# Development Team Project: Risk Identification Report

## Risk Assessment Methodology for Digitalisation

### Combination of ISO 31000 and Qualitative Risk Assessment

### Hybrid Framework Approach

- Comprehensive framework: Integrating ISO 31000 and qualitative risk assessment will allow Pampered Pets to have a well-structured risk assessment that is evaluated through qualitative analysis.
- Cost-effective: this approach would not demand extensive data or resources, making it more affordable for a smaller business.
- Holistic risk assessment: the hybrid approach considers all types of risks. For instance, cyber threats, operational and reputational disruption, and providing an all-around assessment that aligns with the business goals.

## Proposed Digitalisation and Rationale:

### E-commerce Platform Implementation

- This implementation will allow Pampered Pets to expand its local and global customer base. This change will achieve the goal of growing the business and improving its online market. (kwan et al., 2019).
- High sales: online sales with no closing time will permit customers to make purchases at their own time. This will contribute to the overall business goal significantly increasing sales (Tiago et al., 2014). Also, customers may purchase online with ease and smooth payment options that will enhance customer experience and encourage repeat business (Grewal et al., 2017).

### Enterprise Resource Planning System (ERP)

- Real-time data accessibility: ERP system ensures real-time access to data across the business and provides a quick response to market changes and decision-making (Stratman, Bendoly, & Rosensweig 2009).
- Uniform interface: ERP system will combine all the single aspect of the business in a one information system that has a uniform look. All Pampered Pets processes and different computer systems would be integrated in a single uniform interface across the divisions (Csedo et al., 2018).

Customer Relationship Management Implementation (CRM)

- Improve customer Engagement: CRM system will help Pampered Pets to improve customer satisfaction through interactions, that will help meet customer needs. Efficient customer service is achieved as the CRM system enables timely and quicker responses to customer queries. (Buttle & Maklan 2019).

- Customisable marketing: personalised data can be created through promotions, campaigns, and enhancing conversion rates (Reinartz, & Kumar 2018).

Online Marketing Strategies

- Provides cheap advertisement: online marketing like social media and search engines are cost-effective ways to sell globally. Such strategies are affordable as compared to traditional marketing and provide significant returns.

- Provides visibility and accountable results: social media platforms would promote Pampered Pets' visibility by attracting more customers online in a competitive market. Also, Pampered Pets can utilise online marketing tools to monitor their performance and change strategies.

## **Risk Assessment**

| Potential Threat | Likelihood | Impact | ISO 31000 | Qualitative<br>Approach |
|---|---|---|---|---|
| Data Breaches | High | Severe | Critically identifies data protection and serves as a guide for cybersecurity measures. | Through interviews and workshops, stakeholders raise concerns about weak passwords, phishing or data breaches. |
| System Malfunction | Medium | High | Reduces downtime since it prioritises IT infrastructure | Potential marks of failures can be pointed out by frontline support like poor system integration. |
| Insider Threats | Low | High | It ensures strict access control monitoring and regular audits. | Provide an understanding of internal risk through anonymous employees' surveys and awareness of security control by staff. |

|  |  |  |  |  |
|---|---|---|---|---|
| Loss of trust | Low | High | Maintain customer trust by encouraging robust data protection policies. | Conduct customer surveys and focus groups to understand the relevance of data privacy. |

## Mitigation for Digitalisation Risks

Cybersecurity Threats

- ISO 31000 suggests implementation of strong encryption, access controls and regular security audit to protect sensitive data (ISO, 2018).
- Regular staff training and workshops to be aware of phishing threats and updating passwords to enhance Pampered Pets' security system.

Operational Threats

- Implement a comprehensive management plan that involves contingency planning, regular maintenance checks and a redundant system as recommended by ISO 31000.
- Coupled with qualitative methods like collecting feedback from staff about specific challenges and system integration failures can help adjust contingency plans and ensure that they are effective and practical.

Reputational Threats

- Provide transparent data privacy and protection that reassures customers' commitment to the business.
- Feedback from customer surveys and focus groups for feedback concerns about data privacy.

Insider Threats

- Strong access control, regular audit and systems monitoring to detect insider threats.
- Anonymous employee feedback and surveys, which discloses potential risks and help to adjust security measures.

## Risk Assessment Report for Pampered Pets Using the OCTAVE Framework

The following report identifies potential risks and proposes mitigation strategies using the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) risk assessment framework for Pampered Pets and its operational objectives.

