Lecture Two

Risk Assessment Model

Steps to Build a Risk Assessment Model

Risk assessment model is assessed by following the following steps:

1. Identifying assets.
2. Identifying threats.
3. Identifying vulnerabilities.
4. Relating threats to vulnerabilities.
5. Determining the likelihood.
6. Evaluate the impact of each risk.



Figure 1: Risk assessment model

Step 1: Identifying assets

1. Why Identify Assets First?

Risk is always about harm to something of value, so assets come first. The reasons are:

i. An incomplete inventory means unassessed, unprotected systems.
ii. Asset inventory is a foundational control that identifies all hardware and software that need protection.
iii. It supports patching, incident response, and audits.
iv. It enables a fair prioritization of limited security effort.

1.2 Categories of Assets

Assets are commonly divided into three categories:

Table 1: Assets categories

Category	Includes	Example
Primary assets	Business processes and activities; information and data	Admissions process, student records
Supporting assets	Hardware, software, networks; people, buildings, and rooms	Servers, Wi-Fi, IT staff
Intangible assets	Reputation and trust; intellectual property	Research results, brand

1.3 How to Build an Asset Inventory

1. Interview business and department owners.
2. Use network and endpoint discovery scans.
3. Review procurement, licensing, and cloud account records.
4. Use a configuration management database (CMDB) where available.
5. Review and update regularly: an inventory is never finished.

1.4 Typical Asset Inventory Attributes

Each asset is recorded with its *identifier*, *type*, *owner*, and *location*. Example for a *university*:

Table 2: Sample asset inventory

ID	Asset	Type	Owner	Location
A1	Student records database	Primary assets (information)	Registrar	Data center
A2	Registration web server	Supporting assets (Software/Hardware)	IT Manager	Data center
A3	Campus Wi-Fi network	Supporting assets (Network)	IT Manager	All buildings
A4	Exam question bank	Primary assets (Information)	Dept. Head	File server

1.5 Challenges in Asset Identification

i. **Shadow IT:** systems used without IT approval.
ii. **Personal devices (BYOD)** connecting to the network.
iii. **Cloud services** created quickly and forgotten.
iv. **Third-party systems** that hold your data.
v. IoT devices and temporary lab equipment.
vi. **Information assets** are harder to find than hardware.

2. Assets Valuing

Table 3: Valuation approaches

Approach	Description
Qualitative	Rate assets as Low, Medium, or High. Quick, simple, based on judgment.
Quantitative	Express value in money: replacement cost, lost revenue, recovery cost.

2.1 Factors That Influence Asset Value

i. Replacement or recovery cost.
ii. Importance to critical business processes.
iii. Legal and contractual obligations.
iv. Sensitivity of the information held.
v. Reputation damage if lost or exposed.
vi. Time the organization can operate without it.

2.2 Quantitative vs. Qualitative Asset Measurement

Quantitative risk or asset measurement is the standard approach used in many fields such as insurance and finance; however, it is not commonly applied to measuring the value of assets in *information systems*. There are several reasons for this limitation:

1. Difficulty in identifying and assigning accurate numerical values to all assets and components involved in information systems.
2. Human factors (such as user behavior or intent) cannot be effectively measured using quantitative methods.
3. Lack of sufficient statistical data to determine the frequency or probability of specific incidents affecting information system assets.

Therefore, most modern tools used in information systems rely on qualitative asset measurement, which uses descriptive categories (such as low, medium, or high) instead of numerical values to evaluate asset value levels.

Step 2: Identifying threats

A threat is any potential event or action that could cause harm to your assets, operations, or objectives.

Methods:

- **Brainstorming**: Gather a team to list potential threats.
- **Historical Data**: Review past incidents, audit reports, and industry news.
- **SWOT Analysis:** a strategic planning tool used to identify an organization's Strengths, Weaknesses, Opportunities, and Threats.

Examples of Threats:

- **Cyber**: Malware infection, phishing attack, DDoS attack.
- **Operational:** Power outage, key supplier going bankrupt, natural disaster (flood, earthquake).
- **Human:** Employee error, insider theft, workplace accident.
- **Physical:** Theft, vandalism, fire.

Step 3: Identifying Vulnerabilities

A vulnerability is an internal weakness or gap in your defenses that a threat could exploit. It's what makes you susceptible to a threat.

