Context - Asset(s) that we are trying to protect

The assests that need to be protected include:

- Confidential customer data
- Proprietary business information
- Financial information
- Intellectual property
- Physical infrastructure & equipment

Risk					Inherent Risk Rating			Current Risk Rating						Target Risk Rating					
ID	Title	Description	Sources or Causes of Risk	Consequences of Risk	Likelihood	Consequence	Risk Level	Existing control	Effectiveness of existing control measures	Likelihood	Consequence	Risk Level	Additional control measures	Effectiveness of additional control measures	Likelihood	Consequence	Risk Level
R01	Cyber attack	A cyberattack is a deliberate attempt by hackers to gain unauthorised access to a company's computer systems or networks, with the goal of stealing sensitive information, causing damage or disruption, or holding data ransom. The perceived sources for a cyberattack could include organised crime groups, nation-states, or individual hackers.	Organised crime groups, nation-states, or individual hackers	Data theft, system downtime, reputational damage, and financial losses.	Likely	Major	VERY HIGH	Firewalls, intrusion detection systems, antivirus software	**Firewalls -** Excellent control. Configured, maintained & tested properly. Highly effective and very fit for purpose. It substantially reduces the likelihood and/or consequence of the risk. It is cost effective. **Intrusion detection systems -** Moderate control. Configuration needs to be improved. **Antivirus -** Good control. Effective and fit for purpose. Configuration, maintenance and testing are good enough.	Possible	Major	VERY HIGH	**Treat** - reduce the likelihood or impact of risk by following these additional control measures: - Multi-factor authentication (MFA) - Penetration testing - Regular security awareness training **Transfer -** We can also transfer this risk to a 3rd party by letting a Managed Security Service Provider made the organisation's Security Information and Event Management (SIEM) tool.	**Excellent / Good / Moderate / Weak** **Multi-factor authentication (MFA)** - Good Control. This would add an extra layer of security by requiring users to provide additional authentication factors beyond a password. **Security Information and Event Management (SIEM)** - Excellent Control. This would enable real-time monitoring of security events and alerts for any suspicious activity, and help with incident response. **Penetration testing** - Good Control. This would simulate a cyberattack to identify vulnerabilities and weaknesses in the system and help to improve the existing controls. **Regular security awareness training** - Good Control. This would help to educate employees about cyber threats and best practices to prevent them, and reduce the risk of human error or negligence.	Unlikely	Moderate	MEDIUM
R02	Natural Disaster	A natural disaster is an unpredictable event caused by natural phenomena, such as earthquakes, cyclones, floods or bushfires, that can cause significant damage to a company's physical assets, disrupt operations, and pose a threat to employee safety.	Natural phenomena beyond human control	Property damage, loss of life, disruption of supply chains, and financial losses.	Rare	Severe	HIGH	Emergency response plans, backup power generators, and building reinforcement measures.	**Emergency Response Plans:** Good control. The organisation has established plans for responding to natural disasters, which reduces the consequence of the risk. **Back up Power generators:** Good control. Backup power generators can help ensure continuity of operations during a natural disaster, reducing the consequence of the risk. **Building Reinforcement Measures:** Excellent control. The organisation has taken steps to reinforce the building against natural disasters, reducing the likelihood and consequence of the risk.	Rare	Moderate	LOW	**Accept** - Acknowledge the risk and choose not to resolve, transfer or treat.	**Regular testing and maintenance:** Good Control. Regularly testing and maintaining emergency response plans, backup power generators, and building reinforcement measures to ensure they are effective and up-to-date.	Rare	Moderate	LOW
R03	Employee Negligence	Employee negligence arises when employees fail to follow established security protocols or engage in careless behavior that puts company assets at risk. This could include employees failing to properly store or dispose of sensitive information, sharing login credentials, or falling for phishing scams.	Employees who are not aware of the security protocols, don't take security seriously, or don't understand the consequences of their actions.	Data breaches, reputational damage, and financial losses.	Possible	Moderate	MEDIUM	Security awareness training, access Control	**Security Awareness Training:** Good control. Regular training sessions are carried out to educate employees about security threats and best practices to minimise the risks of employee negligence. **Access Control:** Excellent control. Measures have been put in place to ensure that employees only have access to the data and systems that are necessary for their job function.	Possible	Moderate	MEDIUM	**Treat** - reduce the likelihood or impact of risk by following these additional control measures: - Monitoring and auditing of employee actions - Role-based access control - Incident response plan	**Monitoring and auditing of employee actions:** Good Control. Regular monitoring and auditing of employee actions on company systems can help identify any suspicious activity or potential risks. **Role-based access control:** Excellent Control. Implement role-based access control to ensure employees only have access to the systems and data they need to perform their job functions, reducing the risk of accidental or intentional data breaches. **Incident response plan:** Good Control. Develop and implement an incident response plan to provide guidelines on how to respond to security incidents or data breaches caused by employee negligence.	Unlikely	Minor	LOW