

**Pampered Pets Store**

**1 Introduction**

This report presents a security risk assessment for Pampered Pets, evaluating the current operational state and the proposed digitalisation initiative funded by investor Orla O’dour. The objective is to provide a evidence-based recommendation on whether to proceed with digital transformation or not.

1. **Risk Assessment of *Current Business***

* **Selected Methodology: OCTAVE Allegro** OCTAVE Allegro was selected for its focus on information assets within operational risk due to the current technological maturity (old computer devices & small data capacity), its scalability for small - medium enterprises and to support a small orgnizations against any data cyber attack. (Claire Allen 2023)
* **Current Threats and Risks**

The primary assets are the customer database, financial records, and the reputation for high-quality, locally sourced products.

* **Inadequate IT Security:** The old, unpatched warehouse computer is a critical vulnerability, susceptible to malware the risk here due to thedatabases physical devise & the employee using their own devises.
* **Data Loss:** No evidence of backups for the sales or warehouse systems. A hardware failure would cripple operations and VAT compliance, the same network working for deferent portable personal devises which increase the cyberattack
* **Operational Resilience:** The business is highly dependent on key personnel (e.g., Alice, Harry). Illness or departure would cause significant disruption. There is unavailable alternative electronic client’s support such as a small online store.
* **Reputational Damage:** A single quality failure in the food preparation process, while currently mitigated by local sourcing, could severely damage the brand.
* **Potential Mitigations**
* Implement a formal patch management policy for all systems.
* The databases should be copied every minute (online/offline) backup.
* Develop and document standard operating procedures (SOPs) to reduce key-person dependency.

**3 Risk Assessment of the *Proposed Digitalisation***

* **The Methodology selected for this report is the National Institute of Standards and Technology:** the cybersecurity framework (NIST CSF), It is perfectly suited for a small store to guid the digital transformation, providing a structured lifecycle for managing cybersecurity risk, encompassing threat discovery, preventative safeguard, continuous monitoring, incident handling, and restoration of operations. (NIST 2028)
* **Proposed Digitalisation Changes** The transformation will be phased, starting with:
* **E-commerce Portal:** A website for online sales and customer engagement.
* **Cloud-Based ERP System:** To integrate inventory, sales, and supply chain management, replacing the standalone spreadsheet and POS system.
* **Digital Marketing Strategy:** Utilising social media and targeted online advertising.
* **Threats and Risks of Digitalisation**
* **Increased Attack Surface:** An e-commerce portal may be affected or attacked by the Distributed Denial of Service (DDoS) and SQL injection, potentially taking the business offline. Most of the employee using the personal devises the suitable solution here is to engage them in a cybersecurity course to save the new system from any cyber-attack.
* **Supply Chain Complexity**: Global supply chains are vulnerable to shipping holdups, difficulties in maintaining product standards (World Bank, 2022). The current recourses need a high-quality end due to the type of the products (the pet’s food).
* **Data Breach:** A centralised ERP system holding customer and financial data becomes a high-value target for data theft.
* **System Integration Failure:** Poor implementation of new systems could lead to operational downtime.
* **Potential Mitigations**
* Employ a special web firewall and start a regular penetration detection on the online website.
* Conduct rigorous due diligence on international suppliers and maintain relationships with local suppliers as a contingency.
* Implement robust encryption protocols for stored information and data actively being transmitted across networks, within the ERP system and mandate multi-factor authentication (MFA) for all user accounts.
* Engage with experienced implementation partners and adopt a phased rollout with comprehensive staff training.

**4 Recommendations and Conclusion**

* **Response to Core Questions**
* **50% Business Growth:** **Yes, it is feasible.** An online presence opens access to a national market, moving beyond the physical suburb. However, achieving 50% is ambitious and depends on effective digital marketing execution.
* **24% Cost Reduction via International Supply Chain:** **Possible, but high-risk.** Bulk international sourcing could reduce ingredient costs. However, this must be weighed against potential import tariffs, shipping costs, and the significant risk of compromising the brand's core value proposition of *local*, high-quality ingredients.
* Companies that neglect to develop an online presence risk may increase of their customer base to more digitally agile competitors. This loss is driven by the prevailing consumer demand for integrated shopping options that combine physical and digital convenience**,** Failure to adapt would likely lead to this level of attrition.

The below Graph: Impact of Online Store on Revenue and Profit:

This bar chart compares the financial performance of a Traditional Store vs. a Store with an added Online (Cloud) platform. It clearly shows how the 70% revenue increase far outweighs the new 5% operational cost.

* **Final Recommendation**  **is proceeding with the digitalisation process, but with a cautious, risk-aware approach.**

The risk of maintaining the status quo—primarily stagnation and loss of market share to digital competitors—is greater than the manageable risks associated with a well-planned transformation.

The process should involve:

* **Phased Implementation:** Begin with the e-commerce portal and digital marketing, leveraging the existing local supply chain. This builds online revenue without immediately jeopardising product quality.
* **Hybrid Supply Chain Model:** Pilot international sourcing for non-core, non-perishable items while retaining local suppliers for the flagship pet food range. This tests cost-saving without damaging the brand.
* **Investment in Cybersecurity:** A portion of Orla O’dour’s investment must be allocated to security measures (WAF, MFA, encryption, staff training) from the outset, not as an afterthought.
* SSL secure socket layer to encrypt the data at the online store and the clouded databases.

Digitalisation is essential for the long-term growth and resilience of Pampered Pets. By adopting a strategic, phased, and security-focused plan, the business can capture new opportunities while protecting its esteemed reputation.

**Reference:**

Claire Allen (2023) ‘*Threat Modeling Methodology: OCTAVE” . iriusrisk* , Available at : https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies [Accessed 25 August 2025].

NIST (2018) “*cybersecurity framework”. ‘*NIST”. Available at: https://www.nist.gov/cyberframework/csf-11-archive [Accessed 25 August 2025].

World Bank (2022) ‘’*World development report ‘’. ‘*The World Bank’. Available at: <https://www.worldbank.org/en/publication/wdr2022> [Accessed 25 August 2025].