

Risk Identification Report for Pampered Pets' Digital

Transformation Assessment

**Prepared For:** Pampered Pets

**Author:** Cyber Risk Rangers

|  |
| --- |
|  |
|  |
| June 6th 2024 |



Introduction

This report evaluates the risks and opportunities to inform strategic decisions for growth and operational efficiency, focusing on three critical questions:

* Could an online presence grow the business by up to 50%?
* Could changing to an international supply chain reduce costs by up to 24%?
* Could the business lose up to 33% of its existing customers if the business does not provide online features?

This report analyses these questions, assesses impacts, and outlines strategies to manage associated risks.

1: Methodology and Justification

We adopted a hybrid methodology for comprehensive risk management, integrating International Organisation for Standardisation (ISO) 31000, STRIDE, and Factor Analysis of Information Risk (FAIR).

### 1.1 ISO 31000

It provides a structured approach to risk management, aligning with standards such as ISO 9001 and ISO/IEC 27001 (Barafort et al. 2018). As illustrated in Figure 1, it includes:

* Risk Identification: Pinpointing potential risks.
* Risk Analysis: Evaluating risks based on likelihood and impact.
* Risk Evaluation: Comparing risk analysis results with criteria.
* Risk Treatment: Developing strategies to manage risks.
* Monitoring and Review: Regularly reviewing risks and processes.
* Communication and Consultation: Engaging stakeholders for understanding and management.

A diagram of a risk analysis

Description automatically generated

Figure 1: Risk Assessment Process ISO 31000 (AIRMIC, 2010)

### 1.2 STRIDE

The Stride model Identifies Cybersecurity threats. Shevchenko et al. (2018) specify them in Table 1:

A white and black text on a white background

Description automatically generatedTable 1: Threat Categories

### 1.3 FAIR

The FAIR model quantifies the financial impact of identified risks using statistical methods and Monte Carlo simulations (Wang et al. 2019).

### 1.4 Critical Analysis

Combining these methodologies offers a comprehensive, data-driven risk management approach. ISO 31000 provides a structured framework, STRIDE addresses specific Cybersecurity threats essential for digitalisation, and FAIR quantifies risks, translating complex scenarios into clear financial impacts. This integrated approach balances qualitative and quantitative analysis tailored to Pampered Pets' needs.

2: Impact Analysis

The potential impacts are summarised in Table 2:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact Area | Description | Estimated Impact | Confidence Level | Basis of Estimate |
| Business Growth | Expansion through online sales | Up to 50% increase | Medium-High | Market analysis of similar sectors. |
| Cost Reduction | Efficiency from international supply chain. | Up to 24% reduction | Medium | Supply chain optimisation studies. |
| Customer Retention | Necessity of online features | Loss of up to 33% | High | Customer feedback and competitor analysis. |

Table 2: Impact Analysis

3: Current Risk and Threat Modelling

The primary risks in the current business model are detailed in Table 3:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Level | Risk Category | Description | Mitigation Strategy |
| High | Physical Store Dependency | Vulnerable to disasters or downturns. | Diversify with e-commerce. |
| Medium | Manual Data Management | Inefficiencies and data loss. | Implement an ERP system. |
| Medium | Supply Chain Disruption | Over-dependence on specific suppliers | Develop multiple supplier relationships. |

Table 3: Current Business Risks

### **3.1 Assets Identification per Process for Risk Analysis**

The following Turtle diagram provides an overview of the resources, inputs/outputs, and critical criteria related to warehouse inventory and delivery.

A diagram of a warehouse inventory

Description automatically generated

Figure 2: Turtle Diagram for Warehouse Inventory and Delivery process (QUENTIC, 2022)

### **3.2 Assets Criticality**

Following ISO 3100 guidelines, Table 4 defines Assets criticality, Table 5 defines STRIDE

threats definition, vulnerabilities under the current status quo and the proposed

digitalisation process. The analysis indicates that Digitalisation can lead to more tolerable risks.

A list of inventory of assets

Description automatically generated

Table 4: Assets Definition (ISO 31000:2018)

A white rectangular box with black text

Description automatically generated

Table 5: Threats, Vulnerabilities, Status Quo vs Digitalisation, Risk Analysis based on ISO31000:2018





Table 6: Risk Assessment Matrix (ISO 31000, 2018)

### **3.3 FAIR - Quantitative Risk Analysis**

This model estimates the financial impact under the current status quo (Table 7) and proposed digitalisation (Table 8):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Impact | Probability | Mitigation | Estimated Impact |
| Cybersecurity breach | Financial loss and reputational damage. | 15% | Basic Cybersecurity measures, periodic audits. | £5,000-£25,000 |

Table 7: Current Status Quo FAIR Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Impact | Probability | Mitigation | Estimated Impact |
| Cybersecurity breach | Financial loss and reputational damage. | 20% | Advanced Cybersecurity measures, regular audits, employee training. | £10,000-£75,000 |

Table 8: Digitalisation FAIR Analysis

4: Digitalisation Risk Assessment

We propose the following digital initiatives to enhance operational efficiency and customer engagement in Table 9:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Level | Digital Change | Potential Risks | Mitigation Strategy | Specific Technologies |
| High | E-commerce Portal | Cybersecurity threats, breaches. | Strengthen security measures, regular audits, and training. | Shopify. |
| High | ERP System | Integration issues, disruptions. | Utilise IT consultancy for phased implementation. | SAP ERP. |

Table 9: Digitalisation Proposal

This process flow diagram (Figure 3) outlines the steps to implement the proposed digital

changes, highlighting key phases and decision points to ensure a structured and efficient

transformation.

