Pampered Pets is a small bricks-and-mortar enterprise considering undergoing a digital transformation. This report will provide an overview of the current state of the enterprise as well as offer a path for the digitalisation and a preliminary evaluation of the risks for a digital enterprise.

Assessment methodology

Both assessments follow the OCTAVE Allegro methodology (hereafter 'Allegro') to allow for quicker evaluation as well as comparison of the results.

Other frameworks like ISO or NIST are more suitable for mature organisations (Wangen, Hallstensen and Snekkenes, 2018; Tewari, 2022; Violino, 2024; Secureframe, no date), while Allegro is specifically designed for small and medium-sized enterprises (SMEs) yet still allows for diverse analysis of the risks and quantitative assessment (Caralli *et al.*, 2007).

Risks in the current state

The enterprise relies on IT for warehouse and financial records. Customers' personally identifiable information (PII) appears in emails and in sales records.

Common scenarios that lead to the adverse outcomes (disclosure, modification, interruption, destruction) are:

1. Unauthorised access,
2. Employee error or sabotage,
3. Malware,
4. Software or hardware defects.

The business processes may also be interrupted if a key employee is unavailable for work, in case of power outages and natural or local disasters.

Absolute impact is limited by the small customer base, though data disclosure can result in fines under the GDPR ("Regulation (EU) 2016/679 of the European

Parliament and of the Council (General Data Protection Regulation),” 2016; Information Commissioner’s Office, 2024).

Recommended mitigations:

- Regular backups; consider cloud storage.
- Physical and digital access controls (strong passwords, restricted areas.
- Antivirus software.
- Secure network configuration.
- Staff awareness, NDAs.
- Process documentation.

Digitalisation: discussion and recommendations

With platforms like Amazon expanding, digitalisation is essential for customer retention and business survival (Solon and Wong, 2018; Vollero, Sardanelli and Siano, 2023). Online presence directly correlates with SME competitiveness, as demonstrated on the Figure 1 (Lányi, Hornyák and Kruzslicz, 2021), helping retain and attract customers.

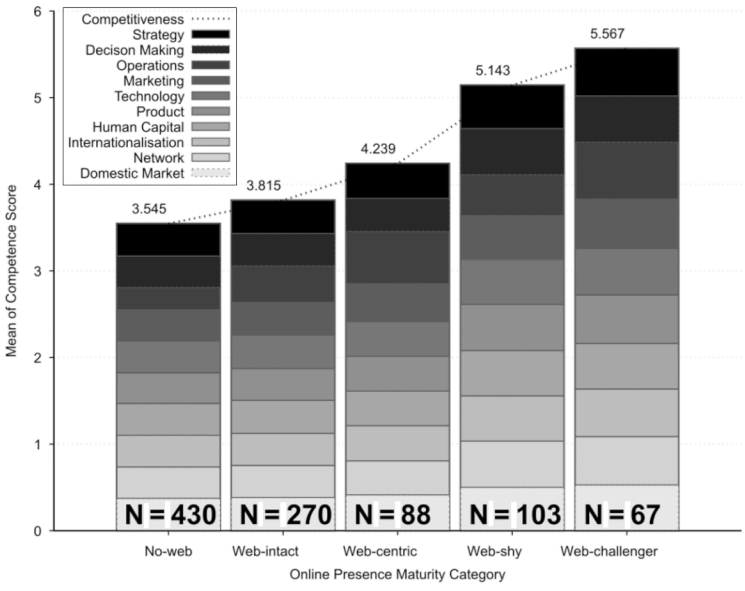

Figure 1. Impact of online presence on enterprise competitiveness (Lányi, Hornyák and Kruzslicz, 2021)

Local supply chains are preferable despite more competitive prices on agricultural produce in other countries (Eurostat, 2025): global supply adds disruption risk and opacity, and is more difficult to manage (Baldwin and Freeman, 2022). Local sourcing strengthens the business image and customer loyalty (Dragonsourcing, 2024; Tendencia, 2025; Torg, 2025).

The plan below suggests a staged rollout of digital services which avoids abrupt changes in processes and spreads costs. If needed, the process may be sped up by shortening phase 2 and merging phases 3 and 4.

