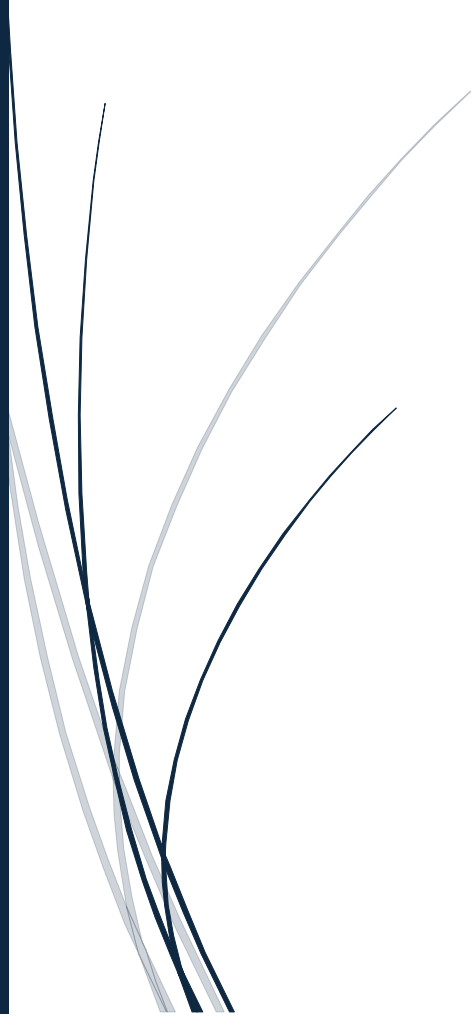
08/09/2025

University Of Essex

Risk Identification Report

MSc Cyber Security



Group Work

Table of Contents

1.Introduction

Pampered Pets (PP), a small enterprise in Hashington-on-the-Water, specialises in premium pet foods sourced from regional farms. Historically dependent on manual processes and face-to-face sales, the company is now pursuing digital transformation through networked inventory systems and wireless connectivity. While these innovations promise operational efficiency and expanded market reach, they simultaneously introduce risks to data confidentiality, service continuity, and regulatory compliance. Like several SMEs, (PP) reflects a wider sectoral challenge: recent studies confirm that over 61 per cent of small firms experienced cyber breaches in the past year, often due to limited technical capacity and reliance on outdated infrastructure (Verizon,2024; Ponemon Institute,2023). In this context, a systematic risk assessment is required to ensure resilience and maintain customer trust. This study evaluates (PP's) cyber risk exposure by applying ISO27005:2022 to current operations and the NIST Cybersecurity Framework v2.0 to future digitalisation, complemented by STRIDE-based threat modelling.

2. Methodology Selection and Critical Comparison

For (PP) current manual operations, ISO27005:2022 is adopted due to its integration with ISO27001 and suitability for SMEs with limited infrastructure. Its qualitative approach enables risk identification and treatment without requiring extensive technical resources (Disterer,2023). ISO27005's reliance on subjective scoring risks undervaluing rare but catastrophic threats—problematic for SMEs like (PP), where a single incident (e.g., supplier-data-compromise) could cripple operations. The analysis highlights (Ahmed,Khan & Patil,2022). This creates a risk that less visible but high-

impact threats, such as supplier-side data compromise, could be underestimated. Alternatives such as FAIR offer financial quantification (Jones & Ashenden,2021), nevertheless their complexity and intensive data needs render them impractical in this context.

For the digitalisation phase, the NIST CSF v2.0 is recommended. Its modular functions Identify, Protect, Detect, Respond, recover, support phased adoption, aligning with incremental SME digitalisation strategies (Keller & Rudy,2024). Despite its origins in U.S. critical infrastructure, its international uptake and compatibility with ISO standards strengthen its global relevance (ENISA,2023). By contrast, OCTAVE and CRAMM were rejected due to greater complexity and cost (Smith & Rupp,2023). A phased application of ISO/IEC 27005 and NIST CSF therefore provides both feasibility and scalability: the former delivers immediate visibility of risks within (PP's) current constraints, while the latter offers a roadmap for controlled security maturity as digitalisation advances.

