A Risk Assessment Report for Pampered Pets based on IEC27005:2022 / ISO/IEC31000:2018

Module: Security and Risk Management October 2025

By Group 2

Date: November 2025

Table of Content

Introduction

Pampered Pets is a small, high-quality pet food retailer in Washington-on-the-Water. It must decide whether to digitalize its operations. We recommend the company aligns ISO 27005:2022 and ISO 31000:2018 standards. Adopting ISO 27005:2022 and ISO 31000-2018 improves risk management by combining information security with business standards.

Standard	**Focus**	**Scope**	**Justification**
ISO 31000:2018 - Risk Management Guidelines	Generic risk management	Any type of organization, any type of risk.	Providing a standard process for managing risk.
ISO 27005:2022 - Information Security, Cyber Risk, Privacy Protection	Information security risk management	Specifically for information security with a focus on the CIA triad.	Providing a standard process for managing information risk, alignment with ISO27001.
Conclusion	Integrating ISO 27005:2022 with ISO 31000:2018 ensures coherence.		

Table 1: ISO 27005:2022 and ISO 31000-2018 (Status Quo).

The Risk Management Cycle

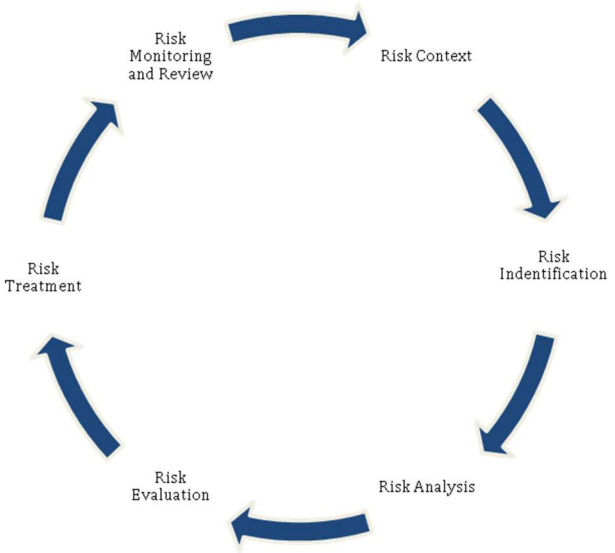

Figure 3: The Risk Management Cycle (ISO).

Risk Assessment Business (Status Quo)

