**Pampered Pets: Risk Identification Report**

**Module:** SRM\_PCOM7E – July 2025 B  
**Assessment:** Development Team Project – Risk Identification Report

**Submission Date:** 8 September 2025

Done by:

Shamma Rashed Jauaan Hamad

Ahmed Mohamed Ahmed Talib Alsalami

**1. Introduction**

Pampered Pets is a small shop retail enterprise operating in Hashington-on-the-Water with four employees and too reliant on face-to-face sales. With minimal online presence and local suppliers, the business has boasted a strong reputation for high-quality pet food. Questions have been posed about whether digitalisation would be capable of bringing in maximum revenue, cutting costs, and safeguarding against customer loss. It analyzes and assesses risk on holding on to the existing model and going for digital transformation. Leveraging systematic risk assessment techniques and cybersecurity journals, analysis is structured to give company direction to balance opportunity with risk.

**2. Current State Risk Assessment**

**2.1 Methodology Justification**

To quantify the current risk position of Pampered Pets, the most suitable is the ISO 31000 risk management standard because it is flexible, globally accepted, and accessible by SMEs. The standard focuses on systematic identification, examination, and resolution of risks, placing even small enterprises in a position to apply its principles effectively (Cremer et al., 2022).

**2.2 Identified Threats and Risks**

The company also faces technical risks in the form of outdated IT infrastructure. Front-desk computer and warehouse spreadsheets share an insecure wireless network that makes them susceptible to malware and intrusion (Li & Liu, 2021). There are also cybersecurity awareness risks due to a lack of formal training among workers and thus their susceptibility to phishing or social engineering (Rohan et al., 2023). Operational risks involve dependence on one spreadsheet to manage the operations of the warehouse, susceptible to error by humans or insider abuse (Stewart & Hobbs, 2025). Supply chain risks are minimal due to nearness to nearby farms, but over-reliance on fewer suppliers exposes the company to vulnerabilities. Lastly, customer service risks arise due to poor online capabilities, the ability to drive away digitally native shoppers, and restrict competitiveness (Aslan et al., 2023).

**2.3 Potential Mitigations**

Mitigations consist of employee cybersecurity training (Rohan et al., 2023), upgrading systems with antivirus/firewall software (Zaid & Garai, 2024), making regular spreadsheet backups, and formalizing agreements with suppliers for guaranteed reliability.

**3. Digitalisation Risk Assessment**

**3.1 Methodology Justification**

For the evaluation of digitalisation risks, the STRIDE threat modelling approach is used in conjunction with ISO 31000. STRIDE enables the systematic determination of digital system risks based on Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The integration offers a well-rounded evaluation of business and technical risks (Zineddine et al., 2024).

**3.2 Proposed Digitalisation Changes**

The envisioned digital revolution involves establishing an online sales e-commerce website, the installation of an ERP system for inventory and finance control, online marketing and blogging, and even buying from overseas suppliers to minimize costs. All these projects support the owner's growth ambitions but present new categories of risk.

**3.3 Identified Threats and Risks**

* Cyberattacks: Move to the internet raises vulnerability to malware, phishing, ransomware, and denial-of-service attacks (Li & Liu, 2021).
* Database weaknesses: Online-stored supplier and customer information can be altered in the presence of poor security protocols (Almaiah et al., 2024).
* Insider threats: Workers may either abuse system privileges or unintentionally initiate breaches (Stewart & Hobbs, 2025).
* Ethical and compliance risks: Global market expansion involves complying with GDPR, data privacy regulations, and cross-border trading regulations (Viganò et al., 2020).
* Reputation risk: Security compromise or disruption of services would harm customer trust and brand reputation.
* Supply chain risks: Transitioning to a global supply chain reduces costs but enhances reliance on global logistics and exposes the company to cyber threats across suppliers (Cremer et al., 2022).

**3.4 Potential Mitigations**

Mitigation measures involve protecting databases with authentication and encryption (Almaiah et al., 2024), implementing strong HTTPS protocols (Zineddine et al., 2024), adding penetration testing and auditing (Aslan et al., 2023), and monitoring insider threats (Stewart & Hobbs, 2025). Supply chain security and transparency may be improved through the employment of blockchain tools (Zaid & Garai, 2024).

**4. Comparative Analysis: Status Quo vs Digitalisation**

Remaining with the current business model provides Pampered Pets with stability and convenience. The local supplier reliance provides it with resilience and quality assurance but limited digital presence limits exposure to online attacks. The limitation of this is risk avoidance. Without being online, the business risks losing up to 33% of its customers, as modern-day consumers anticipate more online interaction and ease of accessibility (Aslan et al., 2023). Lack of scalability as well as antiquated systems also increases operational inefficiency and errors.

