Risk Assessment (RA) Pampered Pets

Gesine Hamberger, Mauricio Lozano, Farhad Karimov, Samer Saleem, Tobias Zeier
9th of September 2024, University of Essex Online

RA – Methodology

To strategically align with the unique threat landscape of each risk, we selected several models. **ISO 31000** was chosen for its broad and flexible approach (ISO 31000:2018), while **FMEA** was selected for its detailed assessment of operational risks. **STRIDE** was used to prioritise technological and cybersecurity (CS) risks (Aven, 2016). The **CIA** Triad was applied to ensure data confidentiality, integrity, and availability (ISO/IEC 27001). Finally, **PESTLE** was employed to assess external risks (Hopkin, 2018).

Threat Assessment – Current Business Operations

Operationally, reliance on basic software and manual processes in supply chain and inventory management leads to inefficiencies and errors, risking inaccurate stock levels and financial losses (Christopher, 2016). Dependence on local suppliers also heightens vulnerability to disruptions from external factors. **Technologically**, outdated IT infrastructure exposes the business to cyber threats like malware and data breaches (Shih, 2020), while weak data governance (DG) increases the risk of data loss, inaccuracies, and regulatory non-compliance (ISO/IEC 27001). **Strategically**, the business's dependence on face-to-face sales and outdated tech makes it vulnerable to market shifts and operational inefficiencies (Sørensen, 2018).

			Risk assessment			Risk treatment						
ID	Category	Area	Event	Impact	Probability	Risk Score before treatment	Proposed treatment	Mitigation	Risk owner	Impact after extra controls	Probability after extra controls	Risk score after extra controls
1	Operationl Risk	Inventory Management	Excess inventory holding costs or stockouts	High	High	3	Reduce	Use of ERP-System to track products in stock, expiry dates, etc.	Harry	Medium	Low	1
2	Operationl Risk	Supply Chain Management	Stockouts and operational slowdowns	High	Medium	2	Reduce	Develop a resilient supply chain strategy that includes multiple suppliers, geographic diversification, and contingency planning for alternative transportation routes.	Cathy	High	Low	1
3	Technology Risk	Cyber Security	Damage, or theft of sensitive data	Very High	High	4	Reduce	Enhanced security measures, such as implementing multi-factor authentication (MFA), data encryption, and role-based access control (RBAC)	Alice/Cathy	Medium	Low	1
4	Technology Risk	Data Managment & Governance	Data inaccuracies, loss, and regulatory non-compliance	Medium	Medium	2	Reduce	Strengthening DG and regularly patching systems are recommended to ensure compliance, protect sensitive information, maintain operational continuity	Alice/Cathy	High	Low	1
5	Strategic Risk	Market Dependecy	Revenue loss, and vulnerability to market fluctuations or downturns	Very High	High	4	Reduce	Enhance resilience with energy-efficient technologies and compliance with data regulations to maintain profitability.	Cathy	im	Medium	2
6	Strategic Risk	Inefficiencies	Increased costs, and reduced productivity, financial losses and decreased competitiveness	Medium	Medium	2	Reduce	Prepare for external risks with flexible pricing, digital transformation incentives, and a disaster recovery plan.	Cathy	Low	Low	1

Table 1: A.1 ISO 31000 (Hamberger et al., 2024)

Operational Risks

Reliance on basic software and manual processes leads to inefficiencies, human error, inaccurate stock levels, and delayed order fulfilment (Shih, 2020). Dependence on local suppliers increases vulnerability to disruptions from natural disasters, economic

downturns, and logistical challenges (Christopher, 2016). The lack of automation and robust forecasting increases the risk of overstock or stockouts.

The **FMEA** analysis identifies two key risks: **Inaccurate Forecasting**, driven by outdated methods, can lead to overstocking or stockouts (Aven, 2016). This results in high inventory costs or missed sales opportunities (Shih, 2020). The risk has a moderate severity and high occurrence, with an RPN (Risk Priority Number) of 245. Mitigation involves implementing advanced forecasting tools within an ERP system (Chevalier, 2024). **Supply Chain Disruptions**, external factors like logistical delays or natural disasters can disrupt the supply chain, causing stockouts and operational slowdowns, negatively impacting customer satisfaction and revenue (Christopher, 2016). The risk severity is high but has a lower occurrence, with an RPN of 144. Mitigation includes developing a resilient supply chain strategy with multiple suppliers and contingency planning (Shih, 2020).