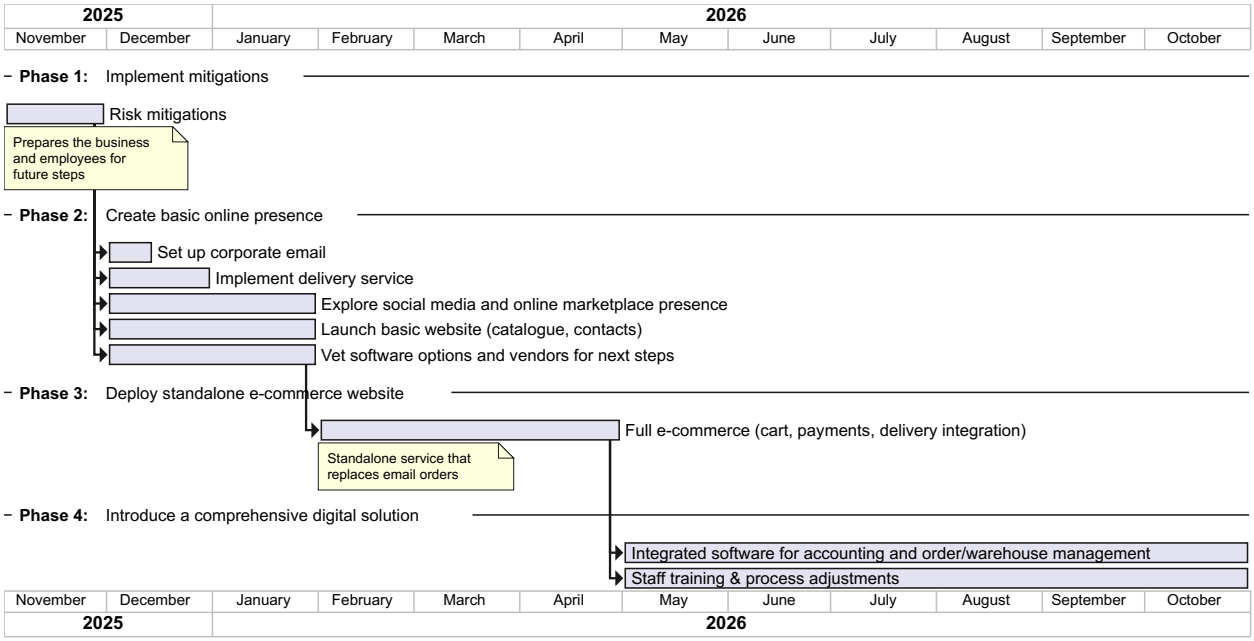

Figure 2. Pampered Pets' digital transformation

The stages 1 and 2 may be accomplished by the existing staff or freelancers. For the stages 3 and 4, it is advisable to contract a vendor that will implement and support the new cloud systems, as well ensure their security and provide training for staff.