In contrast, digitalisation has vast potential for growth and efficiency. Customer bases can be increased up to 50% with an e-commerce portal, and companies can save 24% of costs with an international supply chain. But at greater exposure to cyberattacks, insider abuse, and compliance expenses (Li & Liu, 2021; Stewart & Hobbs, 2025). The combination of ERP and web portals enables efficiency but in lieu of firm cybersecurity governance to avert breaches (Zineddine et al., 2024).

In effect, as the status quo constrains long-term competitiveness, digitalisation, with the proper mitigations, is more aligned with the wishes of the company to grow. The relative comparison concludes that the advantages of transformation greatly exceed the risks where they are accompanied with proper risk management best practices.

**5. Recommendations**

Pampered Pets should adopt a phased digitalisation plan backed by funding from Orla O'dour. The process of change must be initiated by the introduction of a safe e-commerce platform and ERP system since they will bring quicker growth benefits and business efficiency. Diversification of supply chains must be staged with a balance among known dependable local suppliers and thoroughly screened off-shore partners to limit disruption threats (Cremer et al., 2022).

Cyber security leadership should form the core of all the transformations. These include mandatory training of employees to create awareness (Rohan et al., 2023), technical controls like encryption and HTTPS protocols (Zineddine et al., 2024), and ongoing monitoring for insider threats (Stewart & Hobbs, 2025). Blockchain-based solutions may be applied to enhance supply chain transparency and security (Zaid & Garai, 2024).

Overall, a well-financed, well-thought-out digitalisation strategy will make Pampered Pets enjoy sustainable growth as it operates with related risks.

**6. Conclusion**

Pampered Pets' existing model is safe but vulnerable to loss of customers and operational inefficiencies. Digitalisation provides more opportunities for growth, efficiency, and competitiveness if risks can be properly managed. With incremental implementation, strong cybersecurity, and a hybrid supply chain approach, digital transformation provides the best chance of success in the long run.

**References**

Almaiah, M.A., Saqr, L.M., Al-Rawwash, L.A., Altellawi, L.A., Al-Ali, R. and Almomani, O. (2024) ‘Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems’, *Computers, Materials and Continua*, 81(2), pp. 3189–3220. Available at: <https://www.sciencedirect.com/science/article/pii/S1546221824008154> (Accessed: 8 September 2025).

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M. and Yilmaz, A.A. (2023) ‘A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions’, *Electronics*, 12(6), 1333. Available at: <https://doi.org/10.3390/electronics12061333> (Accessed: 8 September 2025).

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022) ‘Cyber risk and cybersecurity: a systematic review of data availability’, *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47, pp. 698–736. Available at: <https://link.springer.com/article/10.1057/s41288-022-00266-6> (Accessed: 8 September 2025).

Li, Y. and Liu, Q. (2021) ‘A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments’, *Energy Reports*, 7, pp. 8176–8186. Available at: <https://www.sciencedirect.com/science/article/pii/S2352484721007289> (Accessed: 8 September 2025).

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. and Thapliyal, H. (2023) ‘A systematic literature review of cybersecurity scales assessing information security awareness’, *Heliyon*, 9(3), e14234. Available at: <https://www.sciencedirect.com/science/article/pii/S240584402301441X> (Accessed: 8 September 2025).

Stewart, A. and Hobbs, C. (2025) ‘Systematic analysis of security advice on the topic of insider threats’, *Computers & Security*, 154, 104411. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0167404825001002> (Accessed: 8 September 2025).

Viganò, E., Loi, M. and Yaghmaei, E. (2020) *The Ethics of Cybersecurity*. In: *Cybersecurity of Critical Infrastructure*. Springer, pp. 157–177. Available at: <https://link.springer.com/chapter/10.1007/978-3-030-29053-5_8> (Accessed: 8 September 2025).

Zaid, T. and Garai, S. (2024) ‘Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers’, *Blockchain in Healthcare Today*, 7, 10.30953/bhty.v7.302. Available at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11073482/> (Accessed: 8 September 2025).

Zineddine, A., Chakir, O., Sadqi, Y., Maleh, Y., Gaba, G.S., Gurtov, A. and Dev, K. (2024) ‘A systematic review of cybersecurity assessment methods for HTTPS’, *Computers and Electrical Engineering*, 115, 109137. Available at: <https://www.sciencedirect.com/science/article/pii/S004579062400065X> (Accessed: 8 September 2025).