Methods:

- **Vulnerability Scanning:** (For IT systems) Automated tools that scan for known software vulnerabilities.
- **Penetration Testing:** Ethical hackers simulate an attack to find weaknesses.
- **Audits & Inspections:** Physical inspections of facilities, financial audits, process reviews.

- **Interviews & Surveys:** Asking employees about process bottlenecks, outdated equipment, or security shortcuts they've observed.

Examples of Vulnerabilities:

- **Cyber:** weak passwords, lack of firewall, poor access controls.
- **Operational:** Single point of failure in a supply chain, lack of employee training.
- **Physical:** Broken lock, missing security camera, flammable materials stored improperly.

Step 4: Relating Threats to Vulnerabilities (Asset-Based Context)

This is the crucial step where you create "risk scenarios." You ask: **"Can a specific threat exploit a specific vulnerability to damage a specific asset?"**

- **Method:** Create a ***Risk Matrix*** **or** ***Pairing Table***.
- **Process:**
  1. Identify the **Asset** (what you are trying to protect: e.g., customer database, production line, reputation).
  2. For each asset, list the relevant **Threats**.
  3. For each threat, list the **Vulnerabilities** that would allow it to succeed.
- **Example Scenarios:**

- **Threat:** Phishing Attack | **Vulnerability:** Lack of employee security awareness training | **Asset:** Employee login credentials & network access.
- **Threat:** Fire | **Vulnerability:** Lack of a fire suppression system in the server room | **Asset:** IT Servers and data.
- **Threat:** Key Supplier Bankruptcy | **Vulnerability:** No alternative supplier identified (single-source dependency) | **Asset:** Production Capability.

Step 5: Determining the Likelihood

This is the probability that a specific threat will exploit a specific vulnerability to cause an incident. It's often rated on a scale (e.g., High, Medium, Low or 1-5).

- **Factors to Consider:**

- **Historical Frequency:** How often has this happened to us or others in our industry?
- **Threat Capability & Intent:** (e.g., For a cyber-threat, how skilled are the hackers? How motivated are they?)
- **Effectiveness of Existing Controls:** How well do your current security measures, policies, and procedures prevent this?

✓ **Likelihood Scale Example:**

❖ **5 - Almost Certain:** Is expected to occur in most circumstances.

❖ **4 - Likely:** Will probably occur in most circumstances.

❖ **3 - Possible:** Might occur at some time.

❖ **2 - Unlikely:** Could occur at some time but is rare.

❖ **1 - Rare:** May occur only in exceptional circumstances.

Step 6: Evaluate Impact for Each Risk

This assesses the severity of the consequences if the risk event occurs. It focuses on the damage to the asset and the organization's objectives. It is also rated on a scale.

○ **Categories of Impact:**

- **Financial:** Cost of recovery, lost revenue.
- **Operational:** Downtime, disruption of service, loss of productivity.
- **Reputational:** Loss of customer trust, negative media coverage.
- **Legal/Compliance:** Regulatory fines, lawsuits, breach of contract.
- **Health & Safety:** Injury or loss of life.

○ **Impact Scale Example:**

- **5 - Catastrophic:** Company-wide shutdown, massive financial loss, loss of life.
- **4 - Major:** Major disruption to a critical business unit, significant financial loss.
- **3 - Moderate:** Localized disruption, manageable financial cost.
- **2 - Minor:** Minor disruption, low financial cost.
- **1 - Insignificant:** Negligible impact.

Putting It All Together: The Risk Matrix

Once you have the Likelihood and Impact for each risk scenario, you plot them on a **Risk Matrix** to determine the overall **Risk Level**.

Impact	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Catastrophic (5)	Medium (5)	High (10)	High (15)	**Extreme (20)**	**Extreme (25)**
Major (4)	Low (4)	Medium (8)	High (12)	High (16)	**Extreme (20)**
Moderate (3)	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
Insignificant (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

- ***Extreme/High Risk:*** *Requires immediate action and senior management attention. Must be mitigated or avoided.*
- ***Medium Risk:*** *Require specific monitoring and response plans. Mitigation should be applied if cost-effective.*
- ***Low Risk:*** *May be accepted or managed by routine procedures.*

This 5-step process provides a rigorous, documented, and repeatable method for assessing risks, ensuring that you are not just identifying threats, but also examining the critical intersection where threats intersect with your specific vulnerabilities.