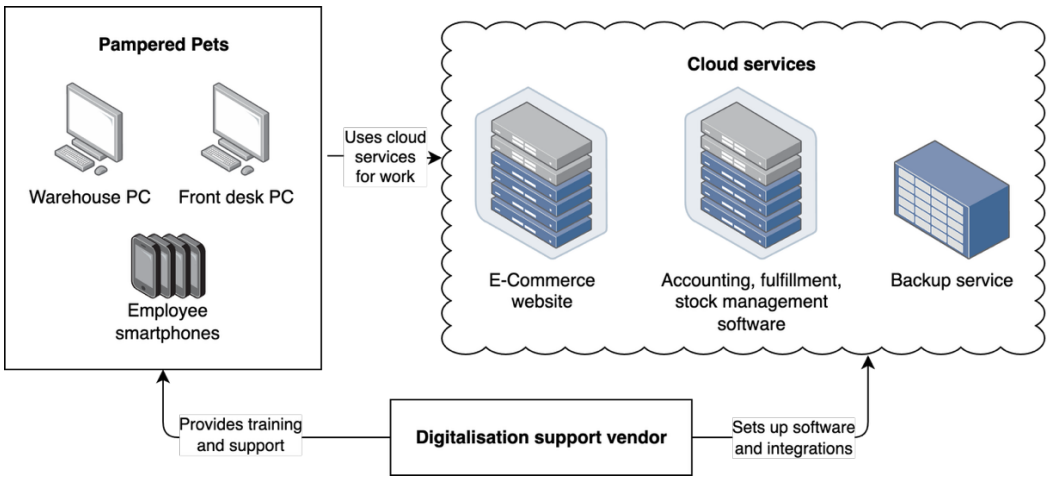

Figure 3. Pampered Pets after digitalisation

Risks after digitalization

Risks broaden and have higher impact due to the higher number of customers. Data disclosure is more severe and has higher impact on reputation and finances. Some of the risks are caused by dependencies on external vendors.

Common scenarios that lead to adverse outcomes (disclosure, modification, interruption, destruction) are:

1. Employee error or sabotage,
2. Account compromise,
3. Authorisation misconfiguration,
4. Online service compromise or defect.

Power supply, network, and cloud provider outages interrupt business operations. Impact of natural or local disasters is lower, as the data is stored remotely.

Recommended mitigations:

- Vetting vendors:

    - Certifications (GDPR compliance, PCI DSS, ISO 27000) (Disterer, 2013; Fruhlinger, 2024; PCI Security Standards Council, LLC., 2024),
    - DDoS protection and service resilience,
    - Backup policies.
- Access controls:
    - Password policies,
    - Role-based permissions.
- Train staff on new systems.
- Backup power sources and alternate network connections.

Conclusion & Recommendations

Despite new high-impact risks, digitalisation is recommended. A staged approach enables stability and staff adaptation while supporting growth and retention. It also lays the foundation for future expansion: online services extend reach, and digital processes enable smoother scaling.

References

Baldwin, R. and Freeman, R. (2022) “Risks and Global Supply Chains: What We Know and What We Need to Know,” *Annual Review of Economics*, 14(Volume 14, 2022), pp. 153–180. Available at: https://doi.org/10.1146/annurev-economics-051420-113737.

Caralli, R.A. *et al.* (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process:* Fort Belvoir, VA: Defense Technical Information Center. Available at: https://doi.org/10.21236/ADA470450.

Disterer, G. (2013) “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” 2013. Available at: https://doi.org/10.4236/jis.2013.42011.

Dragonsourcing (2024) “Why Local Sourcing Is Good for Business & the Environment,” 9 June. Available at: https://www.dragonsourcing.com/the-benefits-of-going-local-why-sourcing-locally-is-good-for-business-and-the-environment/ (Accessed: September 28, 2025).

Eurostat (2025) “Selling prices of soft wheat.” Eurostat. Available at: https://doi.org/10.2908/TAG00059.

Fruhlinger, J. (2024) “PCI DSS defined: Requirements, fines, and steps to compliance,” *CSO Online*, 3 April. Available at: https://www.csoonline.com/article/569591/pci-dss-explained-requirements-fines-and-steps-to-compliance.html (Accessed: August 15, 2025).

Information Commissioner’s Office (2024) *Penalties*. ICO. Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/ (Accessed: August 15, 2025).

Lányi, B., Hornyák, M. and Kruzslicz, F. (2021) “The effect of online activity on SMEs’ competitiveness,” *Competitiveness Review*, 31(3), pp. 477–496. Available at: https://doi.org/10.1108/CR-01-2020-0022.

PCI Security Standards Council, LLC. (2024) “Payment Card Industry Data Security Standard.” Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf (Accessed: August 15, 2025).

“Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)” (2016). Official Journal of the European Union. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: January 19, 2025).

Secureframe (no date) *ISO 27001 vs NIST CSF*, *Secureframe*. Available at: https://secureframe.com/hub/iso-27001/vs-nist (Accessed: September 25, 2025).

Solon, O. and Wong, J.C. (2018) “Jeff Bezos v the world: why all companies fear ‘death by Amazon,’” *The Guardian*, 24 April. Available at: https://www.theguardian.com/technology/2018/apr/24/amazon-jeff-bezos-customer-data-industries (Accessed: September 28, 2025).

