Security and Risk Management July 2025 B

RISK IDENTIFICATION REPORT – PAMPERED PETS

Team Name:	- Group 5
Team Members:	- Devendra Shrestha - Pragadheesh Marimuthu

Executive Summary

Pampered Pets, a traditional pet retail business, faces significant cybersecurity and operational risks as it contemplates digital transformation. This report applies the **ISO 31000 risk management framework** alongside **STRIDE** and **DREAD** threat modelling frameworks to systematically assess risks inherent in digital adoption. While supply chain and financial considerations are acknowledged, the priority lies in developing a robust cybersecurity posture.

Industry data supports that an online presence can boost revenues by **up to 50%** and reduce procurement costs by **up to 44%** (Spendedge, 2024; Fortune Business Insights, 2024). However, the digital shift introduces new vulnerabilities, including cyber-attacks and regulatory challenges, necessitating structured risk assessment and mitigation.

A phased, security-focused approach is therefore recommended to enable safe digital growth and operational resilience.

1. Introduction

Pampered Pets relies heavily on in-person sales, supported by outdated IT systems and unsecured wireless networks shared with personal devices. This exposes the company to traditional operational risks and escalating cybersecurity threats that could compromise business continuity and customer trust.

With digital transformation accelerating across retail sectors, failure to adopt secure e-commerce and ERP platforms risks significant customer attrition, **estimated at around 33%**, and reputational harm (Kovaitė and Stankevičienė, 2019). This report provides a structured assessment of these cybersecurity risks balanced with necessary financial and supply chain considerations.

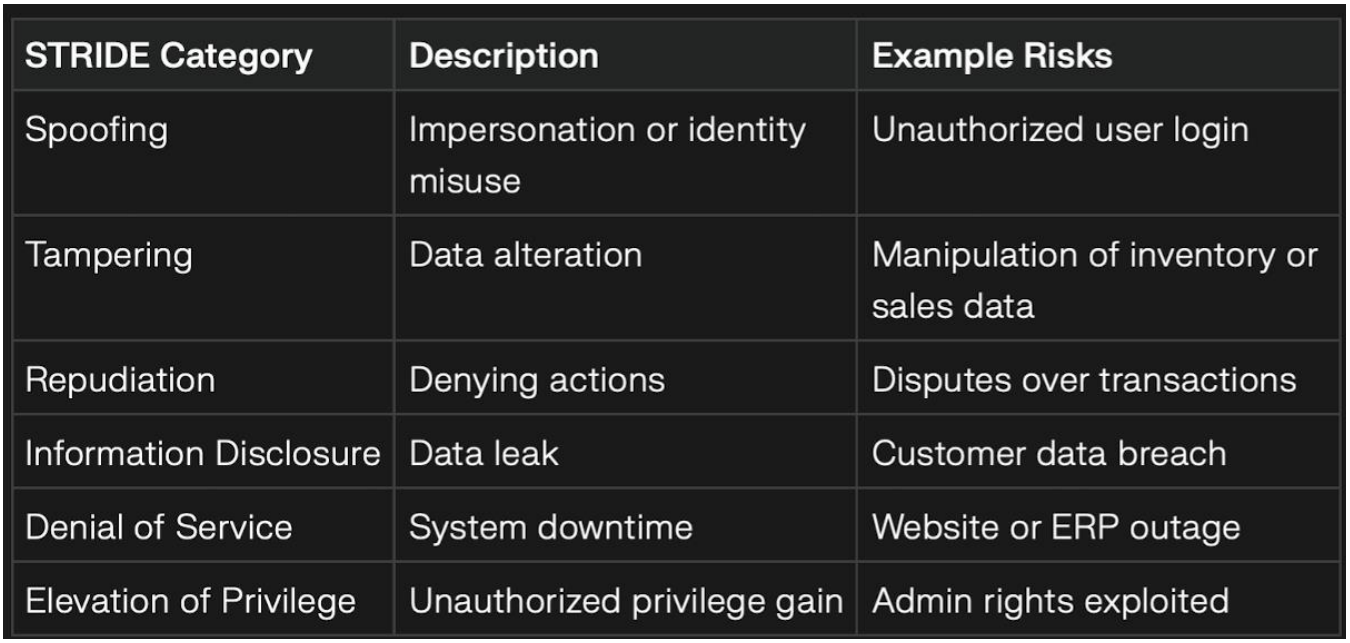
A clear focus is maintained on cybersecurity risk identification and mitigation rather than on detailed financial forecasts, in line with module guidance.

