



TRANSPORTATION COMPANY

VIETPHAT



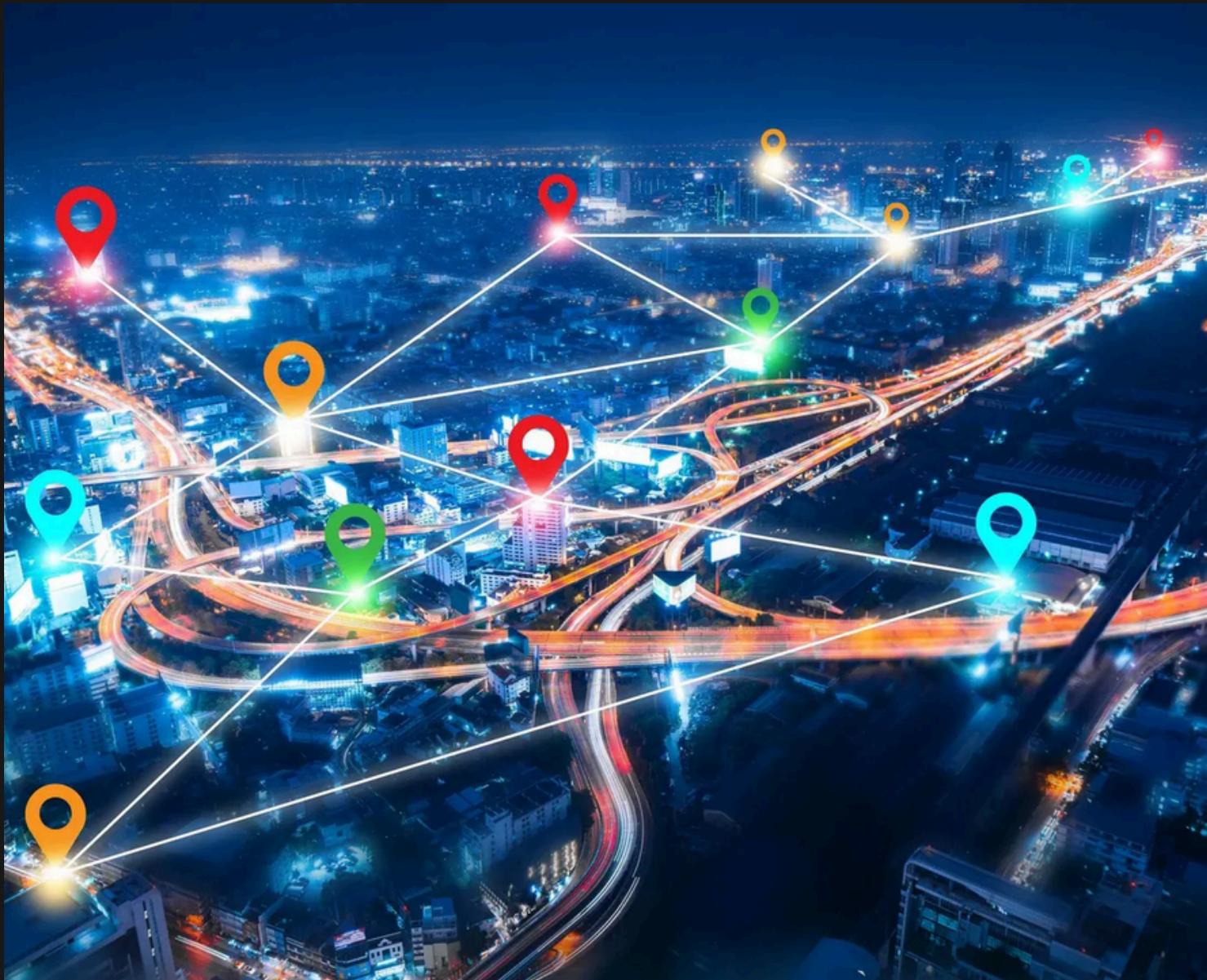
+123-456-7890



www.VietPhatTrans.com



VietPhat@gmail.com



WELCOME TO OUR COMPANY

Company Overview:

- Name: Viet Phat Transportation Company
- Industry: Transportation and Logistics
- Established: 2005
- Headquarters: Ho Chi Minh City, Vietnam
- Key Services/Products: Freight transportation, fleet management, logistics solutions, and warehousing services





OUR SYSTEM

Customer Data Management System

- Functions: Storing and processing customer data, transaction history, and communication records.
- Users: Approximately 500 users, including employees and third-party vendors.
- Technology: Python, SQL, Django framework.
- Version: 3.2.1
- Hosting Environment: Cloud (AWS)
- Vulnerabilities: Insufficient data encryption, potential for unauthorized access.