Failure Mode	Effect	Cause	Severity (S)	Occur-rence (O)	Detection (D)	RPN	Mitigation
Bad Fore-casting	Financial losses from excess inventory holding costs or missed sales opportunities due to stockouts.	Reliance on outdated or manual forecasting methods that fail to account for current market trends and seasonality.	7	7	5	245	Implement advanced forecasting tools within an ERP system that account for market trends, seasonality, and historical data to improve accuracy.
Supply Chain Disruptions	Delays in receiving supplies result in stockouts and operational slowdowns, affecting customer satisfaction and revenue.	Inadequate logistical planning, failure to anticipate or prepare for external disruptions in the supply chain.	8	6	3	144	Develop a resilient supply chain strategy that includes multiple suppliers, geographic diversification, and contingency planning for alternative transportation routes.

2: A.2 FMEA Analysis (Hamberger et al., 2024)

Technology Risks - Cybersecurity & Data Management:

Outdated IT systems and inadequate CS measures are a risk. These vulnerabilities expose the business to threats like malware, ransomware, and data breaches (Priyanka

& Smruthi, 2020). Poor data management and lack of robust governance further increase the risks of data inaccuracies, loss, and regulatory non-compliance (ISO/IEC 27001). Together, these issues threaten data integrity, operational stability, and could result in significant financial and reputational damage (Alzahrani et al., 2022).

The **STRIDE** analysis identifies key risks, including **spoofing**, **tampering**, **repudiation, information disclosure**, **denial of service (DoS),** and **elevation of privilege** (Aven, 2016). These risks stem from improper security controls, inadequate identity management, and outdated IT infrastructure (NIST SP 800-53). The analysis highlights the need for enhanced security measures, such as multi-factor authentication (MFA), data encryption, and role-based access control (RBAC) (ISO/IEC 27001). Additionally, strengthening DG and regularly patching systems are recommended to ensure compliance, protect sensitive information and ensuring long-term resilience.

Threat	Description	Mitigations
Spoofing	Improper security controls could lead to spoofed internal resources, potentially launching phishing campaigns against employees or customers.	Implement MFA, encrypt data, and enforce RBAC to protect against spoofing.
Tampering	Lack of complex identity management and encryption allows unauthorised users to modify data, leading to potential corruption or loss.	Use encryption, data masking, and strict access controls to prevent tampering and information disclosure.
Repudiation	Lack of proper logging and monitoring allows users to deny actions taken within the system, making it difficult to trace incidents or hold users accountable.	Implement strong logging and monitoring practices to ensure accountability and prevent users from denying their actions.
Information Disclosure	Poor DG could result in unauthorised access and exposure of sensitive data, risking non-compliance with regulations like GDPR.	Strengthen data integrity and governance to ensure compliance with regulations and protect against unauthorised access.
Denial of Service (DoS)	Cyberattacks could disable POS and data management systems, causing operational downtime.	Deploy DDoS protection, establish system redundancy, and regularly patch systems to prevent DoS attacks.
Elevation of Privilege (PrivEsc)	Legacy systems with unpatched vulnerabilities increase the risk of attackers gaining elevated access and full control over critical systems.	Enhance security controls, patch legacy systems, and enforce RBAC to mitigate elevation of privilege risks.

Table 3: A.3 STRIDE Analysis (Hamberger et al., 2024)

Strategic Risks - Market Dependency & Inefficiencies:

Reliance on face-to-face sales (constituting 90% of its business) and the use of outdated tech is a risk for its operations (Chevalier, 2024). This dual dependency

exposes the business to vulnerabilities from shifts in consumer behaviour, local economic downturns, and operational inefficiencies (Sørensen, 2018). The lack of modern tech exacerbates these risks by limiting the ability to adapt to changing market conditions, maintain data integrity, and ensure operational continuity (Shih, 2020).