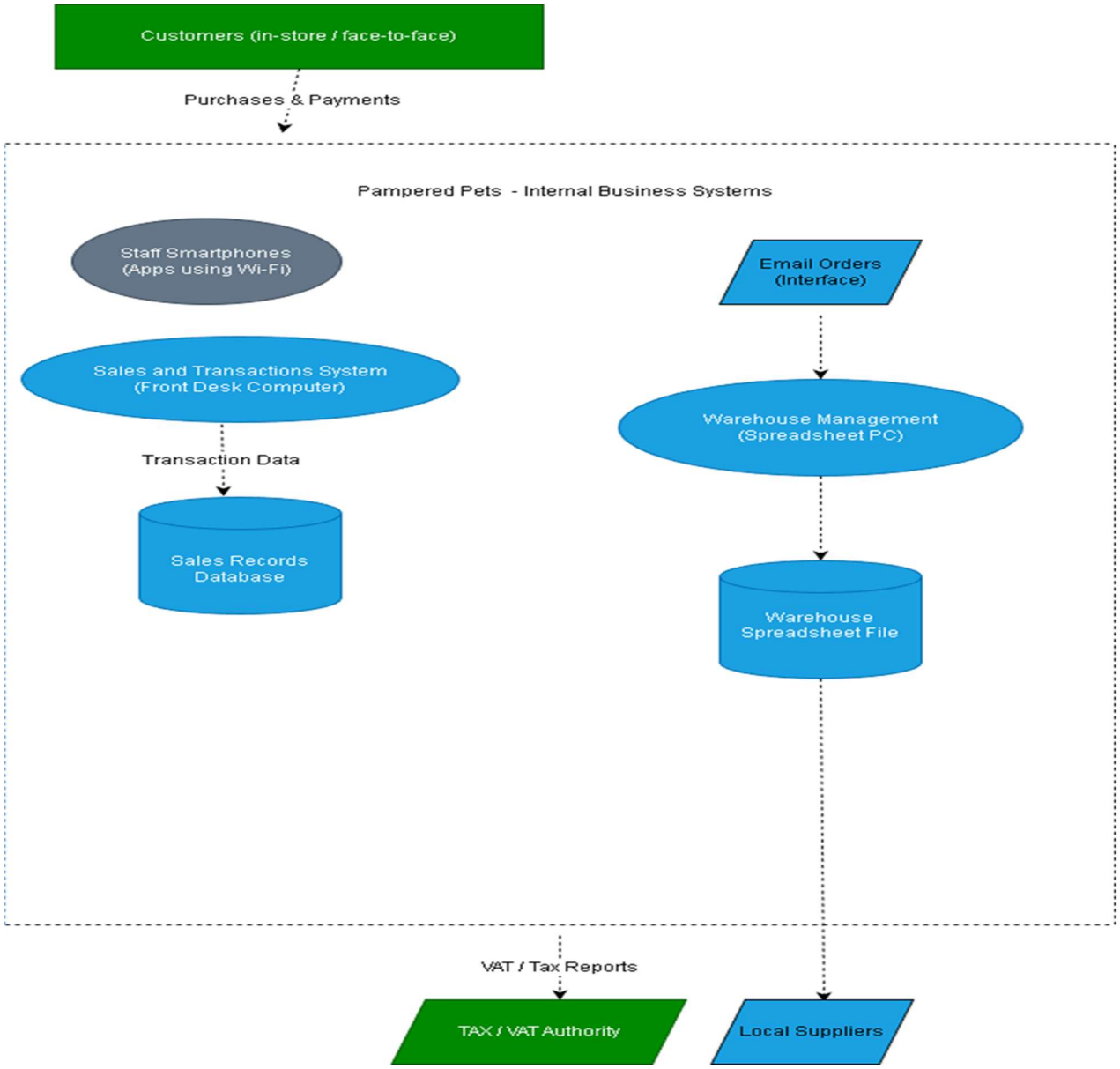

Figure 1: Data flow diagram of Pampered Pets (author-generated, 2025).

Context

- 90% of business is in-store and the company's data is being stored on two local computers.
- PCs in warehouses and front desk handle deliveries/sales.
- Basic hub with Wi-Fi access points connected to systems.
- No cybersecurity measures.
- Staff use personal smartphones on Wi-Fi.
- No online/external databases.
- Rely on local suppliers for ingredients.

Threat	Likelihood	Impact	Risk Level	Notes	CIA Aspect
Cybersecurity threats	Medium	High	Critical	Technology has a limited footprint and imposes some risks.	C, I
Human error	High	Medium	High	No audit trails.	I, A
Data loss or corruption	High	Medium	High	No backup policy redundancy.	A, I
Insider threat / data breach	Medium	Medium	Moderate	Small team, poor access control.	C, I
Supply chain disruption	Medium	Low	Moderate	Local suppliers' dependencies are high.	A
Physical theft or damage	Medium	Medium	Moderate	Limited physical security controls.	A, C
Regulatory non-compliance	Low	Medium	High	Basic compliance, but poor data measures.	C, I

Table 2: Qualitative Risk Assessment

Note: Each threat was evaluated based on likelihood of impact on CIA triad:

C (confidentiality) - **I** (integrity) - **A** (availability).

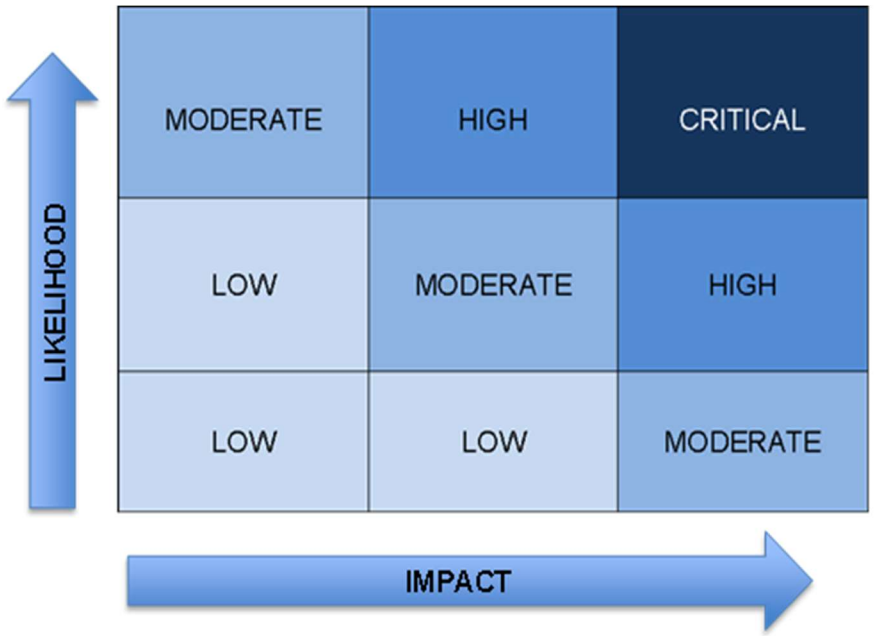

Figure 2: Risk matrix used in the Pampered Pets risk assessment (author-generated, 2025).