Network Infrastructure Management System

- Functions: Managing and securing network infrastructure, including servers and routers.
- Users: Approximately 100 network administrators and IT staff.
- Technology: Java, Kubernetes, Docker.
- Version: 2.1.0
- Hosting Environment: Hybrid (Cloud and On-premises)
- Vulnerabilities: Exposure to DDoS attacks.



GPS Tracking Software

- Functions: Tracking fleet vehicles, managing logistics and route planning.
- Users: Approximately 200 users including operations and logistics staff.
- Technology: .NET, SQL Server.
- Version: 4.5.3
- Hosting Environment: On-premises
- Vulnerabilities: Software vulnerabilities, lack of regular updates.





Web Servers

- Functions: Hosting the company's web applications and online services.
- Users: Public-facing, accessed by customers and partners.
- Technology: Node.js, React, MongoDB.
- Version: 1.8.7
- Hosting Environment: Cloud (Azure)
- Vulnerabilities: Web server software vulnerabilities, risk of SQL injection.





VPN

- Functions: Secure remote access to the company network.
- Users: IT staff and remote employees.
- Technology: OpenVPN, IPSec.
- Version: 2.9.4
- Hosting Environment: On-premises
- Vulnerabilities: Reverse VPN





REGULATORY COMPLIANCE

GDPR: General Data Protection
Regulation for data protection
and privacy in the EU.

01

02

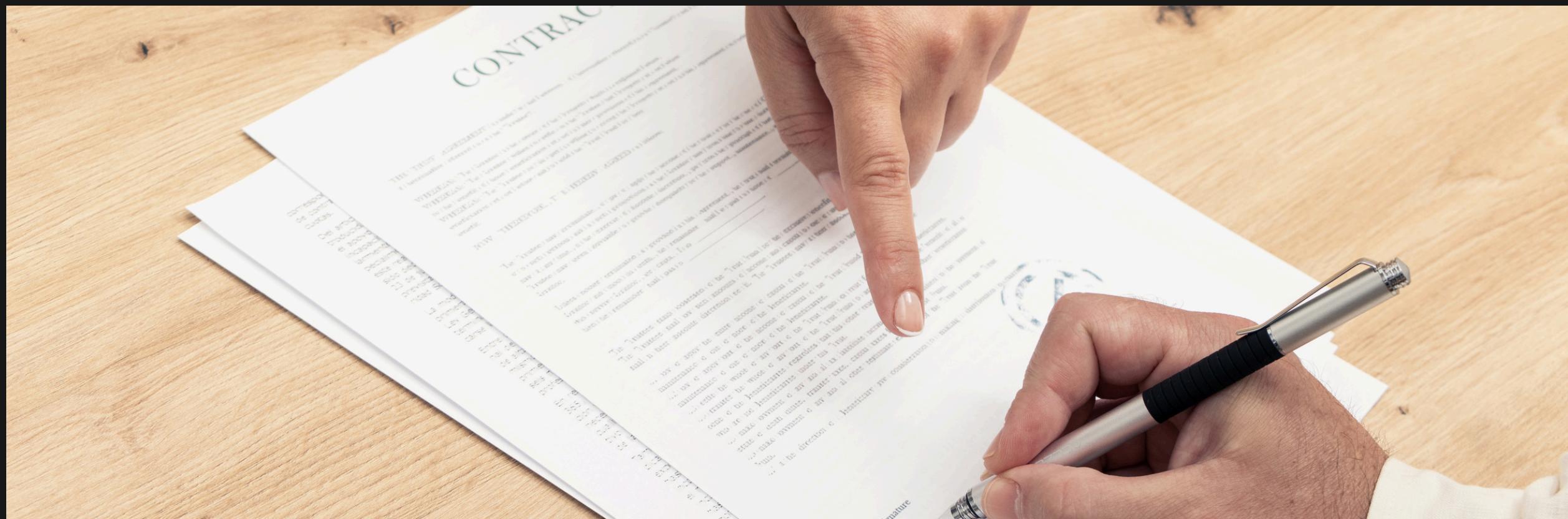
HIPAA: Health Insurance
Portability and Accountability Act
for healthcare data.