2. Methodology

This risk assessment follows the **ISO 31000:2018 framework**, ensuring comprehensive identification, analysis, and prioritisation of risks (ISO, 2018).

To deepen the cybersecurity focus, the report integrates the **STRIDE** and **DREAD** threat modelling frameworks:

- **STRIDE** categorises threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Shevchenko et al., 2018), covering attack vectors relevant to e-commerce and ERP systems.



STRIDE Category	Description	Example Risks
Spoofing	Impersonation or identity misuse	Unauthorized user login
Tampering	Data alteration	Manipulation of inventory or sales data
Repudiation	Denying actions	Disputes over transactions
Information Disclosure	Data leak	Customer data breach
Denial of Service	System downtime	Website or ERP outage
Elevation of Privilege	Unauthorized privilege gain	Admin rights exploited

Table 1: A table summarising STRIDE threat categories with example risks tailored to Pampered Pets.

- **DREAD** supports prioritisation by evaluating Damage, Reproducibility, Exploitability, Affected Users, and Discoverability, informing focused mitigation planning.

A qualitative 3x3 risk matrix is used to translate threat model findings into prioritisation levels (low, medium, high), guiding resource allocation without complex quantitative methods.

3. Cybersecurity Risk Assessment

3.1 Threat Landscape and Vulnerabilities

Pampered Pets' current IT setup includes unsecured Wi-Fi shared by staff devices, outdated hardware lacking up-to-date antivirus protections, and no automated data backup system. These conditions create risks, including:

- **Malware and Ransomware Infections:** Potential for data corruption or system lockout (OWASP, 2023).
- **Unauthorised Access (Spoofing):** Risk of attackers impersonating users due to weak authentication.
- **Data Tampering**: Potential unauthorised modifications to sales or inventory data.
- **Information Disclosure:** Risk of exposing sensitive customer and payment data.
- **Denial of Service (DoS) Attacks:** Threats that could incapacitate online platforms, damaging revenue and reputation.
- **Elevation of Privilege:** Risk of unauthorised escalation of access rights within ERP or other systems.

