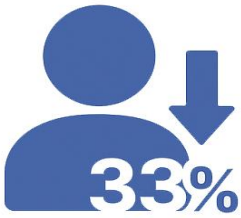
Pampered Pets Risk Identification Report

1. Introduction

This report assesses risks in maintaining Pampered Pets' current business model versus adopting a digitalised approach, to identify the most effective path for sustainable growth. The analysis is structured around three strategic questions:

Could an online presence grow the business by up to 50%?

Could shifting to an international supply chain reduce costs by up to 24%?



Could the business lose up to 33% of its customers if it does not provide online features?

It also considers technical risks and compliance with GDPR (EU, 2016) and PCI DSS (PCI Security Standards Council, 2018).

2. Pampered Pets' current situation

2.1 Risk assessment methodology

For this assessment, the ISO 27005:2022 framework has been selected as the basis for risk identification and analysis. ISO 27005 provides structured guidance on managing information security risks by systematically mapping assets, threats, vulnerabilities, and impacts (ISO, 2022). This makes it suitable for SMEs such as Pampered Pets, where resources are limited but structured risk prioritisation is essential (ENISA, 2021).

To complement this, the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) was applied to threat modelling. STRIDE provides a granular way of categorising attack vectors against digital assets (Shostack, 2014). Combining ISO/IEC 27005 with STRIDE increases analytical rigour by linking business-oriented risk analysis with technical threat categories, thereby ensuring both strategic and operational risks are captured.

2.2 Risk and thread modelling exercise

Risk identification (IEC/ISO 27005)

The risk identification process mapped Pampered Pets' assets against threats, vulnerabilities, and potential impacts.

Asset	Threats	Vulnerabilities	Potential Impact	Impact	Likelihood	Risk Level
Warehouse Computer (old PC with spreadsheet)	Malware, ransomware, data corruption, insider misuse	Outdated OS, lack of patches/antivirus, no backup, weak access controls	Loss of stock records, operational disruption, downtime	High (3)	High (3)	9 – High
Point-of-Sale (POS) Computer	System failure, malware, unauthorized access	Single point of failure, insecure Wi-Fi connection, no redundancy	Loss of sales data, inaccurate VAT/tax records, financial reporting errors	High (3)	Medium (2)	6 – High
Wireless Network (shop Wi-Fi)	Unauthorized access, sniffing, man-in-the-middle attacks	Weak WPA2 encryption, default password, shared with staff personal devices	Customer/financial data breach, regulatory penalties	High (3)	High (3)	9 – High
Customer Data (emails/orders)	Data breach, phishing, GDPR non-compliance	Stored without encryption, no secure handling policies, weak email security	Legal fines, reputational damage, loss of customer trust	High (3)	Medium (2)	6 – High
Local Supply Chain (farms)	Supply disruption, quality inconsistency	Manual ordering, no formal contracts, limited resilience	Stock shortages, inability to meet demand, reduced quality	Medium (2)	Medium (2)	4 – Medium
Staff Smartphones (using shop Wi-Fi)	Malware, data leakage, rogue access	No mobile device management (MDM), insecure apps, unsegmented network	Breach of sensitive data, gateway to wider network compromise	Medium (2)	High (3)	6 – High
E-commerce Website (future)	Hacking, SQL injection, DDoS, defacement	Insecure coding, poor hosting security, weak patch management	Website downtime, lost revenue, reputational loss	High (3)	High (3)	9 – High
Payment System (future)	Fraud, theft of cardholder data	Lack of PCI-DSS compliance, poor fraud detection controls	Financial loss, penalties, legal liability	High (3)	Medium (2)	6 – High
ERP System (future)	Insider misuse, downtime, misconfigurations	Complexity, lack of staff training, weak access controls	Inventory errors, disruption to sales/warehouse operations	Medium (2)	Medium (2)	4 – Medium
International Supply Chain (future)	Delays, counterfeit goods, political/geopolitical risks	Long lead times, no supplier due diligence, lack of monitoring	Stock shortages, reduced product quality, reputational damage	Medium (2)	Medium (2)	4 – Medium
Business Reputation & Customer Loyalty	Customer attrition, negative online reviews	No online services, weak customer engagement strategy	Up to 33% customer loss, long-term revenue decline	High (3)	High (3)	9 – High
Financial Data & Tax Records	Insider theft, ransomware, corruption	Unencrypted storage, no regular backups, limited access control	Inability to meet regulatory requirements, financial penalties	High (3)	Medium (2)	6 – High

Table 2-1 Risk identification for Pampered Pets' current and future assets using the ISO/IEC 27005 structure.

