Pampered Pets: Risk Assessment and Recommendations

Submitted by
Team Cipher

Group 4

Ketan Mone
Franz Stephan

MSc Cyber Security, University of Essex Online
Submission Date: **8 September 2025**

Word Count : **985**

Table of Contents

1. Introduction

Pampered Pets is a small bricks-and-mortar business located in Hashington-on-the-Water, employing four staff and specialising in high-quality, locally sourced pet foods. Its operations are primarily in-person, with minimal digital integration. While this model provides strong local supplier resilience, it exposes the business to risks associated with limited scalability and operational fragility.

The purpose of this report is to evaluate the risks of continuing with the current setup against those of digitalisation. Using an established risk assessment methodology, the report identifies threats, vulnerabilities, and mitigation strategies before making recommendations. This analysis addresses whether an online presence could expand sales, if international sourcing could reduce costs, and whether the lack of digital features may lead to customer loss (Sørensen, 2018).

2. Methodology Selection and Justification

The **ISO 31000 Risk Management Framework** has been selected. ISO 31000 provides an adaptable structure for both strategic and operational risks, enabling businesses to balance opportunities and threats (Aven and Thekdi, 2025).

The justification for this selection includes:

- Suitability for small-to-medium enterprises with limited technical resources.
- Coverage of both business and cyber risks.
- Scalability, allowing Pampered Pets to adapt processes as the company grows.

Alternative approaches such as **NIST SP 800-30** (Stoneburner, Goguen and Feringa, 2002) and **OCTAVE** (Shevchenko *et al.*, 2018) are valuable but narrower in scope. NIST is primarily tailored to IT systems, whereas Pampered Pets requires a broader framework encompassing physical, operational, and reputational risks. ISO 31000 therefore offers the most holistic approach.

3. Current Business Risk Assessment

Overview of Current Operations

Pampered Pets' operations rely on two computers connected via a wireless network: one for warehouse management and the other for in-store sales. Staff also access the Wi-Fi through personal smartphones. Sales are largely face-to-face, with some orders placed via email.

Threat and Risk Identification

Using ISO 31000, risks are identified across three categories:

- **Physical –** theft, fire, flooding, and supply disruption.
- **Cyber –** outdated systems, phishing, and insecure Wi-Fi (Sutton, 2021).
- **Operational –** reliance on one staff member, manual stock errors, no recovery plan.

Risk	Likelihood	Impact	Risk Level
Insecure Wi-Fi leading to intrusion	High	High	Critical
Malware or ransomware on outdated PCs	Medium	High	High
Phishing attacks via staff email	High	Medium	High
Dependency on Harry for warehouse data	Medium	Medium	Medium
Human error in manual stock updates	High	Low	Medium
Lack of disaster recovery procedures	Medium	High	High
Supply chain disruption from local farms	Medium	Medium	Medium
Theft or burglary of stock and cash	Low	High	Medium
Fire or flooding damaging premises	Low	High	Medium

Source: Adapted from ISO 31000 (Aven and Thekdi, 2025).

Critical (Red) = High likelihood and high impact, requiring urgent mitigation.
High (Orange) = Significant risks with either high impact or high likelihood.
Medium (Yellow) = Moderate risks that should be managed and monitored.
Low (Green) = Low-priority risks with limited business impact.

Risk Evaluation

The most critical risks identified are cyber intrusion via insecure Wi-Fi, and operational dependency on single staff members. Physical risks, while relevant, can be mitigated through conventional measures.

Potential Mitigations

- Upgrade locks, alarms, and CCTV to deter theft.

- Apply basic cybersecurity hygiene: patching, antivirus software, and secure Wi-Fi passwords (Renn, Beier and Schweizer, 2021).

- Develop cross-training initiatives to reduce reliance on individuals.

- Formalise incident response and fire safety protocols.

4. Digitalisation Risk Assessment

Proposed Changes

The proposed transformation could include:

- Launch of an **e-commerce platform**.
- Integration of **inventory management software**.
- Expansion into **online marketing channels**.
- Adoption of an **international supply chain** to reduce costs.

Threat and Risk Identification

- **Cybersecurity** – data breaches, denial-of-service, payment fraud.
- **Compliance** – GDPR and cross-border legal challenges (Josey, Hietala and Jones, 2014).
- **Reputational** – trust loss after breaches or delays.
- **Operational** – vendor dependence and staff training needs.

Risk	Likelihood	Impact	Risk Level
Data breach compromising customer information	Medium	High	High
Website denial-of-service attack	Medium	Medium	Medium
Payment fraud in online transactions	Medium	High	High
Breach of GDPR requirements	Low	High	Medium
Legal issues with international suppliers	Medium	Medium	Medium
Customer trust loss after breach/delays	Medium	High	High
Dependence on hosting providers/vendors	High	Medium	High
Staff training gaps with new systems	High	Medium	High
Poorly managed online reputation	Medium	Medium	Medium

Source: Adapted from ISO 31000 (Aven and Thekdi, 2025).