3.STRIDE-Based Threat and Risk Modelling

To evaluate vulnerabilities, the STRIDE framework was applied to (PP) current IT environment. STRIDE classifies threats into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Shostack,2014).

Figure 1: STRIDE Threat Model Analysis for Pampered Pets' Current IT Environment

Threat Category	Before Score	After Score	Residual Risk
Insider threats	4 (High)	2 (Low)	Low
Phishing	4 (High)	3 (Medium)	Medium
Data breach	5 (Very High)	2 (Low)	Low
Weak authentication	4 (High)	2 (Low)	Low
Third-party risk	4 (High)	3 (Medium)	Medium
Incident response	5 (Very High)	2 (Low)	Low
Governance & compliance	4 (High)	2 (Low	Low

Likelihood and impact were assessed on a three-point scale following ISO/IEC-27005:2022 guidance (ISO,2022). This pragmatic approach supports ease of adoption in SMEs, though its limited granularity may oversimplify risk differentiation, particularly where low-frequency but high-severity threats are concerned. The analysis shows Harry's spreadsheet reliance creates integrity risks, Cathy's digitalisation role makes her a prime phishing target, Alice's centralised decision-making is a governance bottleneck, and Andrea's limited training heightens insider error risks. This aligns with ENISA's (2023) findings that SMEs remain disproportionately at risk due to legacy systems, inadequate training, and weak access controls. By combining STRIDE with structured likelihood–impact scoring, (PP) gains an evidence-based risk-register that captures both technical and behavioural vectors. For (PP), this dual perspective reveals that cultural vulnerabilities could amplify technical weaknesses, making investment in both redundancy and staff awareness equally critical to resilience.

4.Risk Mitigation Strategy

(PP's) mitigation plan applies a defence-in-depth approach, addressing technical and human-factors while ensuring scalability, cost-effectiveness, and SME alignment with NCSC (2023) and ENISA (2023).

4a) Network-Security

Segmentation isolates critical systems from guest Wi-Fi, reducing lateral movement. WPA3, unique credentials, hidden SSIDs, and MAC filtering strengthen controls (Alasmary et al., 2021).

4b) Patch & System Management

Structured patching ensures timely OS, app, and firmware updates. Hardening disables unused services, enforces strong passwords, disk encryption, and ISO-aligned configs (ISO, 2022).

4c) Endpoint-Protection

SME-suited antivirus, firewalls, MDM, application whitelisting, and auto-updates safeguard devices.

4d) Backup & Recovery

Hybrid backups—local plus encrypted cloud—aid ransomware resilience. Integrity tests and recovery playbooks cut MTTR (Khan et al., 2022).

4e) Access-Control

RBAC enforces least-privilege; MFA secures privileged accounts. Audit logs enhance accountability (SANS, 2023).

4f) Security-Awareness

Scenario-based phishing/data training, simulations, and refresher policies improve behaviour (Ponemon, 2023).

Threat Posture Metrics (Before vs. After)

Threat Category	Before Score	After Score	Residual Risk
Insider threats	4 (High)	2 (Low)	Low
Phishing	4 (High)	3 (Medium)	Medium
Data breach	5 (Very High)	2 (Low)	Low
Weak authentication	4 (High)	2 (Low)	Low
Third-party risk	4 (High)	3 (Medium)	Medium
Incident response	5 (Very High)	2 (Low)	Low
Governance & compliance	4 (High)	2 (Low	Low

5. Risk Assessment of the Digitalisation Plan

5a) Digitalisation Proposals

(PP's) aims to launch a secure e-commerce platform, deploy an ERP system with cloud-based storage, integrate certified online payment solutions, and expand digital marketing through social media and blogging. Digitalisation enhances efficiency and customer engagement but elevates risks: ERP downtime could mirror today's warehouse failures, cloud misconfigurations could exceed current spreadsheet errors, and GDPR fines could outweigh today's minimal compliance exposure (Alahmari & Duncan,2020).

5b) Methodology Selection

A dual-framework approach is adopted. ISO/IEC-27005:2022 provides a structured yet

flexible process for risk identification and evaluation suited to SMEs with limited resources (ISO,2022). Complementing this, NIST-SP-800-30 enables qualitative assessment of likelihood and impact via a risk matrix (NIST,2012). This balance of rigour and practicality supports prioritisation of critical risks. Alternatives such as FAIR or OCTAVE were considered but rejected due to higher complexity and resource demands (Jones & Ashenden,2021).