The table 2-1 links assets to threats, vulnerabilities, and impacts, with risk levels derived from impact and likelihood scores. High risks focus on digital assets handling sensitive data, while medium risks relate to ERP and supply chain dependencies.

Risk Level	Score	Assets / Key Risks
High	9	Warehouse computer (malware/ransomware); Wireless network (data breach); E-commerce website (SQL injection/DDoS); Business reputation (customer attrition)
Medium–High	6	POS system (single point of failure); Customer data (unencrypted storage); Payment system (fraud); Staff smartphones (rogue access); Financial records (ransomware)
Medium	4	ERP system (downtime/misconfigurations); International supply chain (delays, counterfeit goods)

Table 2-2 Summary of risk prioritisation for Pampered Pets' assets

This prioritisation highlights that customer trust, compliance obligations, and revenue stability are the most vulnerable areas.

Threat modelling (ISO 27005 + STRIDE)

The STRIDE model was applied to classify threats:

STRIDE Category	Example Threat	Target Asset(s)
Spoofing / Tampering	SQL injection	E-commerce portal
Information Disclosure	Eavesdropping on weak Wi-Fi	Customer data via wireless network
Denial of Service (DoS)	Malware disabling POS system; ERP misconfigurations causing downtime	POS system, ERP system
Repudiation	Customer disputes due to weak data integrity controls	Transaction and order records
Elevation of Privilege	Fraudulent transactions through misconfigured payment system	Online payment gateway

This blended approach demonstrates how vulnerabilities such as outdated systems, weak encryption, poor input validation, and untrained staff could be exploited, leading to data breaches, reputational loss, or regulatory penalties.

2.3 Mitigation measures

Mitigations were prioritised based on risk score, regulatory obligations (GDPR, PCI DSS), strategic drivers (growth, customer trust), and feasibility of implementation.

Table 2-3 Mapping of key risks, mitigation strategies, and justifications for Pampered Pets

Risk area	Key threats	Mitigation strategy	Justification
Warehouse PC	Malware, ransomware	Upgrade hardware; apply patches; enable backups	Reduces single point of failure; ensures business continuity
POS system	System failure, malware	Segmented network; redundancy; updated AV	Prevents disruption of sales and financial reporting
Wireless network	Eavesdropping, MITM	WPA3, strong passwords, staff Wi-Fi separation	Protects customer/financial data against interception
Customer data	GDPR non-compliance, breach	Encryption (AES-256), RBAC, secure email handling	Meets GDPR principles of confidentiality and integrity
E-commerce portal	SQL injection, DDoS	Secure coding, WAF, regular penetration testing	Protects availability and customer trust
Payment system	Fraud, card theft	Tokenisation, PCI DSS-compliant provider, fraud detection	Reduces exposure and shifts compliance burden
ERP system	Insider misuse, downtime	RBAC, logging/monitoring, vendor SLA	Ensures resilience and accountability
Supply chain	Delays, counterfeit goods	Supplier vetting, contracts, diversification	Strengthens resilience to external disruption
Reputation & customer loyalty	Poor UX, attrition	UX testing, 24/7 support, customer engagement	Protects long-term growth by reducing churn
Financial records	Insider theft, ransomware	Encryption, backups, limited access	Meets compliance requirements and ensures recovery

2.4 Critical Discussion

While ISO 27005 and STRIDE provide a clear and systematic structure for assessing risks, both have limitations. ISO 27005 relies heavily on qualitative scoring, which can change over time as threats evolve or as stakeholder perceptions shift. STRIDE, while effective at categorising technical threats, does not fully capture wider business considerations such as strategic objectives, regulatory pressures, or resource constraints.

3. Proposed digitalisation process

3.1 Risk assessment methodology

The OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation – Simplified) framework (Alberts and Dorofee, 2002) has been selected for assessing the digitalisation process with following benefits:

- **Designed for small organisations**: Fits Pampered Pets' scale of operations (Shevchenko et al., 2018).
- **Business-centric**: Focuses on organisational risk and technical vulnerabilities, unlike STRIDE, LINDDUN, or Attack Trees (Shostack, 2014; Shevchenko, Frye and Woody, 2018).
- **Supports qualitative analysis**: Asset-focused approach without requiring quantitative data.
- **Scalable**: Can integrate with frameworks like FAIR or ISO 27005 once sufficient data is available (Al-Dosari and Fetais, 2023).