03

PCI DSS: Payment Card Industry
Data Security Standard for
payment processing.

04

SOX: Sarbanes-Oxley Act for
financial reporting and auditing.



PAST INCIDENTS

01

System Downtime (July 2022): Outage caused by a DDoS attack, affecting service availability for 6 hours.

02

Data Breach (March 2023): Compromised customer data due to a phishing attack, affecting 10,000 customers.

03

Compliance Violation (December 2021): Non-compliance with GDPR, leading to a fine of \$50,000.





SCOPE OF THE RISK ASSESSMENT PROJECT

Objective: To identify, assess, and mitigate risks associated with the Customer Data Management System, Network Infrastructure Management, GPS Tracking Software, Web Server, VPN Server .

Stakeholders:

- Internal: IT Department, Security Team, Compliance Team, Executive Management
- External: Third-party vendors, Regulatory bodies





ASSESSMENT AREAS

01

Asset Identification: Cataloging all assets within the system

- **Details:**
 - Customer databases
 - User access controls
 - Encryption keys
 - Backup systems





ASSESSMENT AREAS

02

Threat Analysis: Identifying potential threats

- **Details:**

- Malware and ransomware
- DDoS attacks





ASSESSMENT AREAS

03

Vulnerability Assessment: Evaluating weaknesses in the system

- **Details:**
 - Lack of data encryption
 - Insufficient user access controls
 - Outdated software versions
 - Misconfigured network service.





ASSESSMENT AREAS

04

Impact Analysis: Assessing the potential impact of different threats

- **Details:**
 - Data loss or corruption
 - Legal penalties
 - Financial losses





ASSESSMENT AREAS

05

Control Evaluation: Reviewing current controls and identifying gaps

- **Details:**
 - Firewalls and intrusion detection systems
 - Regular software updates
 - Data backup procedures





