Threat and Vulnerability Identification

Asset Name	Asset Description	Associated Threats	Potential Vulnerabilities	Mitigation Notes
E-commerce Platform (Website + Mobile App)	Customer-facing sales platform hosted on AWS; integrates with PayPal & Afterpay.	Web attacks, account takeover, data exfiltration, DDoS.	Weak API authentication, insecure session management, inadequate WAF rules, outdated plugins.	WAF tuning, MFA for accounts, secure API gateways, regular pentesting.
Customer Data (PII + Tokenized Payments + Behavioural Analytics)	Names, addresses, emails, phone numbers, loyalty data, payment tokens.	Data breach, credential compromise, insider misuse, API scraping.	Overshared access, inadequate encryption at rest, weak RBAC, BYOD access.	Zero Trust, DLP, stricter RBAC, encryption audits.
Salesforce CRM	Customer management, loyalty, marketing automation.	Credential theft, API abuse, misconfigured access permissions.	Misconfigured OAuth, lack of MFA enforcement, shared accounts.	Salesforce security review, SCIM provisioning, enforce MFA.
SAP ERP (Inventory, Finance, HR)	Core business functions and sensitive employee information.	Privilege escalation, ransomware, insider threats.	Legacy modules, non-segmented network access, VPN exposure.	Network segmentation, patching, privileged access management.
Cloud-Connected POS Systems (85 Stores)	In-store transaction & payment systems integrated with cloud backend.	Compromised POS terminals, MITM attacks, payment token theft.	Weak store Wi-Fi, outdated firmware, insufficient endpoint protections.	EDR on POS, firmware patching, network isolation.

Risk Criteria

The below explains what each item in the Risk Assessment means.

Criteria	Description
Risk Description	Detailed explanation of the scenario, what could go wrong, and why it matters.
Assets at Risk	The information, system, or service impacted (e.g. customer data, VDI environment).

Criteria	Description
Threat	Who or what could cause the risk (e.g., insider, cybercriminal, accident, malware). The action or event (e.g., data exfiltration, privilege misuse, physical theft).
Vulnerability	Weakness – the gap or condition that enables the threat (e.g., extended idle session, clipboard sharing).
Existing Controls	Current safeguards in place (e.g., MFA, logging, endpoint DLP).
Inherent Risk Rating	Risk level before any mitigations are applied.
Residual Risk Rating	Risk level after current controls are considered.
Likelihood	The probability of occurrence (e.g., Rare, Possible, Likely).
Consequence	Severity – level of damage if realised (e.g., Minor, Moderate, Major, Extreme).
Rating	The outcome of the risk likelihood and consequence evaluation.
Mitigations	Treatment Plan – actions to reduce, transfer, avoid, or accept the risk.
Risk Owner	Person or role accountable for managing the risk (e.g., the person who uses the software)

Risk Assessment

Risk 1 – Customer Data Breach via Compromised E-commerce Platform

Risk Details			
Risk ID	RN-001	**Date Identified**	2025
Risk Title	Web Application Compromise Leading to Customer Data Exposure	**Review Date**	Quarterly
Risk Identification			
Risk Description	Attackers exploit vulnerabilities in the e-commerce web application/API to exfiltrate PII, tokenised payment details and loyalty data.		
Assets at Risk	Customer PII, behavioural analytics, payment tokens, user accounts.		
Threat	Cybercriminals, botnet operators, credential stuffers.		

Vulnerability	Weak authentication, outdated web components, insufficient WAF rules.		
Existing Controls	Basic firewalls, antivirus, AWS hosting security.		
Inherent Risk Analysis			
Likelihood	**Consequence**	**Inherent Risk Rating**	
Likely (4)	Major (4)	HIGH	
Residual Risk Analysis			
Likelihood	**Consequence**	**Residual Risk Rating**	
Possible (3)	Major (4)	HIGH	
Risk Treatment			
Mitigations	Enforce MFA for all customer accounts. Deploy enhanced WAF with bot protection. Quarterly pentesting. Harden API authentication and rate limiting.		
Risk Monitoring and Review			
Risk Owner	CISO / Head of Digital Platforms		

Risk 2 – Compromise of SAP ERP via Remote Access (VPN + BYOD)

Risk Details			
Risk ID	RN-002	**Date Identified**	2025
Risk Title	Remote Access Breach Leading to SAP Compromise	**Review Date**	Quarterly
Risk Identification			
Risk Description	Attackers gain access through compromised VPN + BYOD device, escalate privileges to SAP and access financial/HR records.		
Assets at Risk	Finance data, HR records, inventory data, employee information.		
Threat	Threat actors using credential theft, BYOD malware.		
Vulnerability	Weak endpoint control on BYOD, VPN without device posture checks, over-permissive RBAC.		
Existing Controls	Antivirus, basic VPN access, security awareness training.		
Inherent Risk Analysis			
Likelihood	**Consequence**	**Inherent Risk Rating**	
Possible (3)	Extreme (5)	HIGH	

