RISK ASSESSMENT WIZARD

Payment Processing

Risk Assessment

ASSESSMENT DETAILS

ESCALATION CONTACT:

Team Lead:	**Contact No.:**
Affected Parties:	

ACTIVITY OR SERVICE DETAILS

Purpose:	**Date:**
Benefit: Enhances customer satisfaction with seamless payment options. | Ensures secure and efficient handling of transactions. | Improves cash flow management through timely settlements. | Provides transparency with real-time transaction tracking. | Reduces risks of fraud with advanced security measures. | Supports business growth through efficient payment solutions.	

HAZARDS

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Compliance violations	Legal actions, Fines, Loss of trust	Minimizing compliance efforts can decrease administrative overhead and allow for more flexible operational strategies.	Stay updated with relevant regulations (e.g., PCI DSS, GDPR) and conduct regular compliance training for staff. Perform periodic audits and assessments to ensure adherence to legal requirements. **(ALL)**	Organization, Employees	Before Measure: **High** After Measure: **Med**
Data breaches	Compromised customer information, Reputational damage	Reducing investment in extensive data protection measures can lower operational costs and allocate resources to other business areas.	Employ robust encryption for data at rest and in transit. Utilize intrusion detection systems (IDS) and regularly update firewall protections. Conduct regular security audits and vulnerability assessments. **(ALL)**	Users, Customers, Organization	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Data loss	Inaccessible critical payment data, Customer dissatisfaction, Business interruptions	Reducing backup frequency and storage can lower operational costs and simplify data management processes.	Perform regular backups of all critical payment data and store them securely offsite. Test backup restoration processes periodically to ensure data can be recovered quickly. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**
Denial of service attacks	Service disruptions, Reduced system availability, Financial losses	Minimizing DDoS protection can lower security costs and focus resources on other strategic initiatives.	Implement DDoS protection services and establish traffic monitoring to detect and mitigate attacks. Develop incident response plans to address service disruptions swiftly. **(ALL)**	Organization, Users	Before Measure: **High** After Measure: **Med**
Fraudulent transactions	Financial loss, Increased chargebacks	Accepting some level of fraud risk can simplify transaction processes and reduce the need for extensive monitoring systems, potentially speeding up transaction times.	Implement real-time transaction monitoring and anomaly detection algorithms. Use machine learning to identify suspicious patterns and establish a fraud response team to investigate alerts promptly. **(ALL)**	Customers, Organization	Before Measure: **High** After Measure: **Med**
Inadequate backup procedures	Data loss, Extended recovery times, Business interruptions	Reducing backup frequency and complexity can lower storage costs and simplify data management practices.	Establish automated, regular backup schedules with secure storage solutions. Verify backup integrity and conduct periodic restoration tests to ensure data can be recovered effectively. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**
Inadequate encryption	Weak data protection, Susceptibility to attacks, Data exposure	Reducing encryption standards can lower computational overhead and speed up data processing times.	Use industry-standard encryption protocols (e.g., AES-256) for all sensitive data. Regularly review and update encryption methods to address emerging threats. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Inadequate logging and monitoring	Missed detection of threats, Delayed incident response, Escalated damages	Minimizing logging and monitoring can reduce storage and processing costs, streamlining IT operations.	Establish comprehensive logging for all payment processing activities. Utilize centralized monitoring systems to detect and respond to suspicious activities in real-time. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**
Inadequate monitoring of emerging threats	Delayed threat identification, Escalated risks, Reputational harm	Minimizing monitoring efforts can lower operational costs and allow the organization to focus resources on other strategic areas.	Establish a dedicated threat intelligence team to monitor and analyze emerging security threats. Integrate threat intelligence into security operations to proactively address potential risks. **(ALL)**	Security Teams, Organization	Before Measure: **High** After Measure: **Med**
Inadequate segregation of duties	Errors in payment processing, Increased fraud risks, Compliance violations	Allowing more flexibility in role assignments can enhance operational efficiency and reduce administrative overhead.	Assign separate roles and responsibilities for critical payment processing tasks. Implement approval workflows and conduct regular audits to ensure compliance. **(ALL)**	Employees, Organization	Before Measure: **High** After Measure: **Med**
Inadequate transaction reconciliation	Unresolved discrepancies, Financial misstatements, Revenue loss	Simplifying reconciliation processes can reduce operational costs and improve transaction processing speed.	Implement automated reconciliation processes to match transactions accurately. Conduct regular audits to identify and resolve discrepancies promptly. **(ALL)**	Organization, Finance Teams	Before Measure: **High** After Measure: **Med**
Insider threats	Data leaks, Unauthorized system changes, Financial fraud	Reducing monitoring and control measures can foster a more trusting and open workplace environment, potentially enhancing employee morale.	Monitor and log all employee activities related to payment processing. Implement strict access controls and conduct background checks during hiring. Foster a culture of security awareness. **(ALL)**	Employees, Organization	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Insufficient encryption key management	Compromised encryption keys, Data exposure, Unauthorized decryption	Simplifying key management can decrease operational costs and reduce the complexity of encryption processes.	Implement strict policies for encryption key generation, storage, rotation, and destruction. Use hardware security modules (HSMs) to manage and protect keys securely. **(ALL)**	Organization, IT Teams	Before Measure: **High** After Measure: **Med**