Although useful for illustration, qualitative risk matrices can introduce subjective bias and oversimplify uncertainty (Hubbard 2020, Ch. 1; Thekdi and Aven 2025).

- This report does not consider quantitative metrics as there is no monetary value indicated.

Key Risk Consequences

- Supply chain disruption or quality issues caused by reliance on one supplier.
- Loss of control over assets.
- Threat to services due to operational issues.
- Competitive threats from digital-first rivals.
- Data loss.
- Financial loss due to downtime or tax data corruption.

- Failure to adhere to laws and regulations.
- Loss of customer trust due to data leaks.

Mitigation Measures

- Manage tangible and intangible assets.
- Improve supply chain practices.
- Improve data protection and recovery practices.
- Improve network resilience, segmentation, and availability.
- Implement staff cybersecurity training and basic access controls.
- Adopt basic endpoint protection.
- Maintain digital presence and practices.

Risk Assessment Methodology (Digitalization)

Chosen Standards: ISO/IEC 27005:2022 and ISO/IEC 31000

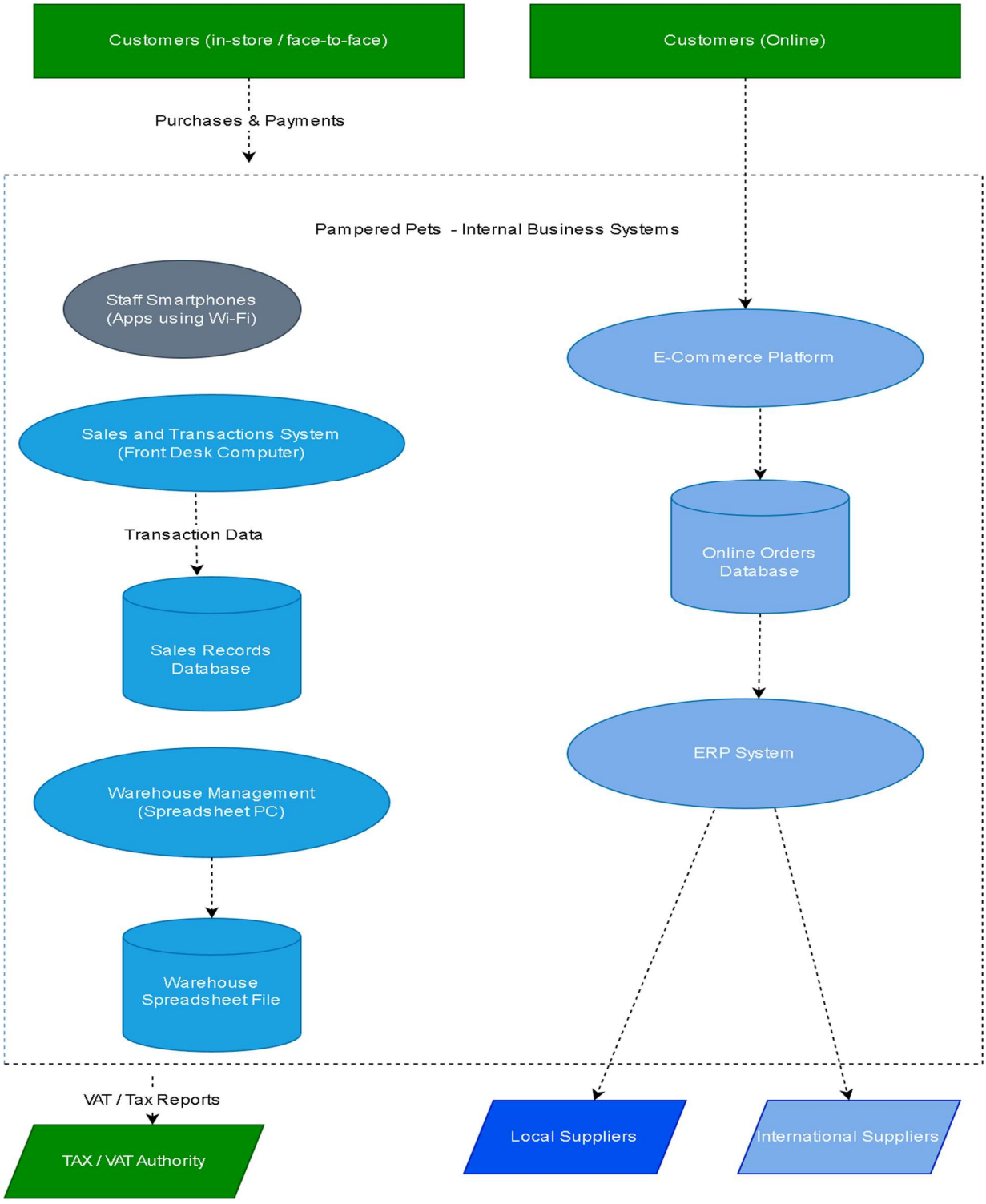

Figure 4: Digitalized Business Data Flow Model (author-generated, 2025).