3.2 Proposed changes

We propose three digitalisation initiatives to support Pampered Pets' strategic objectives:

- **E-commerce portal**
  Enables online sales, expanding reach beyond local customers and offering 24/7 convenience. SMEs adopting e-commerce have reported revenue increases of up to 50% (KPMG, 2015), driven by broader market access and efficiency.
  However, research shows that up to one-third of customers may abandon a brand after just one poor online experience, and two bad experiences could drive away over four-fifths—even among loyal customers (PwC, 2018; Emplifi, 2022). This risk is heightened if features like clear navigation, secure payment, and effective support are missing (Kim et al., 2010; Hossain et al., 2024; Majumder, 2025).
- **ERP system for global supply chain integration**
  Enables integrated management of procurement, inventory, and logistics—vital for international expansion. Although global supply chains are notably cost-intensive, research demonstrates that Industry 4.0-enabled systems can reduce overall supply chain costs by 20–30 % (Baumgartner, Malik and Padhi, 2020).
- **Third-party payment gateway**
  Provides encrypted transactions with fraud protection simplifying the burden of PCI DSS and GDPR compliance.

3.3 Threat model and risk assessment

The proposed digitalisation introduces interconnected risks across Pampered Pets' e-commerce ecosystem. Figure 3-1 illustrates the conceptual threat model and interaction of critical assets.

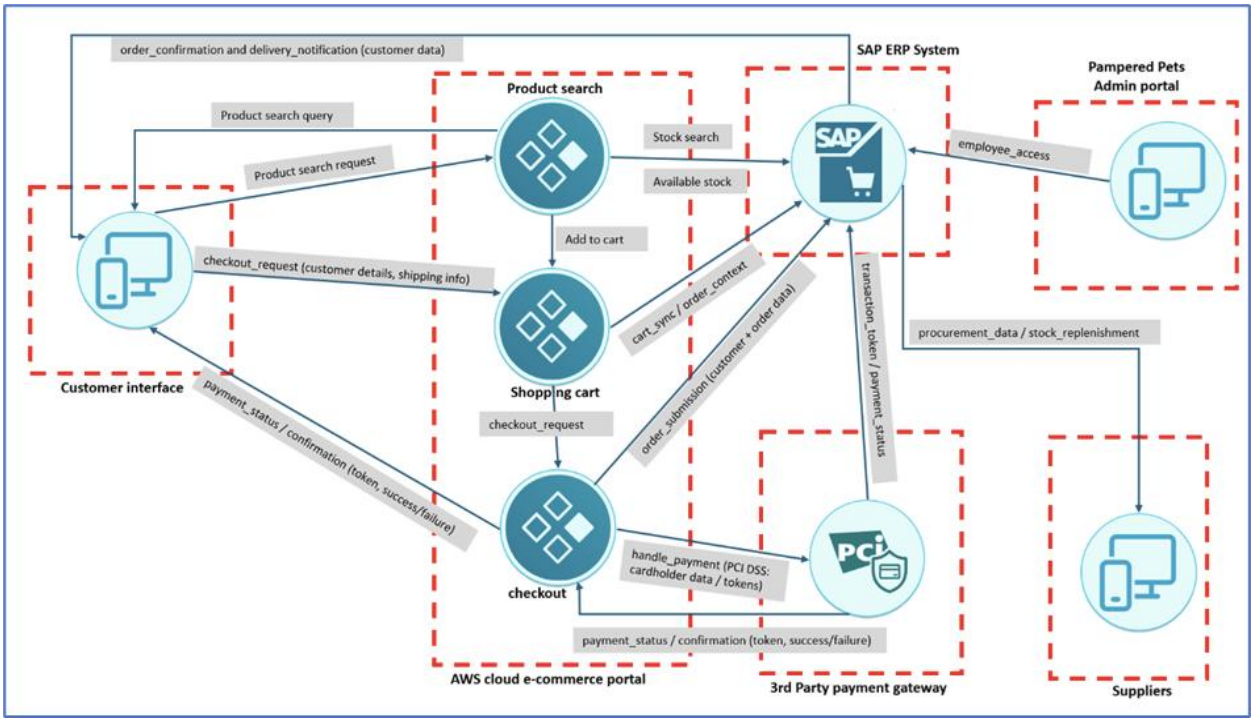


Figure 3-1 - Threat model digitalised e-commerce ecosystem

Table 3-1 defines prioritisation criteria as assessed by the stakeholders.

