (like core banking) are on protected internal networks.
        - **Security Testing Review:** Examining results from vulnerability scans, penetration tests, Disaster Recovery (DR) tests. *Example:* Financial institutions in Malaysia are required by Bank Negara Malaysia (Central Bank) to conduct security testing (e.g., penetration tests) twice a year and report results, demonstrating network readiness and resilience.

    - **3. Physical Data Gathering:** Focuses on the tangible environment and physical security measures.
        - **Purpose:** Understand the physical protections and risks.
        - **Methods/Sources:** Reviewing policies/procedures related to physical access, observing physical controls (locks, guards, CCTV placement), inspecting facilities. *Example:* Checking if server room doors are properly locked, if visitor logs are maintained.

Phase 4: Risk Analysis

- The core phase where gathered data is analyzed to identify and understand risks.
- **Key Activities:**
    - **1. Asset Valuation:** Reconfirming the value (criticality, cost, importance) of the assets identified within the scope. This informs the potential impact of threats.
    - **2. Threat Identification & Analysis:**
        - **Threat Definition:** An undesired event that could result in loss, disclosure, or damage to assets (Confidentiality, Integrity, Availability).
        - *Examples of Threat Types:* Errors (human/system), Omissions, Fraud, Theft, Sabotage, Loss of physical support (power/cooling), Malicious Code (viruses, ransomware), Unauthorized Disclosure.
        - **Relevant Threat:** Identifying threats that are specifically applicable to the assets and environment being assessed.
        - **Threat Agent:** The entity that initiates or causes the threat. *Examples:* Hackers, disgruntled employees, competitors, careless users, natural disasters, hardware failure.
        - **Threat Environment:** The context influencing threats. *Examples:* Physical location (flood zone, earthquake area), geopolitical situation, industry sector.
    - **3. Vulnerability Identification & Analysis:**
        - **Vulnerability Definition:** A flaw, weakness, or loophole in security controls (administrative, technical, or physical) that a threat agent could exploit to cause harm.
        - *Password Example:* A weak control (password) has vulnerabilities like users choosing easy-to-guess passwords (`123456`), using default passwords, or writing passwords down.
        - **Categories of Vulnerabilities:**
            - **Administrative:** Gaps or weaknesses in policies, procedures, standards, guidelines, training. *Example:* A university dress code policy failing to explicitly prohibit male students from wearing earrings (as per lecturer's anecdote), creating a policy gap.
            - **Physical:** Weaknesses in physical security measures. *Example:* Lack of thorough background checks for critical personnel like bus drivers (might be experienced but have a bad driving record/summonses).
            - **Technical:** Flaws or weaknesses in logical/system controls. *Examples:* Misconfigured routers/firewalls, bugs/flaws in software code (programming errors), weak password enforcement mechanisms in systems.
    - **4. Risk Calculation & Statement:**
        - **Security Risk Definition:** The likelihood that a specific **threat** will exploit a specific **vulnerability** associated with an asset, and the potential **impact** (loss/damage) if it occurs.

        - This step involves assessing likelihood and impact (often qualitatively or quantitatively), calculating a risk level, documenting the risk in a clear statement (e.g., "Risk of unauthorized data disclosure due to weak password vulnerability being exploited by external hackers"), and achieving consensus within the assessment team. (Detailed calculation methods discussed in later chapters).