PESTLE identifies several key risks: **Politically**, local regulations and missed opportunities for digital incentives may affect business operations (Qureshi, 2022). **Economically**, downturns could reduce consumer spending, while outdated tech increases maintenance costs (Grewal et al., 2018). **Socially**, shifting preferences towards online shopping could harm customer retention (Custify, 2024). **Technologically**, reliance on old systems makes the business vulnerable to inefficiencies and cyberattacks (Priyanka & Smruthi, 2020). **Legally**, non-compliance with data protection laws poses risks, while **environmental** factors, like natural disasters and high energy consumption, threaten operational continuity (NIST SP 800-53). Mitigations include, modernising operations, ensuring regulatory compliance, and preparing for external challenges (ISO/IEC 27001).

Factor	Description	Mitigations
Political	Local government policies, increased taxes, or restrictions could impact physical sales; government incentives for digital transformation may disadvantage outdated businesses.	Enhance resilience with energy-efficient technologies and compliance with data regulations to maintain profitability. Prepare for external risks with flexible pricing, digital transformation incentives, and a disaster recovery plan.
Economic	Economic downturns could reduce consumer spending and foot traffic; outdated tech maintenance costs could strain profitability.	
Social	Shifting consumer preferences towards online shopping and advanced services could reduce in-store visits and damage reputation.	
Technological	Outdated systems put businesses at a competitive disadvantage, leading to inefficiencies, cyber vulnerabilities, and the inability to leverage new technologies.	
Legal	Outdated tech may not meet legal requirements for data protection, exposing the business to penalties; changes in consumer protection laws could require online services.	
Environmental	Environmental issues like natural disasters could disrupt operations; outdated tech is less energy-efficient, leading to higher costs and environmental impact.	

Table 4: A.4 PESTLE Analysis (Hamberger et al., 2024)

RA – Business Digitalisation

As we embark on this digitalisation journey, it is crucial to assess the risks to ensure a secure and efficient transformation. This section outlines the proposed changes for a digitalisation process, followed by a detailed analysis using the Confidentiality, Integrity,

Availability (CIA) Triad threat model.

Key changes include implementing an **e-commerce (EC) platform** to expand market reach, upgrading to a modern **ERP system** for better inventory and supply chain management, and strengthening **CS measures** through MFA, encryption, and system upgrades (Alzahrani et al., 2022). Additionally, the adoption of **automated DG tools** will ensure compliance with regulations like GDPR and enhance data integrity (NIST SP 800-53). These changes aim to improve efficiency, security, and overall resilience.

Proposed Change	Details
Implementation of an EC Platform	Develop and launch an online store to expand market reach and cater to the growing preference for online shopping. Integrate the EC platform with existing inventory management systems to ensure real-time stock updates and seamless order fulfilment.
Upgrade to a Modern ERP System	Replace the current basic software with a comprehensive ERP system that includes advanced modules for forecasting, inventory management, and supply chain management. Utilise predictive analytics to enhance inventory management and demand forecasting accuracy.
Enhancement of CS Measures	Deploy MFA, encryption, and RBAC to protect against cyber threats. Upgrade legacy systems to reduce vulnerabilities and improve resilience against cyberattacks.
Adoption of Automated DG Tools	Implement automated tools for data management and governance to ensure compliance with regulations such as GDPR. Introduce real-time monitoring and auditing to maintain data integrity and prevent unauthorised access or modifications.

Table 5: A.5 Proposed Changes for Digitalisation (Hamberger et al., 2024)

The **CIA Triad** analysis highlights key risks and mitigation strategies. To protect sensitive business and customer data, the analysis recommends implementing encryption, MFA, and strong access controls, particularly for the EC platform and ERP system upgrade. To maintain data integrity, it advises using data validation checks, secure coding practices, and thorough testing during system migrations (ISO/IEC 27001). For availability, the focus is on deploying DDoS protection, scheduling upgrades during off-peak hours, and ensuring system redundancy (NIST SP 800-53). These measures are essential to safeguard against data breaches, unauthorised access, system downtimes, and potential data corruption (ISO 31000:2018).

