Development Team Project: Risk Identification Report

1. Current Business Risk Assessment

For Pampered Pets, the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method is most suitable. OCTAVE is designed for small to medium-sized businesses, focusing on critical assets, vulnerabilities, and operational risks rather than complex technical analysis. This makes it both practical and cost-effective for a company with limited IT resources (Alberts & Dorofee, 2002).

Identification of Current Risks and Threats

- **Wireless Network Vulnerabilities**: Business computers and staff smartphones share the same Wi-Fi, exposing systems to malware and unauthorised access if strong encryption and segmentation are not enforced (Arief, S., 2024).
- **Warehouse Spreadsheet System**: Records stored on an old computer using spreadsheets risk data loss from hardware failure, accidental deletion, or tampering. Spreadsheets also lack security and are prone to errors (Pech, Vrchota & Bednář, 2021).
- **Front Desk Transaction System**: A single computer manages all sales and VAT/tax recording, creating a single point of failure. Any malware infection or outage could stop business operations (Minnaar and Herbig, 2021).
- **Email Orders**: Customer orders via email expose the business to phishing and social engineering threats.

Risk Mitigation Strategies

- **Secure the Wireless Network**: Use WPA3 encryption and separate staff and business networks (Ghadim, A.D., 2023).
- **Improve Data Management**: Shift warehouse records from spreadsheets to a secure database and enable automatic cloud or external backups (Pech, Vrchota & Bednář, 2021).
- **Protect Critical Systems**: Apply antivirus, keep systems patched, and enforce least-privilege access controls (Shameli-Sendi et al., 2016).
- **Staff Training**: Provide training on phishing detection and safe email use, as human error is a significant weakness (Hadlington, 2017).

2. Risk Assessment of Digitalisation

Methodology of Risk Assessment

The ISO 31000 framework is a suitable approach for assessing digital transformation, which will be further coupled with qualitative risk metrics to assign impact and likelihood categories to operational threats and emerging cyber threats. This hybrid approach will be capable of supporting the prioritisation of risks related to digital initiatives, as well as structured analysis, which includes online platforms and e-commerce.

Proposed Changes in Digitalisation

- The key transformations will include the launch of the e-commerce portal for online payment and ordering. Digital marketing channels will also be introduced, which include social media, SEO, and blogs. An ERP or an order management system will be implemented to integrate inventory, supplier data, and sales. These changes will help boost reach, customer engagement, and efficiency while facilitating growth.

Threat and Risk Modelling

- Cybersecurity threats, including malware, DDOS attacks, compromise of credentials, and ransomware, might threaten the integrity of the site. For example, facing accounts account for almost 43% of the total details identified in 2023, and 69% of retail businesses face ransomware attempts (Keenan, 2024). The attacks on account takeover have also surged, including malicious login attempts that increased by 85% during the 2023 Black Friday period (Marks, 2024).
- Fraud and impersonation have also been identified as increasing. Deepfake scams, along with artificial intelligence-driven fraud, are making impersonations and cloned sites. Moreover, large-scale networks of fraud have also been identified, which have launched various fake retail sites that have cost victims a significant amount of money globally.
- 3rd party vulnerability or supply chain issues include E-commerce platforms that depend on 3rd party vendors are exposed towards cybersecurity threats.
- Regulatory compliance, along with data privacy issues, is also identified. Approximately 30% of e-commerce platforms leak user data to third parties, thereby increasing the risk of regulatory breaches (Vlachogiannakis et al., 2025).
- Negative reviews or even poor experiences of the users might erode customer trust. According to Jones (2024), 93% of consumers rely on online reviews.

3. Risk and Threat Modelling

Risks are evaluated based on their impact (High/Medium/Low) and likelihood (High/Medium/Low), encompassing both general digitalisation and international supply chain expansion (Luo, 2021).

General Digitalisation Risks

Risk	Description	Impact	Likelihood
Cybersecurity threats (e.g., breaches, ransomware)	Attacks on e-commerce/ERP could compromise data or disrupt operations. In 2023, 69% of retail firms faced ransomware (Keenan, 2024).	High	High
Implementation costs/resource strain	High upfront expenses and training burden on a small team.	Medium	High

Employee resistance/skills gap	Low adoption due to change aversion.	Medium	Medium
System downtime	Outages halt sales.	High	Medium
Data privacy/compliance	GDPR violations from data mishandling, 30% of e-commerce sites leak user data (Vlachogiannakis et al., 2025).	High	Medium
Fraud/impersonation	AI-driven scams and fake sites; account takeovers up by 85% in 2023 (Marks, 2024).	High	High
Negative user experiences	Poor reviews erode trust. 93% of consumers rely on reviews (Jones, 2024).	Medium	Medium

International Supply Chain Risks

Risk	Description	Impact	Likelihood
Supplier quality/reliability	Inconsistent deliveries affect product standards.	High	Medium
Geopolitical disruptions	Tariffs/wars delay supplies.	High	Medium
Longer lead times/logistics costs	Delays clash with just-in-time needs.	Medium	High
Currency fluctuations	Volatility erodes cost savings.	Medium	Medium
Supply chain cybersecurity	Breaches via partners.	High	High

Risk Mitigations For -

- **Cybersecurity**: Deploy firewalls, MFA, encryption, train on phishing, and adopt ISO 27001 and/or ISO 27001.
- **Costs/Strain**: Phase implementation using funding, seek grants.
- **Resistance/Gap**: Leadership-driven training, start with user-friendly tools.
- **Downtime**: Use cloud ERP with backups, test integrations.
- **Privacy/Compliance**: Conduct audits, implement privacy-by-design.
- **Fraud**: Monitor with AI tools, verify user identities.
- **User Experience**: Gather feedback, manage reviews proactively.
- **Supply Chain (General)**: Diversify suppliers, use ERP for monitoring.
- **Quality/Reliability**: Audit suppliers, hybrid local-international model.

