Lecture One

General Introduction

1. The General Model for Information Security Risk

A general model for information security risk assessment identifies risk as a function of assets, threats, and vulnerabilities, often expressed as:

Risk = Assets × Threats × Vulnerabilities.

- **Assets:** Any piece of information or IT system that has value to an organization, such as data, hardware, software, and intellectual property.
- **Threats:** Potential events or actors that could exploit vulnerabilities to harm an asset, like malware, phishing, or natural disasters.
- **Vulnerabilities:** Weaknesses or flaws in systems or processes that could be exploited by a threat.
- **Attack:** Execution of the threat.
- **Impact (Incident):** The potential harm or negative consequences that could result from a security incident, affecting the business, reputation, or operations.

2. Risk Categories:

Risk categorization is the process of classifying risks within an organization. By grouping similar risks.

i. **Strategic Risk:** Risks related to the organization's overall business strategy and goals, such as market changes or competitive pressures.

ii. **Operational Risk:** Risks arising from day-to-day business activities and processes, like equipment failure, human error, or supply chain disruptions.

iii. **Financial Risk:** Risks involving the organization's financial health, including credit risk, market volatility, and liquidity.

3. What Is Risk Management?

Risk management is a structured, continuous process to *identify*, *assess*, *treat*, and *monitor* risks.

- **It keeps risk within the level the organization accepts.** The aim is not to remove all risk, but to keep it within the organization's risk appetite.
- **It links security to organizational goals and decisions.** Security choices are made to support the business, not only for technical reasons.
- **It is a repeating cycle, not a one-time activity.** Threats and the business change, so the process is repeated continuously.

4. The Risk Management Process

Risk management is not a one-time task. It is a process with three stages that an organization repeats continuously.

4.1 Context and Identification

The first step is to understand the organization's context, then identify what could go wrong. This means identifying the assets that have value, the threats that could harm them, and the vulnerabilities that a threat could exploit. Without this stage, the organization does not know what it is protecting or what it is protecting it from.

4.2 Analysis and Evaluation

Once the risks are identified, we analyze them. We estimate the likelihood that each risk will happen and the impact it would have, then prioritize the risks accordingly.

$$\text{Risk rating} = \text{likelihood} \times \text{impact}$$

so a risk that is both likely and severe comes first. This stage tells us which risks deserve attention now and which can wait.

4.3 Treatment and Monitoring

For each risk that needs action, the organization chooses a treatment: avoid, reduce, transfer, or accept. Choosing is not the end of the process. The organization must monitor and review continuously, because threats change, new vulnerabilities appear, and controls may stop working as expected.

When the organization chooses to reduce a risk, it defines and implements security controls, procedures, and technologies to mitigate the risk to an acceptable level.

The risk mitigation strategy is to minimize the impact of risks recommended from the risk assessment process. There are 3 types of plans to implement risk mitigation:

1. **Incident response plan:** A set of procedures to detect and mitigate unexpected events before or while an incident is in progress.
2. **Disaster recovery plan:** The most common mitigation plan used to recover losses from any disaster or incident. Small to mid-sized businesses may also incorporate it as part of their business continuity plan.
3. **Business continuity plan:** The most strategic plan that provides the continuation of a business in case of a natural disaster by ensuring the running of the IT system of an organization. It provides non-stop running of the IT system in the midst of the crisis; however, the disaster recovery plan is focused on recovering the IT system to full functionality after a disaster occurs.

These controls and plans are not final. They must be monitored and reviewed, because a control that no longer works leaves the risk higher than expected.

5. Why Manage Risk?

- **Cyber risk is business risk.** An incident affects money, reputation, and operations, not only systems.

- **No system is 100% secure.** Some risk always remains, so the aim is to control it, not remove it.
- **Resources are limited.** Not everything can be protected equally, so the most important assets come first.
- **Decisions need priorities, not intuition.**
- **The goal:** reduce potential losses to a level the organization accepts (its risk appetite).

6. Risk Positions:

Every organization faces risk. Before deciding what to do about it, we need to answer three questions: how bad is the risk with no protection, how bad is it with protection, and how much risk are we willing to live with?