Insufficient encryption standards for APIs	Data interception, Unauthorized access, System breaches	Reducing encryption standards can improve API performance and decrease computational resource requirements.	Use strong encryption protocols (e.g., TLS 1.3) for all API communications. Regularly assess and update API security measures to protect against evolving threats. **(ALL)**	API Developers, Organization	Before Measure: **High** After Measure: **Med**
Lack of employee training	Human errors, Security policy violations, Compliance gaps	Reducing training programs can decrease operational costs and allocate resources to other business development areas.	Develop comprehensive training programs focused on security best practices, regulatory compliance, and payment processing protocols. Schedule regular refresher courses and assessments. **(ALL)**	Employees, Organization	Before Measure: **High** After Measure: **Med**
Lack of incident response plan	Delayed threat mitigation, Increased recovery times, Escalated damages	Foregoing extensive incident response planning can lower operational costs and reduce the time spent on preparedness activities.	Develop and regularly update a detailed incident response plan. Conduct drills and simulations to ensure readiness and effective coordination during actual incidents. **(ALL)**	Organization, Employees	Before Measure: **High** After Measure: **Med**
Lack of vendor risk management	Compromised vendor systems, Supply chain attacks, Service interruptions	Reducing vendor oversight can streamline partnerships and lower administrative efforts associated with vendor management.	Develop a comprehensive vendor risk management program, including security assessments and ongoing monitoring of third-party providers. Establish clear contractual security requirements. **(ALL)**	Organization, Vendors	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Malware infections	System damage, Data corruption, Unauthorized access	Lower investment in anti-malware tools can decrease IT expenditure and simplify system management.	Deploy advanced anti-malware solutions and regularly update them. Conduct routine system scans and educate employees on safe browsing and downloading practices. **(ALL)**	Organization, Employees	Before Measure: **High** After Measure: **Med**
Mobile payment vulnerabilities	Compromised mobile apps, Fraudulent transactions, Data breaches	Allowing some vulnerabilities can expedite mobile payment feature deployment and enhance user accessibility without extensive security constraints.	Secure mobile payment applications with strong encryption, regular updates, and secure coding practices. Conduct security testing and implement fraud detection mechanisms specific to mobile platforms. **(ALL)**	Mobile Users, Organization	Before Measure: **High** After Measure: **Med**
Network vulnerabilities	Exploitation of system weaknesses, Unauthorized access, System disruptions	Simplifying network security measures can decrease complexity and reduce IT maintenance costs.	Regularly scan and monitor network infrastructure for vulnerabilities. Implement segmentation and use secure communication protocols to minimize attack surfaces. **(ALL)**	Organization, Users	Before Measure: **High** After Measure: **Med**
Outdated software	Unpatched vulnerabilities, Compatibility issues, System instability	Continuing to use existing software can minimize transition costs and reduce the need for extensive training on new systems.	Maintain an inventory of all software used in payment processing and ensure timely updates and patches. Replace legacy systems with modern, supported alternatives when necessary. **(ALL)**	Organization, Employees	Before Measure: **High** After Measure: **Med**
Payment gateway failures	Transaction delays, Customer dissatisfaction, Revenue loss	Accepting occasional gateway issues can reduce the complexity and cost of maintaining multiple payment systems.	Utilize multiple payment gateways to distribute transaction load. Monitor gateway performance continuously and establish rapid response teams to address any failures immediately. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Phishing attacks	Compromised credentials, Unauthorized access, Financial loss	Lower investment in phishing defenses can decrease operational costs and simplify communication systems.	Provide regular training to employees on recognizing phishing attempts. Deploy advanced email filtering solutions and conduct simulated phishing exercises to reinforce awareness. **(ALL)**	Employees, Organization	Before Measure: **High** After Measure: **Med**
Physical security breaches	Unauthorized access to facilities, Theft, Data loss	Lower investment in physical security can reduce overhead costs and simplify facility management.	Secure data centers and office spaces with access controls, surveillance cameras, and security personnel. Implement policies for the safe handling and disposal of physical media containing payment data. **(ALL)**	Organization, Employees	Before Measure: **High** After Measure: **Med**
Software vulnerabilities	Exploitation of weaknesses, Unauthorized access, Data breaches	Accepting some software vulnerabilities can decrease maintenance efforts and allow for faster deployment of new features.	Maintain an updated patch management system to apply security updates promptly. Conduct regular code reviews and vulnerability assessments to identify and fix weaknesses. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**
System downtime	Transaction interruptions, Loss of business continuity	Allowing occasional downtime can reduce costs associated with maintaining high-availability systems and infrastructure.	Establish redundant systems and failover protocols. Regularly maintain and update infrastructure. Implement robust disaster recovery and business continuity plans. **(ALL)**	Organization, Users	Before Measure: **High** After Measure: **Med**
Third-party vulnerabilities	Compromising payment data, Supply chain attacks, Service interruptions	Relying more on third parties can allow the organization to focus on core competencies and reduce the burden of managing additional security layers.	Conduct thorough due diligence and regular security assessments of all third-party vendors. Establish clear security requirements and contractual obligations for partners handling payment data. **(ALL)**	Organization, Vendors	Before Measure: **High** After Measure: **Med**