		Impact score		
Priority	**Impact Area**	**Low (1)**	**Medium (2)**	**High (3)**
4	Customer Trust & Retention	<10% reduction in customers; minor complaints, quickly recoverable	10–30% reduction in customers; reputational damage requiring recovery investment	>30% reduction in customers; permanent loss of trust, long-term brand harm
3	Financial	<2% increase in costs, <€10,000 one-time loss	€10,000–€50,000 losses; partial failure to achieve 24% cost reduction	>€50,000 losses; failure to achieve 50% growth or 24% savings; existential risk
2	Productivity & Operations	Minor disruption (<4 hours), no lasting effect	Moderate disruption (4–24 hours); temporary stock/order issues	Major disruption (>1 day); systemic ERP/e-commerce failure
1	Regulatory / Legal (GDPR & PCI)	Internal compliance issue; warning only	GDPR fines up to €10k; PCI fines up to €5k/month; no compromised cardholder data	GDPR fines up to €20m or 4% turnover; PCI DSS termination, lawsuits, data compromise

Table 3-1 - Impact area prioritisation – risk criteria

Table 3-2 presents the risk register for the digitalisation process. The total risk score is derived by multiplying priority and impact score across all areas.

ID	Critical Asset	Business Process	Threats	Vulnerabilities	Financial	Trust	Regulatory	Productivity	Risk score
R1	Admin Portal - Staff access	ERP admin, reporting	A01 Broken Access, phishing; insider misuse	Weak employee awareness, lack of just culture	H	H	H	H	31
R2	Payment Gateway - Payment Status/Confirmation	Transaction validation	A08 Integrity Failures; replay/tampering of tokens	No nonce/expiry checks, weak signature validation	H	H	H	M	28
R3	SAP ERP - Customer Records DB	Order management, CRM	A02 Cryptographic Failures, A09 Logging Failures; GDPR violation	Weak encryption at rest, insufficient monitoring	H	H	H	M	28
R4	Payment Gateway - Transaction APIs	Payment processing	A07 Auth Failures, A10 SSRF; fraudulent/failed payments	Weak API authentication, poor sanitisation	H	H	H	M	28
R5	SAP ERP Payment Records	Finance reconciliation	A02 Cryptographic Failures; reconciliation errors + PCI penalties	Insecure storage of payment tokens	H	M	H	M	24
R6	Customer Interface - Web/App	Customer shopping, login	A01 Broken Access, A07 Authentication failures; account takeover	Weak MFA, reused passwords	M	H	M	M	22
R7	Customer Interface - Order/Delivery Notifications	Order confirmation, delivery updates	A08 Integrity Failures; spoofed/delayed confirmations	Unsigned notifications, weak integrity checks	M	H	M	M	22
R8	E-commerce Portal - Shopping Cart / Checkout	Online ordering	A03 Injection, A05 Security Misconfig; cart/order manipulation	Insecure input validation, default configs	M	H	M	M	22

(Table 3-2 continued)

ID	Critical Asset	Business Process	Threats	Vulnerabilities	Financial	Trust	Regulatory	Productivity	Risk score
R9	SAP ERP - Stock / Product DB	Procurement, inventory	A01 Broken Access, insider misuse; inventory errors	Poor role-based access, no segregation of duties	M	M	M	H	19
R10	Suppliers - Procurement API	Stock replenishment	A08 Integrity Failures, DoS on supplier API	No integrity check, weak availability controls	M	M	M	H	19

Table 3-2 - OCTAVE-S risk register

3.4 Mitigation approach

Mitigation measures were prioritised using four criteria:

1. **Total risk score** – severity across all identified risk areas.
2. **Strategic drivers** – risks threatening growth (50%), cost reduction (24%), or customer retention (33%) as outlined in paragraph 1.
3. **Regulatory/legal obligations** – GDPR and PCI DSS compliance.
4. **Feasibility of implementation** – preference for measures offering quick, high-impact results (e.g., MFA, encryption, API hardening) over resource-heavy redesigns.

Table 3-3 maps each risk to its recommended mitigation, aligning technical controls and business processes within a coherent digitalisation strategy.