B. Inherent risk

Inherent risk is the risk before any controls are applied.

Take a financial services firm that holds sensitive customer data. Imagine it has no access restrictions, no encryption, no staff training and no incident response plan. A data breach is very likely, and the impact would be severe: regulatory fines, reputational damage and operational disruption. High likelihood combined with high impact gives high inherent risk.

C. Controls

Controls are the measures that reduce likelihood, impact, or both.

The same firm now introduces:

- Multi-factor authentication (MFA)
- Staff security training
- Encrypted storage

Some of these make a breach less likely, and others limit the damage if one happens.

D. Residual risk

Residual risk is the risk that remains after controls are applied.

With the controls in place and working effectively, the likelihood of a breach is materially lower and the impact is partially contained. The resulting score is lower than the inherent risk. That is the residual position.

Key idea: Inherent risk − effect of controls = Residual risk

E. Risk appetite

Risk appetite is the amount of risk the organization is willing to take.

It acts as the benchmark. Management compares the residual risk against it:

- **Within appetite:** no further action is needed.
- **Above appetite:** something more must be done.

F. Treatment options

After comparing the residual risk with the risk appetite, the organization chooses one of four responses:

- Avoid: Stop the risky activity.
- Reduce: Add more controls.
- Transfer: Share the loss with a third party.
- Accept: Live with the risk knowingly.