Critical (Red) = High likelihood and high impact, requiring urgent mitigation.

High (Orange) = Significant risks with either high impact or high likelihood.

Medium (Yellow) = Moderate risks that should be managed and monitored.

Low (Green) = Low-priority risks with limited business impact.

Risk Evaluation

The likelihood of cyber incidents increases substantially with digitalisation (Hubbard, 2020). However, the opportunity for significant growth and efficiency outweighs the risks if mitigations are implemented effectively.

Mitigation Measures

- Adopt secure web hosting and encryption protocols (Ross, McEvilley and Oren, 2016).

- Introduce multi-factor authentication and web application firewalls.

- Vet international suppliers with due diligence and service-level agreements (SLAs).

- Provide regular cybersecurity awareness training for staff (Hancock *et al*., 2024).

- Establish an incident response framework in line with FAIR and ISO standards (Josey, Hietala and Jones, 2014).

5. Comparative Analysis: Status Quo versus Digitalisation

To evaluate strategic options, ISO 31000 is applied to compare the current business model with the digitalisation pathway. The analysis highlights differences in growth potential, cost efficiency, customer retention, resilience, and risk exposure. This structured comparison helps clarify the trade-offs between stability and scalability, guiding recommendations for Pampered Pets' future direction.

Criteria	Status Quo	Digitalisation
Growth Potential	Limited to local footfall and email orders.	Online presence could expand sales by up to 50%.
Costs	Stable but dependent on local supply chains.	International supply chain may cut costs by 24%.
Customer Retention	Risk of losing up to 33% without online features.	Stronger retention via e-commerce and loyalty tools.
Risks	Lower cyber risks but higher operational fragility.	Higher cyber risks but controllable with mitigations.
Resilience	Relies on individual staff and local suppliers.	Diversified supply chains, tech-enabled efficiency.

6. Recommendations

It is recommended that Pampered Pets proceed with **phased digitalisation**, balancing opportunity with resilience:

- **Phase 1 (Immediate):** Strengthen IT infrastructure, secure Wi-Fi, and train staff in cybersecurity.

- **Phase 2 (Short-term):** Launch a simple e-commerce platform and digital marketing campaign.

- **Phase 3 (Medium-term):** Implement inventory management software.

- **Phase 4 (Long-term):** Expand cautiously into international supply chains, beginning with pilot suppliers.

This phased strategy ensures that operational maturity develops alongside technical capability. Early investment in cybersecurity and staff training reduces vulnerabilities before digital exposure increases. Gradual e-commerce expansion allows customer trust to be established incrementally, while piloting international suppliers mitigates supply chain risks identified earlier. Aligning with ISO 31000, this staged progression balances opportunity with resilience, ensuring Pampered Pets achieves growth without exceeding its capacity for risk management (Aven and Thekdi, 2025).

7. Conclusion

Pampered Pets faces a strategic choice. Maintaining the current model limits risks but hampers growth, while digitalisation increases exposure to cyber threats yet provides significant opportunities for expansion and efficiency. By applying ISO 31000, implementing appropriate mitigations, and adopting a phased digital strategy, Pampered Pets can achieve sustainable growth whilst safeguarding operational integrity and customer trust.

In the long term, digitalisation is not merely an efficiency exercise but a requirement for competitiveness in the pet retail sector. By embedding robust governance, Pampered Pets can position itself as a trusted provider, resilient to disruptions and adaptable to customer expectations. The balance of innovation and control will define its sustainability in an increasingly digital marketplace.

8. References

Aven, T. and Thekdi, S. (2025) *Risk science*. London: Routledge.

Hancock, J., *et al.* (2024) ‘Trouble at sea: Data and digital technology challenges for maritime human rights concerns’, *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, pp. 988–1001.

Hubbard, D.W. (2020) *The failure of risk management: Why it’s broken and how to fix it*. 1st edn. New Jersey: Wiley & Sons.

Josey, A., Hietala, J. and Jones, J. (2014) *Introducing the Open Group Open FAIR™ risk analysis tool*. Reading: Van Haren Publishing.

Renn, O., Beier, G. and Schweizer, P.-J. (2021) ‘The opportunities and risks of digitalisation for sustainable development: A systemic perspective’, *GAIA – Ecological Perspectives for Science and Society*, 30(1), pp. 23–28.

Ross, R., McEvilley, M. and Oren, J. (2016) *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems*. Washington, DC: NIST.

Shevchenko, N., *et al.* (2018) ‘Threat modelling: A summary of available methods’. Pittsburgh: Carnegie Mellon University, Software Engineering Institute.

Sørensen, B.T. (2018) ‘Digitalisation: An opportunity or a risk?’, *Journal of European Competition Law & Practice*, 9(6), pp. 349–350.

Stoneburner, G., Goguen, A. and Feringa, A. (2002) *SP 800-30: Risk management guide for information technology systems*. Gaithersburg: NIST.

Sutton, D. (2021) *Information risk management*. Swindon: BCS Learning and Development.