Table of Contents

[Introduction 2](#_Toc144085602)

[1. Current Business Risk Assessment 2](#_Toc144085603)

[a. Risk Assessment Methodology Selection 2](#_Toc144085604)

[b. Risk and Threat Modelling Exercise 2](#_Toc144085605)

[Operational Interruptions: 2](#_Toc144085606)

[Data Vulnerability: 2](#_Toc144085607)

[Dependency on Local Suppliers: 2](#_Toc144085608)

[c. Potential Mitigations 2](#_Toc144085609)

[2. Digitalisation Process Risk Assessment 2](#_Toc144085610)

[a. Risk Assessment Methodology Selection 2](#_Toc144085611)

[b. Proposed Changes 2](#_Toc144085612)

[c. Risk and Threat Modelling Exercise 2](#_Toc144085613)

[d. Potential Mitigations 2](#_Toc144085614)

[Critical Evaluation 3](#_Toc144085615)

[Quantitative Analysis: 3](#_Toc144085616)

[Supply Chain Dynamics: 3](#_Toc144085617)

[User Experience: 3](#_Toc144085618)

[3. Recommendations 3](#_Toc144085619)

[a. Approach and Timeline 3](#_Toc144085620)

[Conclusion 3](#_Toc144085621)

[References: 3](#_Toc144085622)

Critical Evaluation and Detailed Risk Identification

# Introduction

This report critically evaluates the risk assessment for Pampered Pets, aiming to enhance its clarity, depth, and critical analysis. The assessment covers both the current business state and the potential digitalisation process, emphasising feasibility and recommendations.

# 1. Current Business Risk Assessment

## a. Risk Assessment Methodology Selection

The ISO 31000 Risk Management Framework was chosen for its internationally recognised standards, offering a comprehensive approach (International Organisation for Standardisation, 2009). This aligns with the complexity of Pampered Pets' operations, ensuring a systematic analysis of risks.

## b. Risk and Threat Modelling Exercise

Identified risks:

Operational Interruptions: Potential technical failures in critical systems.

Data Vulnerability: Exposure of sensitive customer data due to cyber threats.

Dependency on Local Suppliers: Disruption in the supply chain due to external factors.

## c. Potential Mitigations

To address these risks, recommended strategies include regular data backups to prevent data loss, firewall implementation to safeguard digital assets, and supplier diversification to minimise dependency on single sources.

# 2. Digitalisation Process Risk Assessment

### a. Risk Assessment Methodology Selection

The NIST Cybersecurity Framework was selected for its specialised focus on digital risks (National Institute of Standards and Technology ,2014). This choice ensures the assessment is tailored to the unique challenges of digital transformation.

### b. Proposed Changes

The proposed digitalisation entails the establishment of an e-commerce portal and an ERP system to enhance online transactions and inventory management.

### c. Risk and Threat Modelling Exercise

Identified digitalisation risks:

Cybersecurity Breaches: Vulnerability of online systems to hacking attempts.

Technological Dependency: Over-reliance on new digital systems.

Privacy Concerns: Handling customer data online in compliance with data protection regulations.

### d. Potential Mitigations

Mitigation strategies include the implementation of robust cybersecurity protocols, the establishment of system redundancies to ensure operational continuity, and adherence to data protection regulations to ensure customer privacy.

# Critical Evaluation

The risk assessment effectively captures the business's potential risks and benefits associated with digitalisation. However, to enhance the depth of analysis, the following aspects merit attention:

Quantitative Analysis: Integrating quantitative data, such as potential financial losses in the event of cyber incidents, would provide a more precise assessment of risks.

Supply Chain Dynamics: Further exploration of potential disruptions in an international supply chain, considering geopolitical and logistical challenges, would offer a more holistic view.

User Experience: An evaluation of how digitalisation impacts customer experience and whether online features align with customer preferences would enhance risk assessment accuracy.

# 3. Recommendations

Considering the assessment, proceeding with digitalisation is recommended. However, it's advised to conduct a more detailed risk analysis, incorporating quantitative insights, supply chain intricacies, and customer preferences, to provide a comprehensive foundation for decision-making.

## Approach and Timeline

The approach to digitalisation involves phased implementation as outlined below:

A screenshot of a computer

Description automatically generated

# Conclusion

This critical evaluation underscores the importance of a thorough risk analysis to inform decision-making. While the existing assessment offers valuable insights, the suggested refinements would elevate its effectiveness in guiding Pampered Pets' digitalisation journey.

# References:

* International Organisation for Standardisation. (2009). ISO 31000:2009 - Risk management principles and guidelines. ISO.
* National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. NIST.