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

1. **Asset: Customer Data**, **Description**: Personally Identifiable Information (PII), financial details, login credentials. Perceived Value / **Business Impact:** Personally Identifiable Information (PII), financial details, login credentials. Potential **Breaches:** Data breaches, identity theft, financial fraud.

2. **Asset: Financial Information. Description:** Banking details, payroll, internal financial records. **, Perceived Value/ Business Impact:** Very High – Direct financial losses, fraud, or account manipulation.**, Potential Risks:** Ransomware attacks, insider threats, fraud.

3. **Asset: Intellectual Property (IP). Description:** Proprietary research, software code, trade secrets.**, Perceived Value/ Business Impact:** High – Loss could impact competitive advantage and revenue.**, Potential Risks:** Data theft, espionage, insider threats.

4. **Asset: IT Infrastructure. Description:** Servers, databases, cloud storage, network devices. **, Perceived Value/ Business Impact:** High – Downtime could disrupt operations, affecting revenue and productivity.**, Potential Risks:** Denial-of-Service (DoS) attacks, misconfigurations, unauthorized access.

5. **Asset: Business Reputation Description:** Brand trust, customer relationships, and shareholder confidence.**, Perceived Value/ Business Impact:** Priceless – A security breach can severely damage reputation, affecting long-term success.**, Potential Risks:** Phishing, social engineering, data leaks.

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 measures	Effectiveness of exisitng control measures	Likelihood	Consequence	Risk Level	Additional control measures	Effectiveness of additional control measures	Likelihood	Consequence	Risk Level
R01	Phishing Attack	A malicious email tricks employees into revealing credentials, leading to unauthorized access.	Targeted phishing emails, lack of employee awareness.	Compromised accounts, data breaches, financial losses.	Almost Certain	Severe	EXTREME	Email filtering, antivirus, employee awareness training.	**Moderate.** The threats are more likely to harm the users.	Possible	Severe	VERY HIGH	**Treat** Multi-Factor Authentication (MFA), advanced phishing simulations	**Excellent -** MFA prevents unauthorized access, phishing simulations improve employee awareness.	Rare	Minor	VERY LOW
R02	Ransomware Attack	Malware encrypts critical files, demanding ransom for decryption. | Unpatched software, malicious email attachments.	Unpatched software, malicious email attachments.	Data loss, financial harm, operational disruption.	Almost Certain	Severe	EXTREME	Regular backups, endpoint protection, firewalls.	**Good** Although measures are sufficient, there are further space for the threats.	Possible	Moderate	MEDIUM	**Treat -** Network segmentation, Zero Trust security model.	**Excellent -** Network segmentation limits spread, Zero Trust enhances access control.	Rare	Moderate	LOW
R03	Insider Threat - Negligence	An employee misconfigures cloud storage, exposing sensitive data.	Poor access controls, lack of training.	Data leakage, compliance violations, reputational damage.	Possible	Moderate	MEDIUM	Role-Based Access Control (RBAC), security policies.	**Moderate** The insider threat are inevident in any organization.	Rare	Moderate	LOW	**Treat -** Continuous monitoring, real-time alerts for misconfigurations.	**Good -** Continuous monitoring detects misconfigurations, automated alerts reduce human error.	Unlikely	Minor	LOW
R04	Denial-of-Service Attack	Attackers overwhelm network resources, causing downtime.	Unprotected servers, lack of DDoS mitigation.	Service disruption, revenue loss.	Possible	Moderate	MEDIUM	Firewalls, rate-limiting, incident response plan.	**Good** Additional requirement for Cloud based security is required.	Possible	Moderate	MEDIUM	**Transfer** - Cloud-based DDoS protection services (CDN, Web Application Firewall).	**Excellent** - Cloud-based DDoS protection ensures availability, CDN mitigates high-traffic attacks.	Rare	Insignificant	VERY LOW
R05	Credential Theft via Dark Web	Leaked credentials are used to gain unauthorized access.	Employees reusing passwords, previous breaches.	Account takeover, business email compromise.	Likely	Severe	EXTREME	Password policies, dark web monitoring.	**Moderate** Physical security authentication standards are required.	Possible	Severe	VERY HIGH	**Avoid** - Enforce password managers, biometric authentication, regular credential monitoring & rotation.	**Good** - Password managers reduce reuse risks, biometric authentication strengthens security.	Unlikely	Minor	LOW