Asset, Vulnerability, and Threat Analysis Document

1. Introduction

This document provides a detailed analysis of the organization's key assets, identifies associated vulnerabilities, and outlines potential threats that could exploit those vulnerabilities. The purpose is to establish a foundational understanding for developing comprehensive risk mitigation and security strategies.

2. Asset Identification and Valuation

Assets are resources or items of value to the organization. They are categorized based on type, location, and importance to business operations (Confidentiality, Integrity, Availability - CIA triad).

2.1 Asset Categories

Asset Category	Description	Examples	CI
Information	Data critical to business operation, regulatory compliance, or competitive advantage.	Customer PII, Financial Records, Intellectual Property, Source Code	H M
Software/Applications	Business-critical applications, operating systems, and supporting software.	ERP System, CRM Platform, Web Servers, Database Management Systems	H (C
Hardware	Physical devices necessary for infrastructure and operations.	Servers, Workstations, Network Devices (Routers/Switches), Mobile Devices	M (C
Personnel	Employees, contractors, and their knowledge/access.	Key Administrators, Developers, Senior Management	H L (
Physical	Facilities, locations, and essential infrastructure components.	Data Center, Corporate Headquarters, Power Infrastructure	M (C

2.2 Critical Asset Inventory Snapshot

Asset Name	Category	Owner	Lo
Customer Database (DB-PROD-01)	Information/Software	IT Operations	Pr
Financial Reporting Server (FRS-01)	Software/Hardware	Finance	Co
Web Application Firewall (WAF-EXT-03)	Hardware	Network Security	Cl

3. Vulnerability Assessment

A vulnerability is a weakness in an asset or control that can be exploited by one or more threats. Vulnerabilities can be technical, administrative, or physical.

3.1 Common Technical Vulnerabilities

Vulnerability Type	Description	Affected Assets (Example)	Mi
Unpatched Software	Outdated operating systems or application versions missing critical security fixes.	ERP System, Workstations	St Au
Weak Authentication	Use of simple passwords, lack of Multi-Factor Authentication (MFA), or shared credentials.	Network Devices, Remote Access VPNs	En Ma pr
Configuration Errors	Default settings left unchanged, unnecessary services running, or overly permissive access controls.	Web Servers, Firewalls	Re of
Input Validation Flaws	Lack of proper sanitization of user input, leading to SQL Injection or XSS attacks.	Customer-facing Web Applications	Im Fi tra

3.2 Administrative and Physical Vulnerabilities

- **Lack of Security Awareness Training:** Employees susceptible to phishing or social engineering attacks (Personnel).
- **Poor Incident Response Plan:** Slow or ineffective response to a breach, increasing damage (Administrative).
- **Unsecured Server Room Access:** Easy physical access to critical hardware (Physical/Hardware).
- **Inadequate Data Backup:** No tested, off-site backup for critical information (Information/Software).

4. Threat Analysis

A threat is any potential danger that might exploit a vulnerability to breach security and negatively impact an asset. Threats can be internal or external, intentional or accidental.

4.1 Internal Threats

Threat Actor	Description	Target Assets	Po
Disgruntled Employee	Insider with authorized access seeking revenge or financial gain.	Information, Critical Databases	Da Re
Accidental User Error	Employee making a mistake (e.g., misconfiguration, clicking phishing link, unauthorized deletion).	Information, Software	Da int
Over-privileged Contractor	Third-party personnel with excessive access rights.	Software, Hardware	Ur int

4.2 External Threats

Threat Actor	Description	Target Assets	Po
Cyber Criminals	Organized groups seeking financial gain through hacking, ransomware, or fraud.	Information, Financial Systems	Fi Da

Threat Actor	Description	Target Assets	Po
State-Sponsored Actors	Highly skilled groups targeting Intellectual Property or critical infrastructure.	Intellectual Property, Source Code, ERP System	Es co
Script Kiddies	Opportunistic, low-skill attackers using readily available tools.	Web Applications, Unpatched Servers	De (D
Natural Disaster	Non-human threat (e.g., fire, flood, power outage).	Physical, Hardware	Co ex

5. Risk Mapping (Vulnerability-Threat Pairings)

Risk is the likelihood of a threat exploiting a vulnerability and the resulting impact. The table below maps specific vulnerabilities to potential threats.

Asset	Vulnerability	Potential Threat	Ri
Customer Database	Weak Authentication (No MFA)	Cyber Criminals (Credential Stuffing)	Hi
Web Application	Input Validation Flaws (SQLi potential)	Script Kiddies/Cyber Criminals	Me
Financial Server	Unpatched OS Software	State-Sponsored Actors (Zero-day/Exploit)	Hi
Personnel	Lack of Security Awareness	Accidental User Error (Phishing)	Me
Data Center	Single point of failure for power	Natural Disaster (Power Outage)	Me