3.2 Risk Prioritisation via STRIDE and DREAD

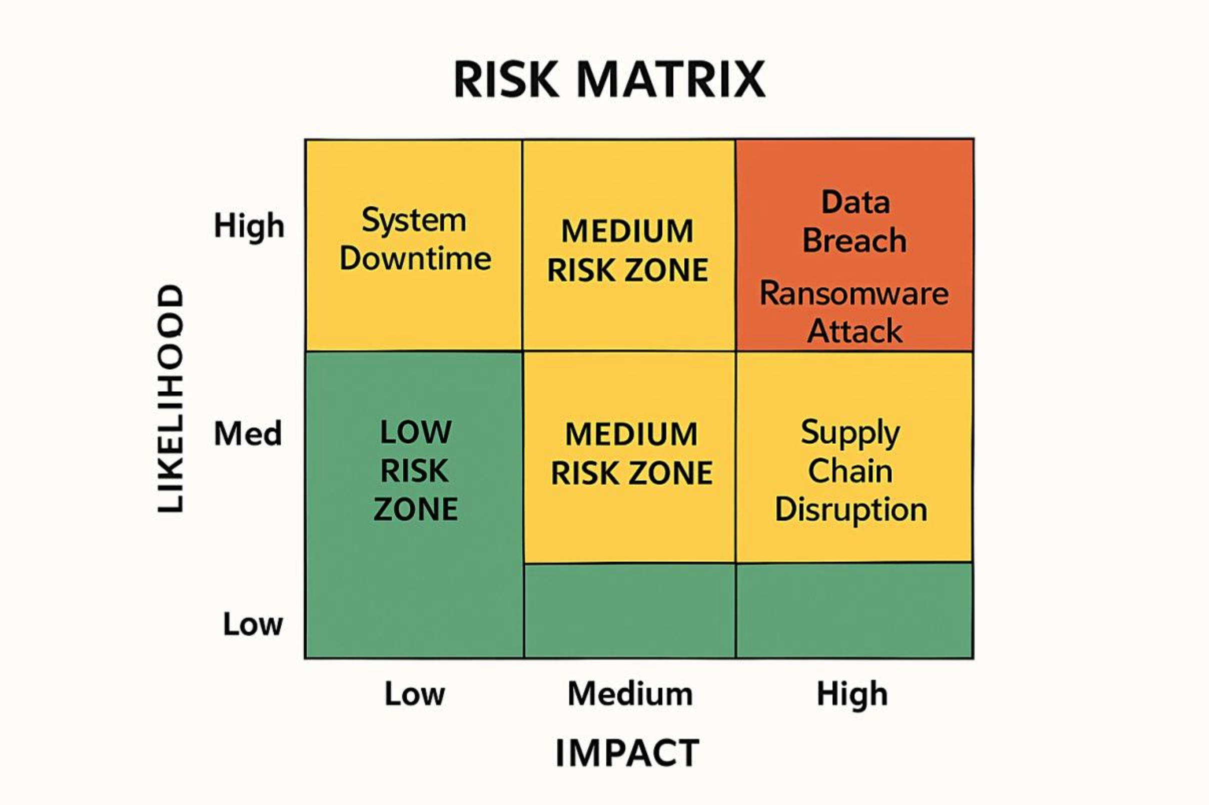


Figure 1: A risk matrix illustrating the likelihood vs. impact of key cybersecurity and operational risks, highlighting high-priority issues.

STRIDE categories informed identification of vulnerabilities, while **DREAD** scoring prioritised the risks as follows:

- Denial of Service impact on sales uptime (high priority).
- Data breaches exposing sensitive customer information (high priority).
- Elevation of privilege within systems (high priority).
- Spoofing and tampering are medium priority, with repudiation monitored but lower risk.

4. Risk Mitigation Recommendations

- **Network Security:** Segregate business Wi-Fi from personal device networks; implement WPA3 encryption and robust firewall policies.
- **Endpoint Security:** Deploy enterprise antivirus and anti-malware with real-time monitoring capabilities.
- **Access Controls:** Enforce role-base access control, strong password policies, and multi-factor authentication.
- **Data Protection:** Encrypt data both in transit and at rest; implement automated secure backups stored offsite or in cloud services.
- **DoS Mitigation:** Use anti-DDoS services to protect critical online platforms.
- Training: Conduct regular cybersecurity awareness and phishing simulation training for all staff.

- **Compliance:** Maintain adherence to **PCI-DSS** for payment processing and **GDPR** for personal data protection, supported by audits and documented policies (ICO, 2024).
- **Incident Management:** Develop and regularly test comprehensive disaster recovery and incident response plans with defined performance targets (RTO and RPO).