Strategic Threats and Opportunities

A. **Evidence:**

- Wider regional reach
- Ability to sell online
- Attract younger customers

Risks:

- Cybersecurity
- Digital marketing investment
- Competition
- High opportunity, medium implementation risk

Recommendation:

- A website can increase online presence by 30% (up to 50%) (Sharma, 2024)

B. **Evidence:**

- Lower ingredients or packaging costs, bulk imports.

- **Risks:**

  - Loss of quality control
  - Customs, tariffs, logistics and exchange-rate volatility
  - Ethical and sustainable sourcing
  - Cyber risks from vendor systems
  - Moderate savings, high strategic / reputational risks.

- **Recommendation:**

  - Cost savings of up to 25%, due to efficiency improvements in supply chain management. (Van Hoek et al. 1999)

C. **Evidence:**

- Online shopping is convenient. (Yell Business, 2020).

- **Risks:**

  - Losing younger demographics and market share to online rivals (Amazon, Homebase).

- Moderate investments, but high strategic potential.

- **Recommendation**:

  - Adopt online features, prevent customer loss, and avoid slower growth (Afnic, 2021).

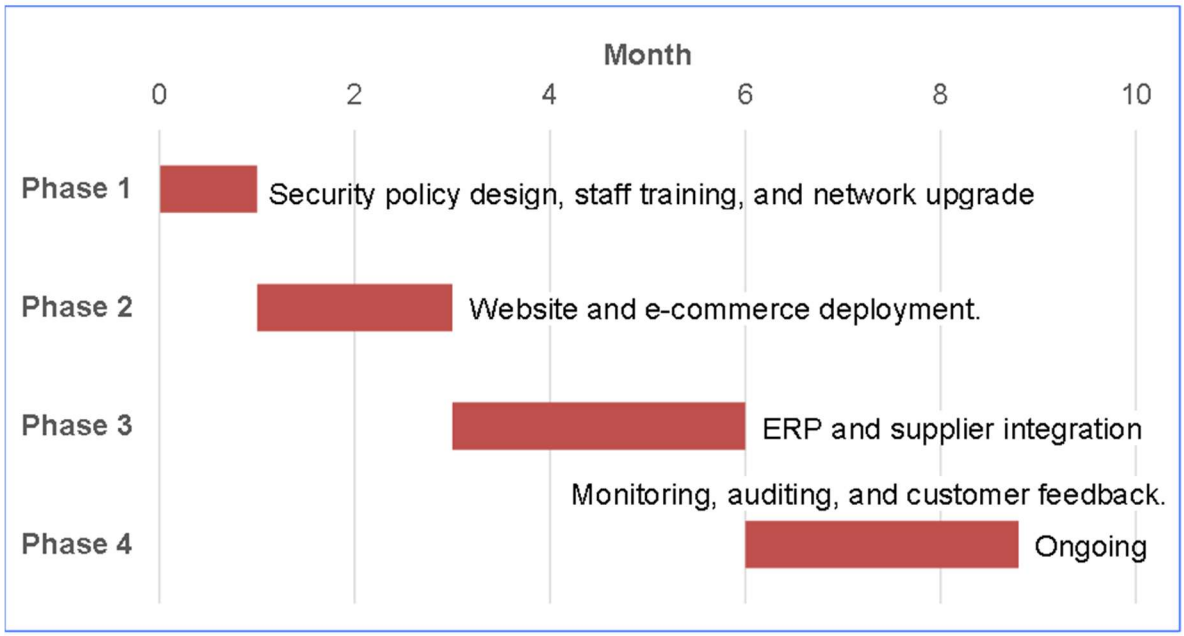

Figure 5: Recommendations A list of proposed changes

Scenario	Advantages	Key Risks	Overall Risk Post-Mitigation
Status Quo	Low cost, familiar systems, trusted local supply	Data loss, customer loss and scalability issues.	High (Unacceptable)
Digitalization	Scalability, efficiency, revenue, competitiveness	Cyber threats, data privacy, and complexity.	Medium (can be reduced)

Table 3: General risks and threats

Threat	Likelihood	Impact	Risk Level	Notes / Mitigation
Cybersecurity threats	High	High	Critical	E-commerce introduces public exposure.
Data breaches	Medium	High	High	Requires privacy protection measures.
Implementation cost overrun	Medium	Medium	Moderate	Project management phased rollout.

