VICTORIAN
INSTITUTE OF
TECHNOLOGY
www.vit.edu.au

ITSC1001
INFORMATION SYSTEMS RISK AND SECURITY

Tutorial 8

Task 1: "Know Yourself" — Asset Identification & Prioritization

First, you must identify what you are trying to protect.

Activity: Imagine you are the security manager for a small e-commerce company.

1. **List Assets:** List **five** key information assets for your company. Use the categories from your lecture to ensure you have a mix.
    - **Hardware:**
    - **Software:**
    - **Data:**
    - **People:**
    - **Procedures:**
2. **Value Assets:** Now, create a simple "Weighted Factor Analysis" table like the one in your lecture. You will rank your five assets.
    - **Step 1:** Choose two criteria and give them weights (must total 100).
        - Criterion 1:
        - Criterion 2:
    - **Step 2:** Score each of your assets from 0.1 (low impact) to 1.0 (high impact) for each criterion.
    - **Step 3:** Calculate the "Weighted Score" for each asset.
        - *Formula: (Criterion 1 score * Weight) + (Criterion 2 score * Weight)*
    - **Table:**

Information Asset	Criteria 1	Criteria 2	Weighted score

do this for your 5 assets

3. **Prioritize:** List your assets in order, from the highest weighted score to the lowest. This is now your **prioritized asset list**.

Task 2: "Know Your Enemy" — Threat & Vulnerability Pairing

Now you know what's important. Next, you identify what threatens it.

Activity:

1. Take your **top two** prioritized assets from Task 1.
2. For each asset, identify **one** relevant threat from the "Threats to InfoSec" table in your lecture.
3. Then, describe a plausible vulnerability.
    - **Asset:**
    - **Threat:**

- **Vulnerability:**

Task 3: Risk Assessment — Calculating the Risk

This is where you combine the asset value, threat, and vulnerability to get a final risk rating.

Activity 1: Qualitative Analysis Use the Australian/New Zealand Standard tables from your lecture for a quick, high-level assessment of your **Asset 1** (from Task 2).

1. **Determine Consequence:** What would be the consequence level if this attack happened?
   - (Choose one: 1-Insignificant, 2-Minor, 3-Moderate, 4-Major, 5-Catastrophic)
2. **Determine Likelihood:** How likely is this attack?
   - (Choose one: A-Almost certain, B-Likely, C-Possible, D-Unlikely, E-Rare)
3. **Find Risk Level (Slide 29):** Use the matrix to find your risk level.
   - **Result:** (e.g., E, H, M, or L)

Activity 2: Quantitative Analysis

- **Formula:** Risk = (Likelihood * Consequence) - % Mitigated by Controls + % Uncertainty
- **Scenario for your Asset 2:**
  - **Consequence (Asset Value):** Use its **Weighted Score** from Task 1.
  - **Likelihood:** The threat is very real. (Likelihood = **0.8**)
  - **Current Controls:** You have a basic firewall that *might* stop it, but you're not sure. (Mitigation = **20%**)
  - **Uncertainty:** You are not very confident in your data. (Uncertainty = **10%**)
- **Calculate the Risk Rating:**
  - Risk = (0.8 * [Your Asset 2's Weighted Score]) - 20% + 10%
  - Risk = [Your final number]

Task 4: Documentation — Creating the Final Report

The final step is to document your findings in a way that management can understand.

Activity: Create a two-line "Ranked Vulnerability Risk Worksheet" based on the results from all your tasks. This is the final deliverable that lists your risks in priority order.

Asset	Asset Impact (Weighted Score)	Vulnerability	Vulnerability Likelihood	**Risk-Rating Factor**

You now have a prioritized list showing exactly where to spend your security budget first.