- **Disruptions**: Test drills, surplus stocks.
- **Currency**: Hedge rates, fixed contracts.
- **Cyber Command in Chain**: Extend policies to partners.

4. Recommendations

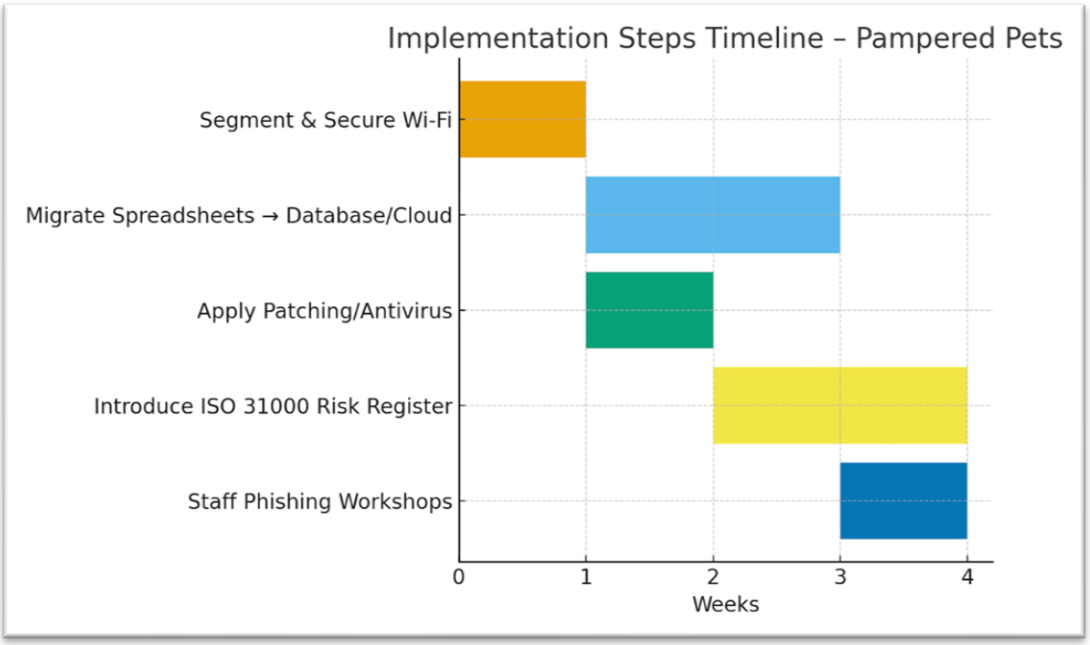
Pampered Pets' current risks highlight weaknesses in Wi-Fi, spreadsheets, and reliance on single systems. Compared with ISO 31000, OCTAVE offers a more practical and cost-effective approach for SMEs, yet ISO strengthens long-term governance. Combining both ensures operational efficiency and compliance.

Recommendation & Rationale

Adopt a hybrid OCTAVE-ISO framework. OCTAVE will address immediate vulnerabilities pragmatically, while ISO provides a scalable structure for digitalisation risks, including e-commerce and AI-driven fraud. This dual strategy strikes a balance between cost, resilience, and regulatory trust.

Implementation Steps

- Segment and secure Wi-Fi.
- Migrate spreadsheets → database/cloud.
- Apply patching/antivirus.
- Introduce ISO 31000 risk register.
- Conduct staff phishing workshops.



References

Alberts, C.J. *et al.* (2009) *Managing information security risks: the OCTAVE approach*. 7th print. Amsterdam Munich: Addison-Wesley (SEI series in software engineering : a CERT book).

Arief, S., (2024). Digital transformation in accounting: The nexus between technology, leadership, and beyond. In *Digital Transformation in Accounting and Auditing: Navigating Technological Advances for the Future* (pp. 29-59). Cham: Springer International Publishing.

Ghadim, A.D., (2023). *Identification of cyberattacks in industrial control systems* (Master's thesis, Malardalen University (Sweden)).

Hadlington, L. (2017) "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, 3(7), p. e00346. Available at: https://doi.org/10.1016/j.heliyon.2017.e00346.

Jones, A. (2024) *7 risks and challenges for online retailers > Small Business Answers*, *Small Business Answers*. Available at: https://www.smallbusinessanswers.com.au/news/7-risks-and-challenges-for-online-retailers/ [Accessed: 27 August 2025].

Keenan, M. (2024) *Retail Risk Management: Threats and strategies to mitigate them (2024) - shopify India*, *Shopify*. Available at: https://www.shopify.com/in/retail/retail-risk-management [Accessed: 26 August 2025].

Luo, Y. (2022) "A general framework of digitization risks in international business," *Journal of International Business Studies*, 53(2), pp. 344–361. Available at: https://doi.org/10.1057/s41267-021-00448-9.

Marks, L. (2024) *What 2023 taught us about eCommerce security*, *TechRadar*. Available at: https://www.techradar.com/pro/what-2023-taught-us-about-ecommerce-security [Accessed: 26 August 2025].

Minnaar, A. and Herbig, F.J., (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), pp.155-185.

Pech, M., Vrchota, J. and Bednář, J., (2021). Predictive maintenance and intelligent sensors in smart factory. *Sensors*, *21*(4), p.1470.

Shameli-Sendi, A. et al., (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, pp.14-30.

Vlachogiannakis, I. *et al.* (2025) "I Know What You Bought Last Summer: Investigating User Data Leakage in E-Commerce Platforms." arXiv. Available at: https://doi.org/10.48550/ARXIV.2504.13212.