**1. Define the Context**

Identify the assets that need to be protected. These could include:

Sensitive Information: Confidential business data, intellectual property, trade secrets.

Customer Data: Personal information, payment details, transaction history.

Financial Information: Financial records, bank account details, investment information.

Critical Systems: IT infrastructure, databases, communication systems.

**2. Define the Risk Matrix**

For each potential risk scenario, define:

Likelihood : Probability of the risk scenario occurring (e.g., Low, Medium, High).

Consequence : Severity of the potential impact (e.g., Low, Medium, High).

Risk Rating : Overall risk posed by the scenario, calculated as ( R = L \times C ).

**3. Define Three Risk Scenarios**

Identify specific risks the client is trying to protect their assets from:

Cyberattack: Unauthorised access to sensitive information.

Natural Disaster: Damage to critical systems due to events like floods or earthquakes.

Employee Negligence: Accidental data breaches or loss of sensitive information.

**4. Assess Risk Rating for Each Risk Scenario (Inherent Risk)**

Assume no measures are in place to reduce the risk:

**Cyberattack**:Likelihood: High Consequence: High Risk Rating: High (High (\times) High)

**Natural Disaster:** Likelihood: Medium Consequence: High Risk Rating: Medium-High (Medium (\times) High)

**Employee Negligence:** Likelihood: Medium Consequence: Medium Risk Rating: Medium (Medium (\times) Medium)

**5. Assess Risk Rating for Each Risk Scenario with Existing Measures (Current Risk)**

Consider existing measures in place:

**Cyberattack:** Existing Measures: Firewalls, antivirus software Likelihood: Medium

Consequence: Medium Risk Rating: Medium (Medium (\times) Medium)

**Natural Disaster**: Existing Measures: Backup systems, disaster recovery plans

Likelihood: Low Consequence: High Risk Rating: Medium (Low (\times) High)

**Employee Negligence:**

Existing Measures: Security policies, access controls Likelihood: Low

Consequence: Medium Risk Rating: Low-Medium (Low (\times) Medium)

**6. Assess Risk Levels for Each Risk Scenario with Additional Measures (Target Risk)**

Identify additional measures to further reduce the risk:

**Cyberattack**:Additional Measures: Regular software updates, security awareness training

Likelihood: Low Consequence: Medium Target Risk Rating: Low-Medium (Low (\times) Medium)

**Natural Disaster:**

**Additional Measures:** Enhanced physical security, redundant systems Likelihood: Low Consequence: Medium Target Risk Rating: Low-Medium (Low (\times) Medium)

**Employee Negligence:** Additional Measures: Regular training, stricter access controls

Likelihood: Low Consequence: Low Target Risk Rating: Low (Low (\times) Low)