CIA Component	Area	Risk	Mitigation
Confidentiality	EC Platform	Data breaches exposing customer information.	Implement SSL/TLS encryption, secure payment gateways, and strong access controls. Conduct regular security audits.
Confidentiality	ERP System Upgrade	Unauthorised access to business-critical data during and after the system upgrade.	Implement RBAC and MFA and encrypt data during transfer and storage.
Confidentiality	CS Enhancement	Phishing attacks leading to compromised credentials.	Conduct regular employee training, enforce MFA, and implement email filtering tools.
Confidentiality	Automated DG Tools	Inadequate protection of customer and business data, leading to compliance failures.	Use encryption, data masking, and access controls to comply with regulations like GDPR.
Integrity	EC Platform	Tampering with customer orders or financial transactions, leading to data corruption or loss.	Implement data validation checks, transaction logging, and secure coding practices. Perform regular audits.
Integrity	ERP System Upgrade	Data loss or corruption during migration from the old to the new ERP system.	Develop a detailed data migration plan with backups and integrity checks. Perform thorough testing before going live.
Integrity	CS Enhancement	Insider threats or cyberattacks altering or deleting critical data.	Enforce strict access controls, regularly update and patch systems, and monitor for suspicious activity.
Integrity	Automated DG Tools	Automated tools failing to maintain data accuracy, leading to decision-making errors.	Combine automated data integrity checks with manual oversight. Conduct regular audits.
Availability	EC Platform	DDoS attacks could make the online platform unavailable to customers.	Deploy DDoS protection services and a CDN to ensure continuous availability.

Table 5: A.6 CIA Analysis (Hamberger et al., 2024)

Conclusion

Pampered Pets is at a pivotal point in deciding whether to embrace digital transformation, weighing potential benefits against the associated risks. Establishing an online presence could boost revenue by up to 50%, while transitioning to an international supply chain might reduce costs by 24% (Shih, 2020). Conversely, not adopting a digital strategy could result in the loss of up to 33% of its existing customers as consumer preferences shift towards online shopping (HubSpot, 2024).

Finally, digitalisation offers an opportunity for growth and competitiveness, provided it is accompanied by risk management to mitigate potential disruptions and quality control challenges. By strategically navigating, they can safeguard a secure and successful future in an increasingly digital marketplace. Pampered Pets needs to be aware that adopting the changes would imply significant transformation costs (Sørensen, 2018).

Word count: 1095

APPENDIX

A.1 ISO 31000 Risk Matrix

The Risk matrix below was used to conduct the risk assessment of Pampered Pets' business as it currently is.

Impact				
Very High (4)	Medium (2)	High (3)	Very High (4)	Very High (4)
High (3)	Low (1)	Medium (2)	High (3)	Very High (4)
Medium (2)	Low (1)	Medium (2)	Medium (2)	High (3)
Low (1)	Low(1)	Low (1)	Medium (2)	Medium (2)
	Low (1)	Medium (2)	High (3)	Very High (4)
		Probability		

Table 6: Risk Matrix (Hamberger et al., 2024)

A.2 FMEA Analysis Table

Purpose:

The purpose of the Failure Modes and Effects Analysis (FMEA) Table is to pinpoint ways things could go wrong in the day-to-day operations at Pampered Pets when transitioning to a digital setup. The table examines the impacts, reasons behind failures how severe they are, how likely they are to happen and how easily they can be detected. It then calculates a Risk Priority Number (RPN) to rank these risks in order of importance. Recommendations, for managing each identified risk are also provided.

A.3 STRIDE Analysis Table

Purpose:

The STRIDE Analysis Table helps Pampered Pets pinpoint risks to their digitalisation initiatives by applying the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). This table explains each potential threat and suggests ways to avoid or reduce their negative effects.

A.4 PESTLE Analysis Table

Purpose:

Pampered Pets' business environment can be impacted by external factors that are identified and evaluated in the PESTLE Analysis Table, especially in context of digitalisation. This analysis considers Political, Economic, Social, Technological, Legal, and Environmental factors and suggests mitigation strategies to manage or minimise the potential impact of these factors

A.5 Proposed Changes for Digitalisation Table

Purpose:

The Table of Proposed Digitalisation Upgrades details the strategies that Pampered Pets intends to introduce to upgrade its business practices and keep up with today’s digital focused market trends effectively enhancing productivity and customer satisfaction while prioritising data protection.