HAZARD	RISK	RISK BENEFIT	MEASURE	RISK TO	RISK LEVEL
Unauthorized data modification	Tampered payment data, Reconciliation issues, Fraud risks	Lowering controls on data modification can enhance flexibility in data management and reduce administrative burdens.	Implement strict access controls and audit trails to monitor changes to payment data. Use checksums and data integrity verification methods to detect unauthorized modifications. **(ALL)**	Organization, Customers	Before Measure: **High** After Measure: **Med**
Weak authentication mechanisms	Compromised accounts, Unauthorized access, Data theft	Simplifying authentication processes can improve user experience and reduce the complexity of access management systems.	Strengthen authentication methods by implementing MFA, using biometrics, and enforcing complex password policies. Regularly review and update authentication protocols. **(ALL)**	Users, Employees	Before Measure: **High** After Measure: **Med**
Unauthorized access	Compromised accounts, Data exposure	Allows for streamlined user access processes without the complexity of extensive security protocols, potentially enhancing user convenience and operational speed.	Implement multi-factor authentication (MFA) for all users accessing payment systems. Regularly update and enforce strong password policies. Conduct periodic access reviews and revoke access for inactive or unauthorized users promptly. **(ALL)**	Users, Employees, Customers	Before Measure: **High** After Measure: **Low**
Unforseen hazard	Illness, injury, death		Ongoing dynamic risk assessment conducted by all relevant personnel. Any identified potential risks should be immediately reported to the appropriate supervisor or risk manager, and corrective action should be taken as necessary. **(ALL)**	All	**N/A**

NOTES

Extra notes & evaluation:

NOTES

Extra notes & evaluation:

Completed by	Reviewed/Approved by	Risk Assessment Date	Review Required Date