Phase 5: Risk Mitigation

- Developing and recommending solutions to reduce the identified risks to an acceptable level.
- **Core Principle:** The goal is **risk reduction**, *not* risk elimination. It's impossible to eliminate all risk.
- **Key Activities:**
    - **1. Safeguard/Control/Countermeasure Selection:**
        - Identifying and proposing specific actions, techniques, activities, or technologies (**safeguards**) to reduce risk. (Safeguard = Control = Countermeasure).
        - Process involves:
            - Matching potential safeguards to the specific threats and vulnerabilities identified.
            - Estimating how much each safeguard will reduce the risk.
            - Determining the cost and feasibility of implementing the safeguard.
            - Grouping related safeguards into comprehensive solutions.
    - **2. Types of Safeguards/Controls:**
        - **Preventive Controls:** Aim to *stop* undesirable events from occurring in the first place.
            - *Examples:* Access control systems (badges, biometrics), firewalls blocking malicious traffic, door locks, strong password policies, security awareness training teaching users safe practices.
        - **Detective Controls:** Aim to *identify* undesirable events or conditions *after* they have occurred or are in progress.
            - *Examples:* Audit logs recording system activity, Intrusion Detection Systems (IDS) alerting on suspicious network traffic, CCTV monitoring, regular security testing, system monitoring for abnormal activity (e.g., login attempts at 3 AM).
            - *Example (Indonesian Flag Incident):* Detecting attack traffic originating from Indonesian IP addresses after the flag incident allowed for defensive actions (alerting technical teams to strengthen controls).
        - **Corrective Controls:** Aim to *remedy* or minimize the damage *after* an undesirable event has occurred.
            - *Examples:* Restoring data from backups after a deletion or corruption event, implementing Disaster Recovery (DR) procedures after an outage, updating policies or procedures based on lessons learned from an incident.
    - **3. Understanding Residual Risk:**
        - **Definition:** The risk that *remains* even after recommended safeguards have been implemented.
        - **Why it Exists:** No control is 100% effective; some threats are unpredictable or unavoidable; there's always a possibility of control failure or unforeseen circumstances.
        - **Goal:** To reduce risk to a level that is *acceptable* to the organization (within its **risk tolerance** or **risk appetite**), not to eliminate it entirely.
        - *Example (Driving):* Following speed limits and driving carefully (controls) reduces accident risk. The residual risk is the chance of an unavoidable accident (e.g., another

car suddenly swerving into your lane, tire blowout).
    - *Example (Passwords):* Implementing strong password policies and training (controls) reduces unauthorized access risk. The residual risk includes users still sharing passwords or falling for sophisticated phishing attacks.
    - Risk assessment must identify and acknowledge this leftover risk.

Phase 6: Risk Reporting & Resolution

- The final phase involves communicating the assessment results and facilitating management decisions.
- **Key Activities:**
    - **1. Risk Reporting:**
        - Develop a formal report and potentially a presentation summarizing the assessment findings.
        - Target audience: Management, **project sponsor** (the executive who commissioned the assessment).
        - Content: Clearly identifies the risks discovered, the analysis performed, and the **recommended safeguards** or actions.
        - Purpose: To provide clear, actionable information for decision-making, including justifying necessary resources (budget, personnel) for implementing controls.
    - **2. Risk Resolution:**
        - The process by which **senior management** decides how to address each identified risk presented in the report.
        - **Resolution Options:**
            - **Risk Reduction (Mitigation):** Implement the recommended safeguards/controls to decrease the likelihood or impact of the risk. *Example:* Installing biometric time clocks to reduce buddy-punching (time theft).
            - **Risk Acceptance:** Acknowledge the risk but decide not to take action, typically because the risk level is within tolerance, or the cost of control outweighs the potential loss. *Example:* Deciding not to add expensive grills to office windows if break-ins haven't occurred in years and the windows are already locked.
            - **Risk Transfer (Delegation/Sharing):** Shift the financial impact or responsibility for the risk to a third party. *Examples:* Buying insurance to cover losses from fire or flood; Outsourcing a specific function (like security monitoring) to a specialized vendor.
        - **Documentation is Crucial:** The final risk resolution decisions made by management *must* be documented. This serves as evidence for future audits and demonstrates due diligence. Auditors will ask *why* certain controls were chosen, improved, or remained unchanged, and this documentation provides the justification based on the risk assessment.

Announcements & Miscellaneous

- **Next Class (Week 3):** Will be held **online** (synchronous via MS Teams) due to the Hari Raya holiday period falling near the scheduled Thursday class.
- **Following Class (Week 4):** Will be a **physical class** held on campus.

- **Exam Format:** The final exam will be **open book**. Students can bring printed lecture notes and the textbook. Internet access and laptops are *not* permitted. The focus is on **understanding** the concepts, not memorization.
- **Tutorial 1:** Answers can be found using the textbook or reliable internet sources. Students are encouraged to discuss if unsure.