A.6 CIA Triad Analysis Table

Purpose:

The CIA Triad Analysis Table evaluates the risks and mitigation strategies for Confidentiality, Integrity, and Availability (CIA) concerning different components of Pampered Pets' digitalisation initiatives. Throughout the process of transformation, it is crucial to prioritise maintaining data security and always ensuring business continuity.

References:

Hamberger, G., Saleem, S., Karimov, F., Lozano, M. & Zeier, T. (2024) Risk Assessment (RA) Pampered Pets. *SRM September 2024*. Essay submitted to the University of Essex Online.

Aven, T. (2016). *Risk assessment and risk management: Review of recent advances on their foundation*. European Journal of Operational Research. Available at:https://www.sciencedirect.com/science/article/pii/S0377221715011479 [Accessed 7 September 2024].

Alzahrani, A., Alqazzaz, A., Fu, H., & Almashf, N. (2022). *Cyber Security Threats in Cloud Computing: A Literature Review. Security Journal*. Available at: https://personales.upv.es/thinkmind/dl/journals/sec/sec_v15_n34_2022/sec_v15_n34_2022_1.pdf [Accessed 24 August 2024].

Chevalier, S. (2024). *Global retail e-commerce sales 2014-2027*. Available at: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ [Accessed 22 August 2024].

Christopher, M. (2016). *Logistics & Supply Chain Management*. Pearson Education Limited. Available at:https://www.ascdegreecollege.ac.in/wp-content/uploads/2020/12/Logistics_and_Supply_Chain_Management.pdf [Accessed 7 September 2024].

Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital Marketing: Strategy, Implementation, and Practice*. Pearson Education Limited. Available at:https://digilib.stiestekom.ac.id/assets/dokumen/ebook/feb_27aff686c21a3ec16bdc9e2e8d785bf6b8d8e4e8_1655821975.pdf [Accessed 7 September 2024].

Custify (2024). 8 Challenges in Customer Retention and How to Overcome Them. Available at: https://www.custify.com/blog/customer-retention-challenges [Accessed 11 August 2024].

Frigo, M.L., & Anderson, R.J. (2011). *Strategic Risk Management: A Primer for Directors and Management Teams*. The Journal of Corporate Accounting & Finance. Available at: https://corpgov.law.harvard.edu/2012/08/23/strategic-risk-management-a-primer-for-directors/ [Accessed 7 September 2024].

Grewal, D., Roggeveen, A.L., & Nordfält, J. (2018). *The Future of Retailing. Available at:* https://www.sciencedirect.com/science/article/pii/S0022435916300872 [Accessed 7 September 2024].

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

HubSpot (2024). 22 Examples of Customer Retention Strategies That Actually Work. Available at: https://blog.hubspot.com/service/customer-retention-strategies [Accessed 22 August 2024].

Innab, N., & Alamri, A. (2018). The Impact of DDoS on E-commerce. *IEEE Xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/8593125 [Accessed 24 August 2024].

ISO 31000:2018. *Risk Management - Guidelines*. Available at:https://www.iso.org/standard/65694.html [Accessed 7 September 2024].

ISO/IEC 27001: *International Standard for Information Security Management Systems*. Available at:https://www.iso.org/standard/27001 [Accessed 7 September 2024].

NIST SP 800-53. *Security and Privacy Controls for Information Systems and Organizations*. Available at:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed 7 September 2024].

Priyanka, A.K., & Smruthi, S.S. (2020). Web Application Vulnerabilities: Exploitation and Prevention. *IEEE Xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/9182928 [Accessed 24 August 2024].

Qureshi, Z. (2022). How digital transformation is driving economic change. *Brookings Institution*. Available at: https://www.brookings.edu/articles/how-digital-transformation-is-driving-economic-change/ [Accessed 10 August 2024].

Shih, Willy C. (2020). Global Supply Chains in a Post-Pandemic World. *Harvard Business Review*. Available at: https://hbr.org/2020/09/global-supply-chains-in-a-post-pandemic-world [Accessed 22 August 2024].

Sørensen, B.T. (2018). *Digitalisation: An Opportunity or a Risk? Journal of European Competition Law & Practice*. Available at:https://academic.oup.com/jeclap/article/9/6/349/5026007 [Accessed 7 September 2024].