A diagram of a flowchart

Description automatically generated

Figure 3: Digitalisation Process Flow

5: Risk Response Treatments and Recommendations

Using risk response treatments (AIRMIC, 2010), we propose the following strategies (Table 10).

* Treat: Measures to minimise the risk.
* Transfer: Move risk to another party (e.g. insurance).
* Tolerate: Accept the risk if mitigation costs outweigh the benefits.
* Terminate: Eliminate the risk by stopping the activity.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Level | Risk Description | Response Treatment | Recommended Action |
| High | System Failures, Cyber Threats | Treat | Enhance Cybersecurity measures and system redundancies. |
| High | Physical Store Dependency | Transfer | Obtain business interruption insurance. |
| Medium | Data Management Inefficiencies | Treat | Implement advanced data management systems. |
| Low | Logistical Challenges | Tolerate | Regularly monitor supplier performance. |
| Medium | High Operational Costs | Transfer | Partner with cost-effective suppliers. |
| Medium | Resistance to Digital Adoption | Terminate | Conduct change management workshops. |

Table 10: Risk Mitigation and Recommendations

6: Ethical and Compliance Considerations

The digitalisation will adhere to ethical standards and GDPR compliance to ensure data protection and privacy, including data encryption, user consent protocols, and regular audits.

7: Limitations

The FAIR model’s effectiveness depends on the accuracy of the data used. Thorough data collection and validation are critical for reliable assessments (Barafort et al. 2018). Integrating multiple frameworks can be complex and resource-intensive (Shevchenko et al. 2018). Continuous updates are essential to maintaining relevance and accuracy in meeting evolving Cybersecurity threats (Shostack, 2014).

Human errors and change resistance can impact success, necessitating training and effective change management (Annosi et al. 2021). Moreover, specific risks like natural disasters, which could significantly impact the business, still need to be addressed. A broader risk assessment incorporating this is recommended.

8: Recommendations

The impact analysis supports digitalisation, highlighting growth potential, cost efficiency, customer retention, and improved operations.

9: Implementation Plan

The Gantt Chart in Figure 4 provides the implementation plan timeline for the Digitalisation.

A screenshot of a computer

Description automatically generated

Figure 4: Gantt Diagram

Conclusion

Digitalisation presents substantial growth opportunities, efficiency, and sustainability. Through careful planning, robust risk management, and strategic implementation, Pampered Pets can enhance its market position and customer satisfaction. Moreover, it can foster sustainable practices, operational empowerment, and supply chain collaboration (Rijswijk et al. 2021; Annosi et al. 2021).

Approval

This report has been submitted for approval to Pampered Pets' management and stakeholders.

References List:

AIRMIC. (2010) A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. Available from: <https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf> [Accessed 11 May 2024].

Annosi, M.C., Brunetta, F., Bimbo, F. & Kostoula, M. (2021) Digitalisation within food supply chains to prevent food waste. Drivers, barriers, and collaboration practices. *Industrial Marketing Management*, 93: 208-220. DOI: <https://doi.org/10.1016/j.indmarman.2021.01.005>

Barafort, B., Mesquida, L-A. & Mas, A. (2018) ISO 31000‐based integrated risk management process assessment model for IT organisations. *Journal of Software: Evolution and Process.*1-15. DOI: <https://doi.org/10.1002/smr.1984>

ISO. (2023) ISO31000:2018 Risk Management Guidelines Second Edition. Available from: <https://www.iso.org/standard/65694.html> [Accessed 14 May 2024].

PECB. (2015) ISO31000 Risk Management – Principles and Guidelines. Available from:

<https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines> [Accessed 14 May 2024].

QUENTIC. (2022) The Turtle Diagram. How to get process management and analysis. Available from: <https://www.quentic.com/articles/the-turtle-diagram/> [ Accessed 25 May 2024].

Rijswijk, K., Klerkx, L., Bacco, M., Bartolini, F., Bulten, E., Debruyne, L., Dessein, J., Scotti, I. & Brunori, G. (2021) Digital transformation of agriculture and rural areas: A socio-cyber-physical system framework to support responsibilisation. *Journal of Rural Studies.* 85: 79-90. DOI: <https://doi.org/10.1016/j.jrurstud.2021.05.003>

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P. & Woody, C. (2018) Threat modelling: a summary of available methods. Available from: <https://apps.dtic.mil/sti/pdfs/AD1084024.pdf> [Accessed 25 May 2024].

Shostack, A. (2014) *Threat Modeling: Designing for Security. ProQuest Ebook Central:* John Wiley & Sons, Incorporated.Available from: <https://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=1629177> [Accessed 25 May 2024].

StandardStores (2024) How to use Turtle Diagrams. Available from: <https://16949store.com/articles/how-to-use-turtle-diagrams/> [ Accessed 25 May 2024].

Wang, J., Neil, M. & Fenton, N. (2019) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security.* 89:1-20. DOI: <https://doi.org/10.1016/j.cose.2019.101659>