5c) Threat and Risk-Modelling

Asset/Service	Threat	Likelihood	Impact	Risk
Online store	Phishing & credential theft	Medium	High	High
Cloud storage	Misconfiguration & breach	Medium	High	High
Online payments	Fraud/insecure processing	Low	High	Medium
Website/social media	DDoS attacks	Medium	Medium	Medium
ERP software	Malware/ransomware	Medium	High	High
Customer database	GDPR non-compliance	Medium	Very High	High
APIs/plugins	Third-party exploits	Medium	High	High

5d) Risk-Mitigation Strategy

Controls include MFA, phishing training, encryption, and access controls for cloud storage, PCI-DSS-compliant gateways, WAFs, and CDN-based DDoS protection, endpoint-detection, GDPR-compliant consent management, and vendor risk assessments with SLAs (OWASP,2023; ENISA,2023; Gartner,2024). These align with defence-in-depth and provide a scalable pathway to cyber resilience.

6.Strategic Recommendations

6a) Summary of Key Risks and Benefits

(PP's) current operations face high-impact risks, including unpatched legacy systems,

unsecured wireless connectivity, lack of structured backups, and minimal user access controls. These weaknesses expose the business to service disruption and reputational harm. Digitalisation amplifies exposure to cloud misconfiguration, GDPR non-compliance, and supply chain vulnerabilities but simultaneously enables improved governance, scalability, and customer engagement. Research indicates that an online presence could increase revenue by up to **50%** (Culot et al.,2021), while reliance on international supply chains could reduce procurement costs by approximately **24%** (Deloitte,2023) but weaken resilience against disruption. Conversely, failure to digitalise risks the loss of up to **33%** of existing customers (Deloitte,2023), underscoring the strategic necessity of transformation.

Risk Area	Current Operations	Digitalised Operations	Risk Level
Legacy systems	Frequent downtime, manual errors	Requires investment, migration risks	Medium
Data security	Low threat, mostly local	Higher cyber risk, mitigated via protocols	High
Staff readiness	Familiarity with processes	Training needed, cultural change	Medium
Backup & continuity	Manual, limited	Automated backups, continuity plan	Low
Supply chain resilience	Localised, stable	Global exposure, mitigations required	Medium

Area	Impact	Metric (%)
Online presence	Projected growth in sales and brand reach	50%
International supply chain	Potential cost reduction, reduced local resilience/trust	24%
Failure to digitalise	Risk of customer attrition due to outdated processes	33%

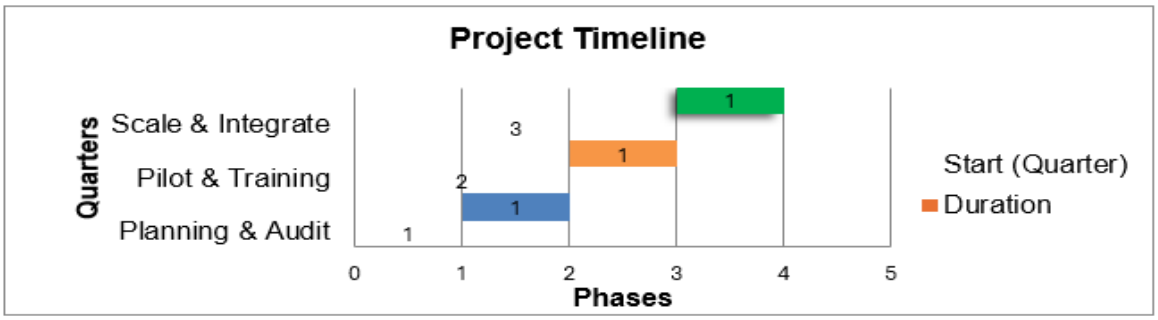
6b) Phased Implementation Approach

Security Baseline: Patch-management, network segmentation, encrypted hybrid backups, and enforced multi-factor authentication.