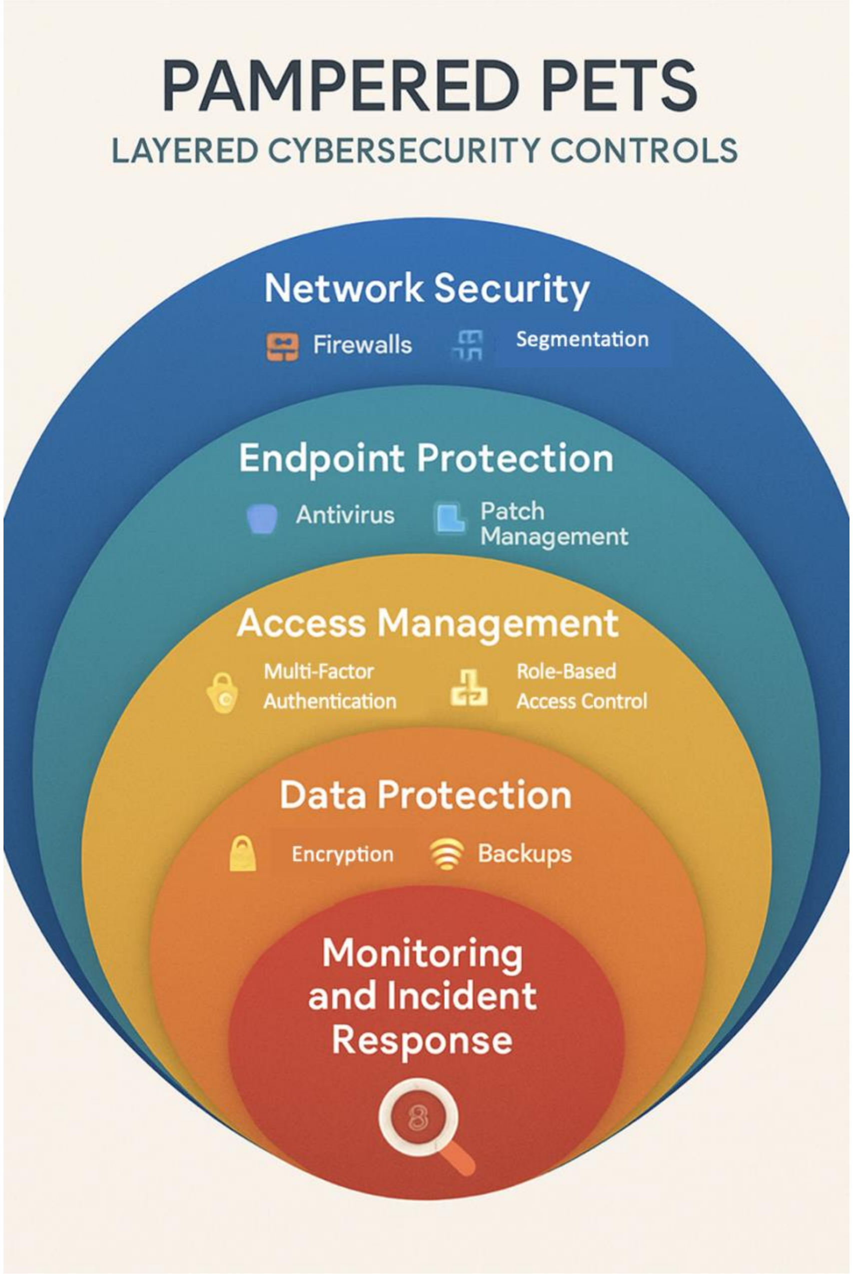


Figure 2: Layered Cybersecurity Controls Diagram illustrating a defence-in-depth strategy for Pampered Pets, featuring successive security layers from network protection and endpoint defence to access management, data encryption, and continuous monitoring with incident response.

5. Supply Chain and Financial Considerations

While cybersecurity is the main focus, digital transformation impacts procurement and finances:

- Transitioning to international suppliers can reduce costs by **up to 44%** due to labour and material cost advantages and bulk purchasing (Spendedge, 2024).
- Local suppliers ensure quality but have scalability and cost limitations.
- A hybrid supply chain strategy is recommended for balancing cost-effectiveness, quality, and operational resilience.

Estimated initial investment for digital platforms ranges between **£2,400** and **£4,500** with ongoing maintenance and training costs between **£500** and **£900** annually, manageable within business projections.

