1. Define the Context: Identify Assets to Protect

- **Sensitive Information**: Includes customer data, financial records, and intellectual property.
- **IT Infrastructure**: Servers, network devices, databases, and backup systems.
- **Physical Assets**: Computers, access control systems, and security equipment.
- **Reputation**: Maintaining customer trust and market position.
- **Human Resources**: Protecting employees and their access to information.

2. Define the Risk Matrix

Likelihood Descriptions:

- **Rare**: The event is highly unlikely to occur; may happen once in 10 years.
- **Unlikely**: The event is not expected but could occur; may happen once in 5 years.
- **Possible**: The event might occur occasionally; may happen once a year.
- **Likely**: The event is expected to occur in most circumstances; may happen multiple times a year.
- **Almost Certain**: The event is highly likely to occur; may happen frequently (e.g., monthly).

Consequence Descriptions:

- **Insignificant**: No significant impact on operations or finances; minor inconvenience.
- **Minor**: Some impact on operations but manageable; minor financial loss or reputational damage.
- **Moderate**: Noticeable impact on operations; moderate financial loss or temporary reputational damage.
- **Major**: Severe impact on operations; significant financial loss or reputational damage.
- **Severe**: Critical impact; could lead to major financial loss, legal implications, or long-term reputational damage.

3. Define Three Risk Scenarios

Cyber Attack (Data Breach)

- **Description**: Unauthorized access to sensitive information through a targeted cyberattack.
- **Likelihood**: Likely (due to increasing frequency of such attacks)
- **Consequence**: Severe (loss of sensitive data, legal liabilities)

Insider Threat (Employee Negligence)

- **Description**: An employee accidentally or intentionally leaking sensitive information.
- **Likelihood**: Possible (depends on employee awareness and access control)
- **Consequence**: Major (potential loss of data and reputational damage)

Physical Security Breach

- **Description**: Unauthorized access to the premises despite existing security measures.
- **Likelihood**: Unlikely (given existing fence and padlock)
- **Consequence**: Moderate (damage to property or theft of physical assets)

4. Assess Risk Rating for Each Scenario (Without Measures)

Risk Scenario	Likelihood	Consequence	Risk Rating
Cyber Attack (Data Breach)	Likely	Severe	Extreme
Insider Threat (Negligence)	Possible	Major	Very High
Physical Security Breach	Unlikely	Moderate	Medium

5. Assess Risk Rating with Existing Measures

Risk Scenario	Likelihood	Consequence	Risk Rating
Cyber Attack (Data Breach)	Possible	Severe	Very High
Insider Threat (Negligence)	Unlikely	Major	High
Physical Security Breach	Rare	Moderate	Low

6. Assess Risk Levels with Additional Measures

1. **Cyber Attack (Data Breach)**

- Additional Measures: Regular software updates, enhanced firewall and IDS/IPS, employee security training.
- **Target Risk Rating**: Medium (Likelihood: Unlikely, Consequence: Major)

2. **Insider Threat (Negligence)**
- Additional Measures: Implement access controls, regular employee training, data loss prevention (DLP) solutions.
- **Target Risk Rating**: Low (Likelihood: Rare, Consequence: Moderate)

3. **Physical Security Breach**
- Additional Measures: Install surveillance cameras, implement biometric access controls.
- **Target Risk Rating**: Very Low (Likelihood: Rare, Consequence: Minor)

7. Create a Risk Assessment Report

Introduction: This risk assessment report provides an overview of potential risks to [Client Name] and suggests mitigation strategies to protect its assets, ensuring the confidentiality, integrity, and availability of information.

Identified Assets:

- Sensitive information, IT infrastructure, physical assets, reputation, and human resources.

Risk Scenarios and Assessment:

1. **Cyber Attack (Data Breach)**
    - **Inherent Risk**: Extreme
    - **Current Risk**: Very High (with existing measures)
    - **Target Risk**: Medium (with additional measures)
2. **Insider Threat (Employee Negligence)**
    - **Inherent Risk**: Very High
    - **Current Risk**: High (with existing measures)
    - **Target Risk**: Low (with additional measures)
3. **Physical Security Breach**
    - **Inherent Risk**: Medium
    - **Current Risk**: Low (with existing measures)
    - **Target Risk**: Very Low (with additional measures)

Recommendations:

- Implement advanced technical controls, regular training, and comprehensive monitoring to further reduce risks.

- Review and update the risk assessment periodically to adapt to new threats and vulnerabilities.