Pilot Deployment: Launch GDPR-compliant e-commerce and PCI-DSS-certified payments, supported by cloud-hosted ERP and vendor risk management.

Cultural Integration: Deliver regular security awareness training, phishing simulations, and policy refreshers to embed cyber resilience.

This model reflects defence-in-depth and the NIST-CSF principle of continuous improvement. Quarterly reviews against ISO27005 and NIST benchmarks will ensure iterative adaptation to emerging threats.



7. Conclusion

Digitalisation is strategically essential: delaying risks 33% customer attrition, while Orla O'dour's investment offsets adoption costs and governance gaps. Though GDPR and cloud reliance add overheads, these are outweighed by efficiency gains, resilience, and survival in a digital-first market. Combining ISO27005 with STRIDE modelling offers a cost-effective, standards-aligned strategy for SMEs, enabling (PP's) to balance risk, resilience, and sustainable growth.

Word Count 1100

8.Reference

Ahmed, R., Khan, S. & Patil, P. (2022) *Risk assessment practices in micro and small businesses: challenges and opportunities*. Journal of Small Business Security, 14(2), pp. 45–63.

Alahmari, A. & Duncan, B. (2020) Cybersecurity challenges in SMEs adopting digital platforms: a risk-based approach. *International Journal of Cybersecurity Intelligence and Cybercrime*, 3(2), pp. 22–41.

Alasmary, W., Alhaidari, F., Alasmary, W., Alsolami, E. & Alhaidari, S. (2021) Enhancing wireless security in SMEs: WPA3 adoption and implementation challenges. *International Journal of Information Security Research*, 11(3), pp. 120–129.

Culot, G., Nassimbeni, G., Orzes, G. & Sartor, M. (2021) Behind the definition of Industry 4.0: analysis and open questions. *International Journal of Production Economics*, 226, pp. 1–15.

Deloitte (2023) *2023 Global SME Digitalisation Report*. London: Deloitte.

Disterer, G. (2023) Risk management for SMEs: application of ISO/IEC 27005. *Information Security Journal: A Global Perspective*, 32(1), pp. 36–44.

ENISA (2023) *Cybersecurity for SMEs: Challenges and Recommendations*. European Union Agency for Cybersecurity. Available from: https://www.enisa.europa.eu [Accessed 16 August 2025].

Gartner (2024) *Top Cybersecurity Trends for 2024*. Stamford, CT: Gartner Inc.

ISO (2022) *ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection – Guidance on Information Security Risk Management*. Geneva: International Organization for Standardization.

Jones, A. & Ashenden, D. (2021) *Risk Management for Information Security: A FAIR Approach*. London: Routledge.

Keller, P. & Rudy, T. (2024) SME adoption of the NIST Cybersecurity Framework: global perspectives. *Journal of Information Assurance and Security*, 19(1), pp. 12–29.

Khan, R., McLaughlin, K. & Laverty, D. (2022) Cloud-based backup strategies for ransomware resilience in SMEs', *Computers & Security*, 115, pp. 102–122.

NCSC (2023) *Small Business Cyber Security Guide*. National Cyber Security Centre (UK). Available from: https://www.ncsc.gov.uk [Accessed 16 August 2025].

NIST (2012) *Guide for Conducting Risk Assessments (SP 800-30 Rev.1)*. Gaithersburg, MD: National Institute of Standards and Technology.

OWASP (2023) *OWASP Top 10 – 2023: The Ten Most Critical Web Application Security Risks*. Open Worldwide Application Security Project. Available from: https://owasp.org [Accessed 16 August 2025].

Ponemon Institute (2023) *Cost of a Data Breach Report 2023*. Traverse City, MI: Ponemon Institute.

SANS Institute (2023) *Security Best Practices for SMEs*. Bethesda, MD: SANS Institute.

Shostack, A. (2014) *Threat Modeling: Designing for Security*. Indianapolis: Wiley.

Smith, J. & Rupp, T. (2023) Comparative evaluation of cyber risk assessment frameworks for SMEs. *Journal of Information Security Research*, 13(4), pp. 67–84.

Verizon (2024) *2024 Data Breach Investigations Report (DBIR)*. New York: Verizon Communications.