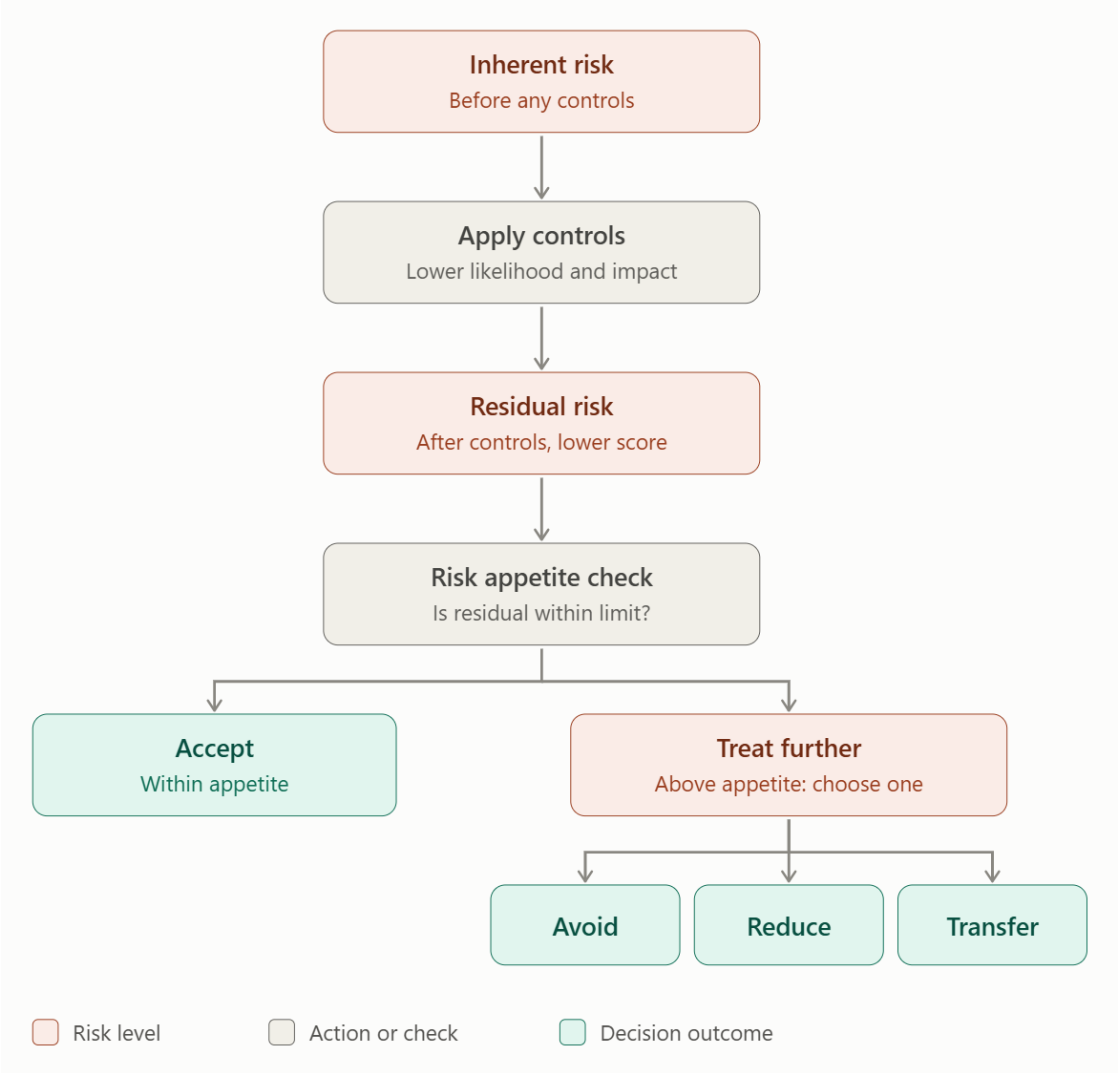


Figure 3: Risk position flow

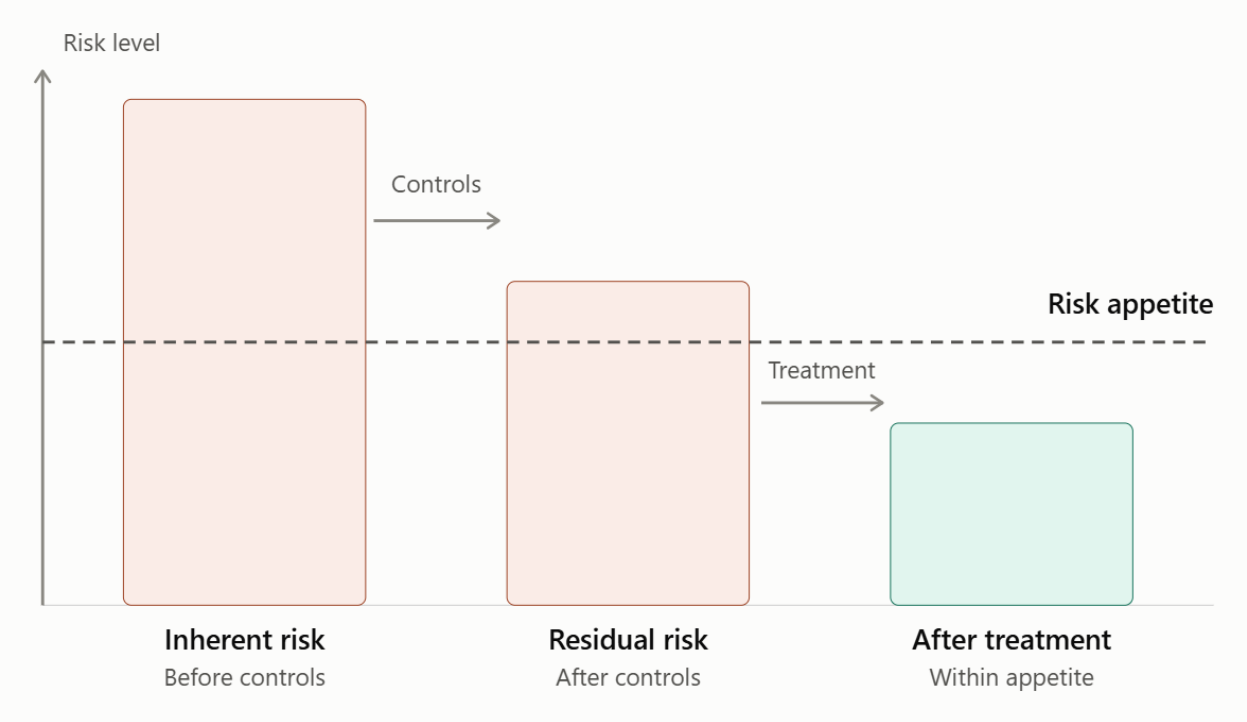


Figure 4: Risk Positions at a Glance