Table 4: Threat and Risk Modelling (Digitalization)

Category	Threat Example	Assets Affected	Potential Impact	Likelihood	Overall Risk
S – Spoofing	Phishing emails	Email, invoices, supplier trust	Monetary loss, reputational	Medium	High
T – Tampering	Malware or unauthorized modification	computer, warehouse spreadsheets	Tax/VAT errors, stock inaccuracies	Medium	High
R – Repudiation	No email order audit trail.	Email systems, manual logs	Financial, data inconsistency	Low	Medium
I – Information Disclosure	Customer, supplier data leaked	Customer, supplier data	breach, fines, reputational	Medium	High
D – Denial of Service	Network outage (Hub failure)	order management	Lost sales, operational downtime	High	Medium

Table 5: Threat and Risk Modelling STRIDE (Digitalization)

- The STRIDE model was selected because it is simpler than DREAD and PASTA.

  A more rigorous asset scoping process was deemed necessary for threat modelling.

  (Jbair et al. 2022; Shevchenko et al. 2018; Meier et al. 2006).

Potential Mitigation Strategies

- Establish a foundation for strategy, risk, information security, data, privacy, business continuity planning (BCP) and compliance.
- Ensure that digitalization aligns with regulations and Laws.
- Get cyber insurance.
- Partner with cloud providers.
- Aim for Level 2 CMMI maturity and focus on quick wins to avoid overspending.
- Implement low-hanging fruit, for instance, longer passwords, WPA3, or other measures.

Conclusion

Pampered Pets can grow and evolve through digitalization. By expanding its online presence, the business could boost sales by up to 50%, optimize its supply chain and reduce costs by around 24%, and prevent a potential loss of 33% of its existing customer base. Guided by the ISO 27005 and ISO 31000 standards, digital transformation can provide a structured and secure foundation for improved efficiency, resilience, and long-term competitiveness. However, successful implementation will depend on effective risk management and mitigation strategies to address the associated cyber and operational risks.

References

- Afnic (2021) Results of Afnic's "*Succeed with the Web*" Study on the Online Presence of VSE/SMEs. Available at: https://www.afnic.fr/en/observatory-and-resources/news/results-of-afnics-succeed-with-the-web-study-on-the-online-presence-of-vse-sme/ [Accessed November 5, 2025]
- Barafort, B., Mesquida, A.-L. and Mas, A. (2019) ISO 31000-based integrated risk man2019) process assessment model for IT organizations', *Journal of Software: Evolution and Process*, 31(1), Article e1984. DOI: 10.1002/smr.1984
- Hubbard, D.W. (2020) *The Failure of Risk Management: Why It's Broken and How to Fix It***.** 1st edn. Wiley and Sons.
- Jbair, M., Ahmad, B., Maple, C. and Harrison, R. (2022) 'Threat modelling for industrial cyber physical systems in the era of smart manufacturing', *Computers in Industry*, 137, p. 103611. doi: 10.1016/j.compind.2022.103611.
- Meier, J.D. (2006) 'Web application security engineering', *IEEE Security & Privacy*, 4(4), pp. 16–24.
- Sharma, K., (2024). Building a Strong Online Presence for Strengthening Entrepreneurship. Available at SSRN 4925930. Available at: https://dx.doi.org/10.2139/ssrn.4925930 [Accessed November 16, 2025]
- Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P. and Woody, C. (2018) *Threat Modeling: A Summary of Available Methods*. Carnegie Mellon University Software Engineering Institute.

- Thekdi, S. and Aven, T. (2025) ‘Evaluating risk analyst views on uncertainty and knowledge aspects for risk characterization approaches’, *Journal of Risk Research*, 28(8), pp. 912–928.
- Van Hoek, R.I., Vos, B. and Commandeur, H.R., (1999). Restructuring European supply chains by implementing postponement strategies. *Long Range Planning*, *32*(5), pp.505-518. Available at: https://doi.org/10.1016/S0024-6301(99)00071-0 [Accessed November 19, 2025]
- Yell Business (2020) The Business Impact of a Strong Online Presence. Yell Business SME Insight. Available at: https://business.yell.com/sme-insight/cant-see-the-web-for-the-trees/the-business-impact-of-a-strong-online-presence/ [Accessed November 5, 2025]