ID	Mitigation Approach	Justification
R1	Mitigate	Highest score (31). Insider misuse + weak awareness training expose ERP to GDPR/PCI breaches. Controls such as MFA, RBAC, and just culture training are critical.
R2	Mitigate	Payment validation tampering (28) risks direct fraud and PCI DSS fines. Strong financial and trust impacts. Implement nonce/expiry checks and signature validation.
R3	Mitigate	Customer Records DB compromise (28) = GDPR violation + customer trust loss. Encryption at rest and enhanced logging are essential controls.
R4	Mitigate	Payment API exploitation (28) risks fraud and PCI DSS non-compliance. Requires stronger API authentication and SSRF protection.
R5	Mitigate	Payment record failures (24) risk PCI penalties and financial errors. Tokenisation and secure storage must be applied.
R6	Mitigate	Customer login weaknesses (22) risk account takeovers and customer churn. Enforce MFA and password hygiene controls.
R7	Mitigate	Delivery notification spoofing (22) undermines customer trust, leading to abandonment. Apply digital signing and integrity controls.
R8	Mitigate	Shopping cart manipulation (22) threatens 50% growth driver. Secure coding practices, input validation, and WAF required.
R9	Defer	Stock/Product DB access risks (19) threaten cost savings (24%) but less critical than customer/payment risks. RBAC improvements may be planned over time.
R10	Accept	Supplier API disruption (19) has limited direct impact on customers. Can be managed contractually with redundancy and SLAs rather than immediate technical investment.

Mitigation approach	Description
Mitigate	indicates risks requiring immediate or near-term controls
Defer	indicates risks that can be addressed in the medium term due to lower priority
Accept'	indicates risks tolerated with monitoring or contractual/operational measures rather than new technical investment

Table 3-3 - Proposed mitigation

This approach is based on assumptions and limitations that keep the assessment transparent and realistic, avoiding overestimation of certainty or underestimation of residual risks. Key assumptions include:

- Vulnerabilities and threats reflect conditions at the time of modelling and may shift as the threat landscape evolves.
- Cloud providers (AWS, SAP, payment gateway) are assumed to meet baseline compliance obligations according to service-level agreements (SLAs).
- Personnel for digitalisation will be scaled gradually, though SME skill shortages remain a challenge (ENISA, 2020).

These considerations highlight the need for a cautious, staged implementation, keeping risk management adaptive to Pampered Pets' evolving digital strategy

4. Recommendation and timeline

Considering the assessment and the assumptions and limitations, we recommend that Pampered Pets proceed with digitalisation, as it is essential for achieving its strategic objectives outlined in the introduction.

Our risk assessment confirms that these goals are achievable, and risks can be managed through the identified mitigations. A phased implementation is needed, as research shows SMEs benefit from staged transformation to minimise disruption and optimise limited resources (Sagala and Őri, 2024). The timeline and sequencing are shown in Figure 3-2.