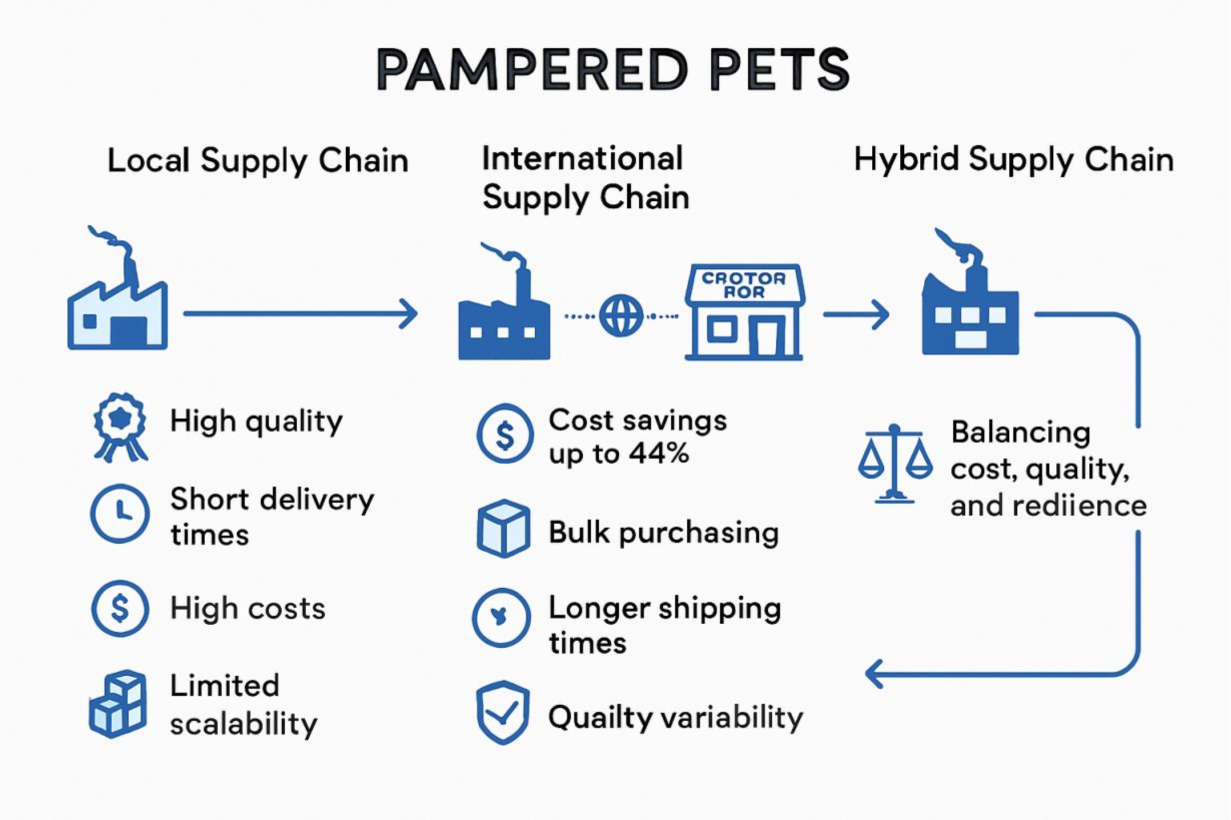
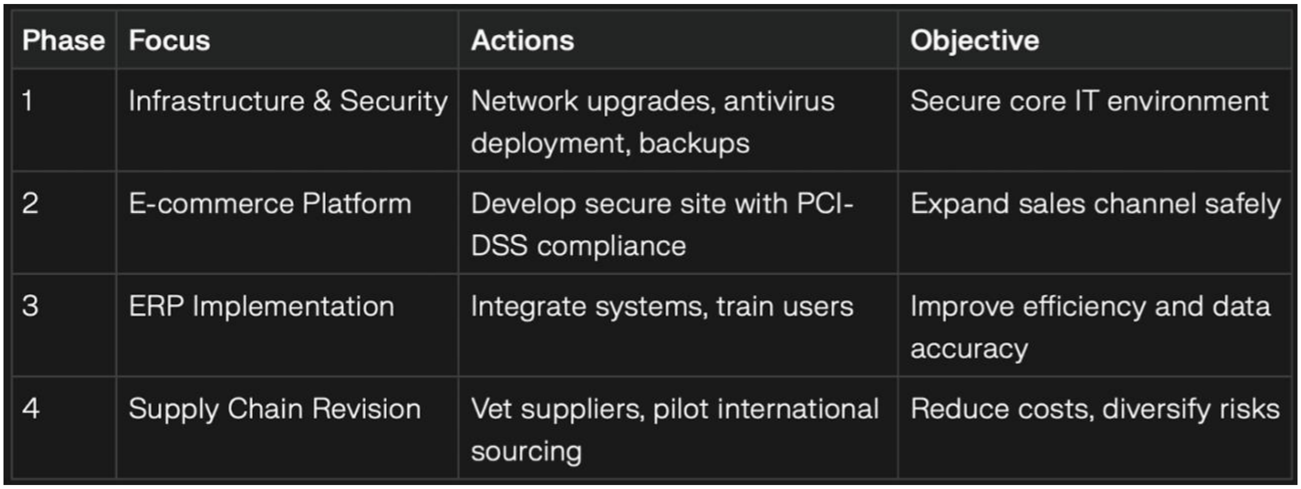


