**Risk Identification Report**

**Executive summary**

Pampered Pets’ legacy processes heighten operational and cyber exposure. A scoped e-commerce portal can expand sales, but adds web, payment, and supplier risk. Proceed conditionally: establish ISO 31000 governance; build with NIST CSF 2.0; minimise PCI scope; adopt monitoring/logging, tested backups, incident response, and role-based training (ISO, 2018; NIST, 2024a; NIST, 2024b; ENISA, 2021; OWASP Foundation, n.d.-a/b/c; PCI Security Standards Council, n.d.; Akamai Technologies, n.d.). We address 50% online growth, 24% sourcing savings and 33% churn risk in Recommendations.

**Methodology**

To ensure proportionality, we pair a governance standard with an operational security framework and a people-focused learning standard. The table below shows how each supports decision-making and implementation (ISO, 2018; NIST, 2024a; NIST, 2024b).

**Figure 1 - ISO 31000:2018 risk management process (adapted from ISO, 2018).**

|  |  |  |
| --- | --- | --- |
| **Area** | **Framework** | **Purpose & rationale** |
| Overall governance | **ISO 31000** (ISO, 2018) | Principles and process to set context, identify/analyse/evaluate/treat risks; proportionate to an SME and tool-agnostic. |
| Portal security lifecycle | **NIST CSF 2.0** (NIST, 2024a) | Structure controls across Identify–Protect–Detect–Respond–Recover; scalable for web retail. |
| People capability | **NIST SP 800-50r1** (NIST, 2024b) | Establish role-based, measurable learning to reduce human-factor risk. |

**Table 1 - Methodology**

**Risk Assessment of Current Operations**

Pampered Pets relies on legacy IT, a shared wireless hub and informal processes. The table summarises priority operational and cyber risks and proportionate mitigations: backup and patch discipline, basic network segmentation, simple incident logging, and a lightweight governance cadence for a small retail team (ISO, 2018; NIST, 2024b).

|  |  |  |
| --- | --- | --- |
| Risk | Concern (evidence-based) | Mitigation (proportionate) |
| Legacy PC + spreadsheets (inventory/VAT) | Single point of failure; ad-hoc patching/backups to data loss/downtime | Risk register/ownership; 3-2-1 backups with test restores; patching and anti-malware; simple incident log (ISO, 2018). |
| Flat Wi-Fi / POS exposure | Weak config enables lateral movement to front-desk system | WPA2/3; rotate admin creds; separate POS/staff VLANs; least-privilege admin (ISO, 2018). |
| People/process gaps | No formal policy/learning for phishing & weak credentials | Role-based learning programme with refreshers (NIST, 2024b). |
| Continuity/physical | Theft/fire/device failure disrupts stock control/VAT evidence | Locks/CCTV; offsite backups; minimal business-continuity checklist (ISO, 2018). |

**Table 2 - Risk Assessment of Current Operations**

**Risk Assessment of Digitalisation**

Here, we assess moving ahead with digitalisation via an e-commerce platform, routing card payments through a third-party gateway to minimise PCI scope. We map credible threats like SQL injection, XSS, denial-of-service, and web skimming to NIST CSF control themes, focusing on secure build, monitoring, incident readiness, and role-based training (OWASP Foundation, n.d.-a; n.d.-b; n.d.-c; Akamai Technologies, n.d.; PCI Security Standards Council, n.d.; NIST, 2024a; NIST, 2024b; ENISA, 2021).

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Typical vector | CSF focus | Key controls (evidence) |
| SQL injection | Unsanitised inputs (search/cart/forms) | Protect | Parameterised queries; strict input validation (OWASP Foundation, n.d.-a). |
| Cross-site scripting (XSS) | Unencoded output/user content | Protect | Output encoding; Content Security Policy; input validation (OWASP Foundation, n.d.-b). |
| Denial-of-Service | Volumetric/app-layer floods | Detect/Recover | Upstream DDoS protection; health checks; capacity planning (OWASP Foundation, n.d.-c; NIST, 2024a). |
| Web-skimming (Magecart) | Malicious/third-party JavaScript at checkout | Detect/Respond | Minimise third-party scripts; Subresource Integrity; file-integrity monitoring; alerting (Akamai Technologies, n.d.). |
| Payment/PCI exposure | Merchant site handles card data | Protect/Govern | Use PCI-listed **redirect/hosted fields** to reduce scope; complete relevant SAQ; follow PCI DSS (PCI Security Standards Council, n.d.). |
| Supplier/SME posture | Limited controls; vendor dependencies | Identify/Govern | Supplier inventory/clauses; baseline hygiene and stepwise improvements (ENISA, 2021). |

**Table 3 - Risk Assessment of Digitalization**

**Recommendations & timeline**

**Recommendation:** Proceed conditionally once governance, scope-reducing payment architecture, secure coding, monitoring/logging, tested backups, incident response, and staff training are in place; otherwise, residual risks (skimming, injection, outages) remain material (ENISA, 2021; OWASP Foundation, n.d.-a/b/c; PCI Security Standards Council, n.d.; NIST, 2024a; 2024b).

* 50% growth: Plausible. With click-and-collect + targeted local ads, the uplift is feasible; it implies ≥ (0.5B / AOV) extra orders per month.
* 24% cost saving (international): Unlikely net for core items; trial selective, non-core sourcing only.
* 33% churn without online features: Credible risk. Competitor convenience can drive attrition; offering a web catalogue/ordering materially reduces this.

**Timeline:**

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 2 - E-commerce portal implementation timeline**

**References**

Akamai Technologies (n.d.) What is Magecart? Available at: <https://www.akamai.com/glossary/what-is-magecart> (Accessed: 25 September 2025).

ENISA (European Union Agency for Cybersecurity) (2021) Cybersecurity for SMEs: challenges and recommendations. Available at: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> (Accessed: 25 September 2025).

International Organization for Standardization (2018) ISO 31000:2018 Risk management — Guidelines. Geneva: ISO. Available at: <https://www.iso.org/standard/65694.html> (Accessed: 25 September 2025).

National Institute of Standards and Technology (2024a) The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST. doi: 10.6028/NIST.CSWP.29. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (Accessed: 25 September 2025).

National Institute of Standards and Technology (2024b) SP 800-50r1: Building a cybersecurity and privacy learning program. Gaithersburg, MD: NIST. doi: 10.6028/NIST.SP.800-50r1. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf> (Accessed: 25 September 2025).

OWASP Foundation (n.d.-a) SQL Injection. Available at: <https://owasp.org/www-community/attacks/SQL_Injection> (Accessed: 25 September 2025).

OWASP Foundation (n.d.-b) Cross Site Scripting (XSS). Available at: <https://owasp.org/www-community/attacks/xss> (Accessed: 25 September 2025).

OWASP Foundation (n.d.-c) Denial of Service (DoS). Available at: <https://owasp.org/www-community/attacks/Denial_of_Service> (Accessed: 25 September 2025).

PCI Security Standards Council (n.d.) PCI Data Security Standard (PCI DSS). Available at: <https://www.pcisecuritystandards.org/standards/pci-dss/> (Accessed: 25 September 2025).