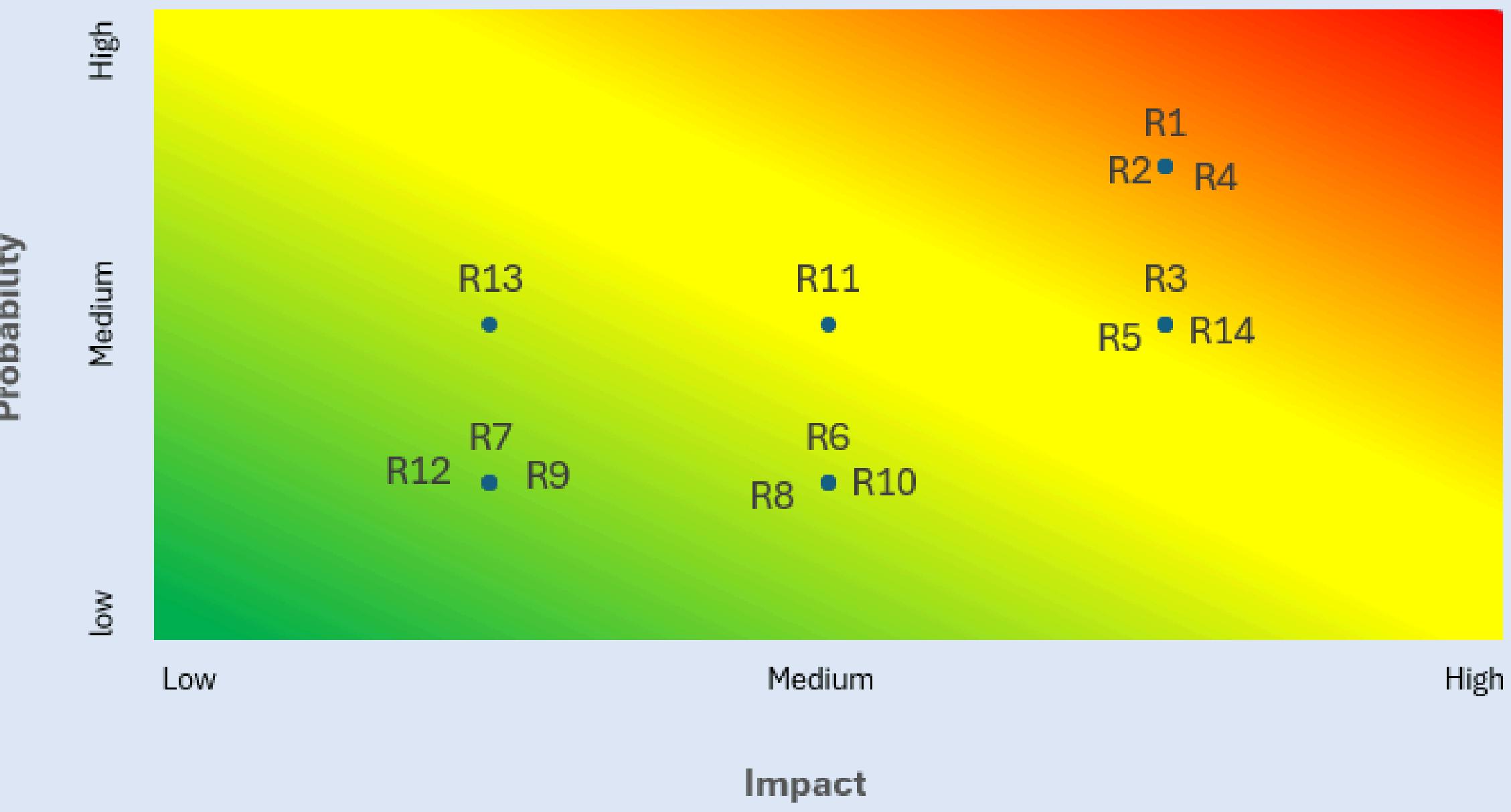
HEATMAP

RISK ASSESSMENT TABLE

	Risk	Impact	Probability
R1	Customer Data	3	3
R2	Network Infrastructure	3	3
R3	GPS Tracking Software	3	2
R4	Web Servers	3	3
R5	VPN Server	3	2
R6	Employee laptops	2	1
R7	Financial records	1	1
R8	Office workstations	2	1
R9	Email Server	1	1
R10	Ticketing System	2	1
R11	Cloud Services	2	2
R12	Social Media Accounts	1	1
R13	IOT Sensors	1	2
R14	Payment Processing System	3	2

1 Low
2 Medium
3 High

RISK ASSESSMENT



DETAILED RISK ASSESSMENT WITH IN-PLACE / PLANNED CONTROLS

Risk	In-Place Controls	Planned Controls
Data Breach Involving Customer Data	Encryption Multi-factor Authentication (MFA)	Enhanced Intrusion Detection Systems (IDS) Regular Security Audits
DDoS Attack on Network Infrastructure	Redundant Systems Regular Backups	Implement measures to prevent and mitigate distributed Improved Failover Mechanisms
GPS Tracking Software Exploitation	Secure API Integration Regular Security Assessments	Conduct thorough code reviews to identify and fix security issues. Regularly update the software to patch vulnerabilities.
Unauthorized Access to Software of Company	Access Controls Network Segmentation	Enhance access control with biometric verification. Regular Penetration Testing
Security Breach of Web Servers	Web Application Firewalls (WAF) Regular Security Updates	Encourage security researchers to report vulnerabilities. Implement tools to detect and respond to threats in real-time.
VPN Gateway Compromise	Strong Encryption MFA for VPN Access	Regular Security Audits VPN Gateway Upgrades
Theft or Loss of Laptops	Endpoint Security Software Encryption	Remote Wipe Capability Employee Training
Financial Fraud	Encryption Access Controls	Regular Audits Advanced Threat Protection
Malware Infection	Antivirus Software Email Filtering	User Training Network Monitoring
Email Phishing Attacks	Spam Filters User Training	Phishing Simulations Advanced Email Security Solutions
Attack on Ticketing System	Access Controls Regular Security Assessments	Regularly apply security patches to the ticketing system. Train users on secure practices when using the ticketing system
Unauthorized Access to Cloud Services	Use strong encryption for data stored and processed in the cloud. Define and enforce strict access controls for cloud services.	Regular Security Audits Implement tools to continuously monitor cloud compliance.
Hacking of Social Media Accounts	Strong Passwords Two-Factor Authentication (2FA)	Review account access and activity regularly. Security Training
Unauthorized Access to IoT Sensors	Isolate IoT devices on a secure network Regular Firmware Updates	Advanced Threat Detection Security Training
Unauthorized Access to Payment Processing Systems	Encryption Access Controls	Fraud Detection Tools Regular Security Audits

THANK YOU