Figure 3: Supply Chain Flow Diagram illustrating the benefits and limitations of Local and International supply chains for Pampered Pets, with a Hybrid approach balancing cost savings, quality assurance, and operational resilience.

6. Phased Implementation Plan

This section presents a structured roadmap designed to guide Pampered Pets through a safe and effective digital transformation. The implementation plan is divided into four sequential phases: strengthening IT infrastructure and security, developing a compliant e-commerce platform, integrating ERP systems with user training, and revising the supply chain through careful supplier selection and international sourcing pilots. Each phase includes targeted actions and clear objectives, ensuring risks are managed and business goals are met at every step.



Phase	Focus	Actions	Objective
1	Infrastructure & Security	Network upgrades, antivirus deployment, backups	Secure core IT environment
2	E-commerce Platform	Develop secure site with PCI-DSS compliance	Expand sales channel safely
3	ERP Implementation	Integrate systems, train users	Improve efficiency and data accuracy
4	Supply Chain Revision	Vet suppliers, pilot international sourcing	Reduce costs, diversify risks

Table 2: Phased Implementation Plan for Pampered Pets summarising each transformation stage's focus, required actions, and intended objectives to enable secure and sustainable digital adoption.

7. Conclusion

Pampered Pets is at a strategic juncture where digital adoption is needed for competitive survival and growth. This report identifies critical cybersecurity risks and recommends a framework to mitigate them without overextending into complex financial forecasting.

Applying **ISO 31000** with **STRIDE** and **DREAD** threat modelling ensures focused, practical risk assessment. A phased digital transformation, coupled with strong cybersecurity practices and balanced supply management, positions Pampered Pets for sustainable success.

References

Aven, T. and Thekdi, S. (2024) Risk Science. 2nd edn. Abingdon: Routledge.

Fortune Business Insights (2024) Pet Care Market Size, Share, Trends. Available at: https://www.fortunebusinessinsights.com/pet-care-market-104749 (Accessed: 2 September 2025).

Friedman Corp. (2024) Top 10 Supply Chain Cost-Reduction Strategies. Available at: https://friedmancorp.com/blog/10-supply-chain-cost-reduction-strategies/ (Accessed: 2 September 2025).

Information Commissioner's Office (ICO) (2024) Guide to the General Data Protection Regulation (GDPR). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ (Accessed: 2 September 2025).

International Organization for Standardization (ISO) (2018) ISO 31000:2018 Risk Management — Guidelines. Available at: https://www.iso.org/standard/65694.html (Accessed: 2 September 2025).

Kovaitė, K. and Stankevičienė, J. (2019) 'Industry 4.0 and SMEs: Opportunities, Risks and Policy Responses', Engineering Economics, 30(2), pp. 142–153. doi:10.5755/j01.ee.30.2.23234.

Open Web Application Security Project (OWASP) (2023) OWASP Top 10 Web Application Security Risks. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 2 September 2025).

Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T. and Woody, C. (2018) Threat Modelling: A Summary of Available Methods. Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=521317 (Accessed: 2 September 2025).

Spendedge (2024) Pet Resin Market Procurement Intelligence Report. Available at: https://procurement.spendedge.com/report/pet-resin-market-procurement-intelligence-report (Accessed: 2 September 2025).

Stoneburner, G., Goguen, A. and Feringa, A. (2002) Risk Management Guide for Information Technology Systems (NIST SP 800-30). Gaithersburg, MD: National Institute of Standards and Technology.

Word Count (excluding references): 1027 words