**OCTAVE Framework Overview**

The OCTAVE framework consists of three main phases:

1. **Phase 1: Build Asset-Based Threat Profiles**
2. **Phase 2: Identify Infrastructure Vulnerabilities**
3. **Phase 3: Develop Security Strategy and Mitigation**

**Phase 1:**

**1. Critical Assets**

The critical assets of Pampered Pets include:

- **Customer Information**
- **Product Inventory and Tracking System**
- **Financial Data**
- **In-House Recipe Information**
- **Supplier Information**

**2. Threats to Critical Assets**

| **Threat Category** | **Asset Affected** | **Threat Description** | **Likelihood** | **Impact** |
|---|---|---|---|---|
| **Cybersecurity** | Customer Information | Unsecured wireless network- vulnerable to hackers. | Medium | High |
| **Data Integrity** | Product Inventory and Tracking System | Corruption or data loss from system failure. | Medium | Medium |
| **Human Error** | Product Inventory and Tracking System | Accidental deletion or overwriting of key inventory data. | High | Medium |
| **Theft/Vandalism** | Customer Information, Financial Data | Theft of computers or physical breaches could lead to loss of data. | Low | High |
| **Supply Chain Disruption** | Supplier Information, In-House Recipe Information | External supplier issues or disruptions in local farms could impact inventory. | Low | Medium |

**Phase 2:**

**1. Wireless Network Security**

- **Weakness**: The wireless network is shared by employees for personal apps, which increases exposure to threats like unauthorised access, malware, or viruses. Unauthorised access could lead to data breaches or cyberattacks, compromising customer and financial data.

**2. Limited Cybersecurity Awareness**

- **Weakness**: Employees may not be fully trained on cybersecurity best practices, especially given their reliance on smartphones and a wireless network. Human error, such as clicking on phishing emails or using weak passwords, could introduce vulnerabilities.

**3. Physical Security**

- **Weakness**: The shop's location in a leafy suburb reduces the risk of crime, but the lack of robust physical security measures (e.g., surveillance) could expose the business to theft or vandalism. Theft or vandalism could result in the loss of equipment and critical data stored on physical machines.

**Phase 3:**

**1. Wireless Network Security**

- **Mitigation**: Upgrade the wireless network with strong encryption protocols (WPA3) and restrict personal device access to a separate network. Implement a secure password policy that requires regular changes. This will lead to improved protection against unauthorised access and cyberattacks.

**2. Employee Cybersecurity Training**

- **Mitigation**: Conduct regular cybersecurity training for all employees, focusing on recognising phishing attempts, using strong passwords, and ensuring device security. This will reduce the likelihood of human error introducing vulnerabilities.

**3. Physical Security Enhancements**

- **Mitigation**: Install security cameras, alarms, and secure locks for the store. Implement a policy for locking away computers and other critical devices when not in use. This will reduce the risk of theft or vandalism leading to data loss or business disruption.

### Conclusion

Pampered Pets faces a variety of risks, both from its IT infrastructure and its reliance on local suppliers. The OCTAVE framework has helped identify critical assets, potential threats, and vulnerabilities, leading to specific mitigation strategies. By implementing the recommended actions, Pampered Pets can significantly reduce the likelihood and impact of risks, safeguarding its business operations, customer data, and financial integrity.

## REFERENCES

- Buttle, F. & Maklan, S. (2019). *Customer Relationship Management: Concepts and Technologies. 4th ed. Routledge.*
- Grewal, D., Roggeveen, A.L., and Nordfalt, J. (2017). *The future of retailing*. Journal of Retailing, 93(1), pp. 1-6.
- ISO (2018). *ISO 31000:2018 Risk management- Guidelines*. International Organisation for Standardisation.
- Kwan, M., Chan, A., and Lau, J. (2019). *Digital Transformation and Risk Management: Navigating the future of Business. Cambridge University Press.*
- Reinartz, W. & Kumar, V. (2018). Customer Relationship Management: Concept, Strategy, and Tools. 3rd ed. Springer.
- Stratman, J.K., Bendoly, E., & Rosenzweig, E.D. (2009). *The dynamics of capacity expansions in the service sector: Linking human resources and operations. Journal of operations Management, 27(2), pp 169-179.*