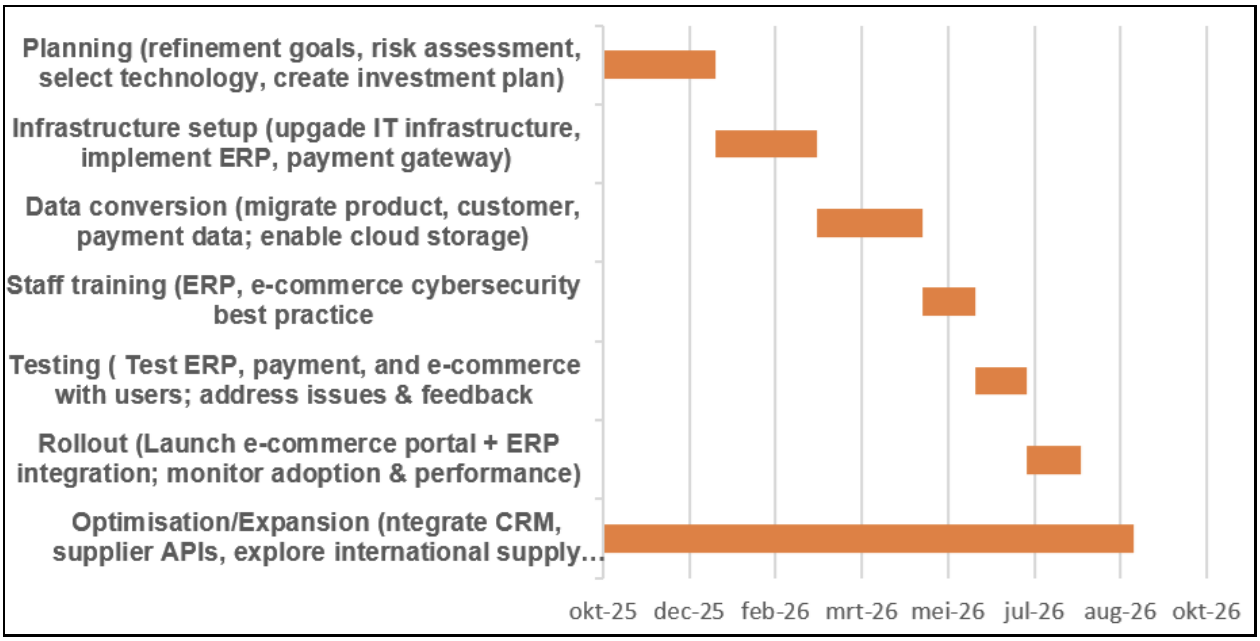


Figure 3-2 - Gantt chart with implementation timeline

By committing to this roadmap, Pampered Pets will not only meet its growth and efficiency targets but also build the trust and adaptability needed for long-term competitiveness in a digital marketplace.

Reference list

Alberts, C. J. and Dorofee, A. J. (2002) *Managing information security risks : the OCTAVE approach*. 1st edition. Boston: Addison-Wesley.

Al-Dosari, K. and Fetais, N. (2023) 'Risk-Management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach', *Electronics*, 12(17), 3629. Available at: https://doi.org/10.3390/electronics12173629 (Accessed 21 August 2025).

Baumgartner, T., Malik, Y. and Padhi, A. (2020) *Reimagining industrial supply chains*, McKinsey & Company, 11 August. Available at: https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/reimagining-industrial-supply-chains (Accessed: 17 August 2025).

Emplifi (2022) *86% of consumers will leave a brand after two poor experiences, study finds*. Available at: https://emplifi.io/press/86-percent-consumers-will-leave-brand-after-two-poor-experiences/ (Accessed: 17 August 2025).

ENISA **(**2021) *Cybersecurity for SMEs – Challenges and Recommendations*. ENISA Publications, June. Available at: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (Accessed: 16 August 2025).

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union, L119, pp. 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 17 August 2025).

Hossain, M.A., Islam, S. and Rahman, M.M. (2024) 'Impact of inline payment systems on customer trust and loyalty in e-commerce analyzing security and convenience', *Academic Journal on Science, Technology, Engineering & Mathematics Education*, 4(3), pp.1–15. Available at: https://doi.org/10.69593/ajsteme.v4i03.85 (Accessed: 16 August 2025).

Kim, C., Tao, W., Shin, N. and Kim, K-S. (2010) 'An empirical study of customers' perceptions of security and trust in e-payment systems', *Electronic Commerce Research and Applications*, 9(1), pp. 84–95. Available at: https://doi.org/10.1016/j.elerap.2009.04.014 (Accessed: 16 August 2025).

KPMG (2015) *Impact of e-commerce on SMEs in India*. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2015/10/Snapdeal-Report_-Impact-of-e-Commerce-on-Indian-SMEs.pdf (Accessed: 16 August 2025).

Majumder, A.S. (2025) 'The influence of UX design on user retention and conversion rates in mobile apps', *arXiv*, January. Available at: https://arxiv.org/abs/2501.13407 (Accessed: 16 August 2025).

PCI Security Standards Council (2018) *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard*. Wakefield, MA: PCI Security Standards Council. Available at: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (Accessed: 17 August 2025).

PwC (2018) *Future of customer experience: 'It's time for a change'*. Available at: https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/future-of-customer-experience.html (Accessed: 17 August 2025).

Sagala, G.H. and Őri, D. (2024) 'Toward SMEs digital transformation success: a systematic literature review', *Information Systems and e-Business Management*, 22, pp. 667–719. Available at: https://doi.org/10.1007/s10257-024-00682-2 (Accessed: 21 August 2025).

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T. and Woody, C. (2018) *Threat modelling: A summary of available methods.* Available at: https://www.sei.cmu.edu/documents/569/2018_019_001_524597.pdf (Accessed 14 August 2025).

Shevchenko, N., Frye, B. and Woody, C. (2018) *'Threat modelling: Evaluation and recommendations.* Available at: https://apps.dtic.mil/sti/pdfs/AD1083907.pdf (Accessed: 14 August 2025).

Shostack, A. (2014) Threat modeling : designing for security. 1st edition. Indianapolis, IN: John Wiley and Sons.