Residual Risk Analysis		
Likelihood	**Consequence**	**Residual Risk Rating**
Unlikely (2)	Major (4)	MEDIUM
Risk Treatment		
Mitigations	Implement Zero Trust access (device compliance checks). Enforce MDM for BYOD devices. SAP RBAC review & least privilege. VPN hardening with conditional access.	
Risk Monitoring and Review		
Risk Owner	IT Security Manager (Infrastructure)	

Risk 3 – Third-Party Vendor Breach Affecting Customer Email and Loyalty Data

Risk Details			
Risk ID	RN-003	**Date Identified**	2025
Risk Title	Third-Party Data Leak (Marketing Vendor / Logistics Integrations)	**Review Date**	Semi-annual
Risk Identification			
Risk Description	A third-party provider suffers a breach, exposing RetailNova customer PII or loyalty data, similar to the 2025 incident that leaked 5,000 customer emails.		
Assets at Risk	Customer email addresses, loyalty profiles, marketing data.		
Threat	Third-party compromise, supply-chain attacks..		
Vulnerability	Weak vendor security, over-permissioned API integrations, lack of data minimisation.		
Existing Controls	Vendor agreements, basic audits, antivirus, firewalls.		
Inherent Risk Analysis			
Likelihood	**Consequence**	**Inherent Risk Rating**	
Likely (4)	Moderate (3)	HIGH	
Residual Risk Analysis			
Likelihood	**Consequence**	**Residual Risk Rating**	
Possible (3)	Moderate (3)	MEDIUM	
Risk Treatment			

Mitigations	Implement Vendor Security Assessment Framework. Enforce API token rotation & least-privilege. Continuous monitoring of third-party access. Data minimisation policies.
Risk Monitoring and Review	
Risk Owner	Governance, Risk & Compliance (GRC) Lead

Summary (for Executive Briefing)

RetailNova faces significant cybersecurity exposure driven by:

- Large customer dataset (PII + payment tokens)
- BYOD + remote access risks
- Reliance on third-party cloud services
- E-commerce and POS attack surfaces
- History of recent incidents
- Rapid operational growth with lagging security maturity

Highest Priority Risks:

- Customer data breach (HIGH)
- SAP ERP compromise (HIGH)
- Third-party vendor data leak (MEDIUM–HIGH)

Recommended Prioritised Actions

Immediate (0–3 months)

- Enforce MFA across all systems
- Harden web application + WAF rules
- Deploy EDR across all endpoints & POS
- Lock down VPN with device compliance

Medium Term (3–6 months)

- Full RBAC review for SAP & Salesforce

- Vendor security governance framework
- Improve monitoring (SIEM + anomaly detection)

Long Term (6–12 months)

- Zero Trust network segmentation
- Continuous pentesting of e-commerce platform
- Data minimisation & lifecycle management

Cybersecurity Risk Prioritisation Matrix

Understanding the Likelihood Rating

The table below provides the categories and ratings for likelihood:

Likelihood Ratings	Description	Criteria
Rare (1)	Exceptional circumstances only	May occur only in very unusual situations
Unlikely (2)	Possible, but not expected	Could happen but not typical; requires specific conditions (e.g. targeted phishing bypassing all filters).
Possible (3)	Might occur at some point	Has occurred in similar organisations; realistic but not frequent (e.g. ransomware attempt on enterprise endpoint).
Likely (4)	Will probably occur in most circumstances	Expected to happen periodically (e.g. phishing emails, credential stuffing attempts).
Almost Certain (5)	Expected to occur frequently	Has occurred multiple times, highly predictable (e.g. malware probes, daily scanning activity).

Understanding the Consequence Ratings Table

The table below provides the categories and ratings for impacts:

Consequence Rating	Description	Criteria
Insignificant (1)	Negligible impact	No compromise of sensitive data, no disruption, minimal financial or reputational impact.
Minor (2)	Small impact	Limited operational disruption; minimal data exposure (non-sensitive data); easily contained.
Moderate (3)	Noticeable impact	Partial service disruption; limited sensitive data exposure; moderate cost or compliance breach.
Major (4)	Severe impact	Significant outage of critical systems; large-scale sensitive data breach; regulatory non-compliance with penalties.

Extreme (5)	Catastrophic impact	Extended enterprise-wide outage; compromise of PROTECTED/SECRET data; severe financial/reputational damage; possible criminal or regulatory prosecution.

The 5x5 Risk Matrix

Use this 5x5 risk matrix to evaluate and prioritise cybersecurity risks. For each identified risk, assess its likelihood (1 = Rare, 5 = Almost Certain) and impact (1 = Insignificant, 5 = Critical). Plot the risk in the matrix and use the result to guide mitigation priorities.

Risk Levels

Likelihood ↓ Impact →	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
5 – Almost Certain	**MEDIUM**	**HIGH**	**HIGH**	**EXTREME**	**EXTREME**
4 – Likely	**MEDIUM**	**MEDIUM**	**HIGH**	**HIGH**	**EXTREME**
3 – Possible	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**HIGH**
2 – Unlikely	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
1 – Rare	**LOW**	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**

- **Low** – Acceptable; manage by routine controls and monitoring.
- **Medium** – Requires management attention; additional controls may be needed.
- **High** – Significant; must be treated with priority, monitored closely, and escalated to senior management.
- **Extreme** – Unacceptable; immediate executive-level attention and remediation required.