Tendencia, R. (2025) *Local vs Global Sourcing: Choosing the Right Strategy for Your Business*. Available at: https://www.csvnow.com/blog/local-sourcing-vs-global-sourcing (Accessed: September 28, 2025).

Tewari, A. (2022) “Comparison between ISO 27005, OCTAVE & NIST SP 800-30 | SISA Blog,” *SISA*, 8 January. Available at: https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30-sisa-blog/ (Accessed: September 28, 2025).

Torg (2025) *Local Sourcing: Why Businesses Are Making the Switch*, *Torg*. Available at: https://usetorg.com/blog/local-sourcing (Accessed: September 28, 2025).

Violino, B. (2024) “6 IT risk assessment frameworks compared,” *CSO Online*, 9 August. Available at: https://www.csoonline.com/article/525128/it-risk-assessment-frameworks-real-world-experience.html (Accessed: September 28, 2025).

Vollero, A., Sardanelli, D. and Siano, A. (2023) “Exploring the role of the Amazon effect on customer expectations: An analysis of user-generated content in consumer electronics retailing,” *Journal of Consumer Behaviour*, 22(5), pp. 1062–1073. Available at: https://doi.org/10.1002/cb.1969.

Wangen, G., Hallstensen, C. and Snekkenes, E. (2018) “A framework for estimating information security risk assessment method completeness,” *International Journal of Information Security*, 17(6), pp. 681–699. Available at: https://doi.org/10.1007/s10207-017-0382-0.

Appendix 1 — OCTAVE Allegro worksheets for evaluation

Risk Measurement Criteria – Reputation and Customer Confidence

Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than 5% reduction in customers due to loss of confidence	5 to 15% reduction in customers due to loss of confidence	More than 15% reduction in customers due to loss of confidence
Other:			

Risk Measurement Criteria — Financial

Impact Area	Low	Moderate	High
Operating Costs	Increase of less than 5% in yearly operating costs	Yearly operating costs increase by 5 to 15%	Yearly operating costs increase by more than 15%
Revenue Loss	Less than 5% yearly revenue loss	5 to 15% yearly revenue loss	Greater than 15% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $5000	One-time financial cost of $5000 to $15000	One-time financial cost greater than $15000
Other:			

Risk Measurement Criteria — Productivity

Impact Area	Low	Moderate	High
Staff Hours	Staff work hours are increased by less than 10% up to 5 days.	Staff work hours are increased between 10% and 25% or up to 8 days.	Staff work hours are increased by greater than 25% or for 8 or more days.
Other: Production downtime	Production halted for up to 2 days.	Production halted for 2 to 4 days.	Production halted for more than 4 days.
Other:			
Other:			

Risk Measurement Criteria — Safety and Health

Impact Area	Low	Moderate	High
Life	No loss or significant threat to customers', their pets', or staff members' lives	Customers', their pets', or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers', their pets', or staff members' lives
Health	Minimal, immediately treatable degradation in customers', their pets', or staff members' health with recovery within four days	Temporary or recoverable impairment of customers', their pets', or staff members' health	Permanent impairment of significant aspects of customers', their pets', or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

Risk Measurement Criteria — Fines and Legal Penalties

Impact Area	Low	Moderate	High
Fines	Fines less than 1% of annual revenue are levied.	Fines between 1 and 5% of annual income are levied.	Fines greater than 5 % of annual revenue are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than 1% of annual revenue are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between 1 and 5% of annual revenue are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than 5% of annual revenue are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records.	Government or other investigative organization initiates an investigation into organizational practices.
Other:			

Impact Area Prioritization

Priority	Impact Areas
1	*Reputation and Customer Confidence*
3	*Financial*
2	*Productivity*
5	*Safety and Health*
4	*Fines and Legal Penalties*
	User Defined

Critical Information Asset Profile Example

(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Warehouse records.	Modification or corruption of the data can lead to issues concerning safety (expired ingredients), productivity (need to locate or re-acquire ingredients), and finances.	Data about warehouse deliveries and items' locations.
(4) Owner(s) *Who owns this information asset?*		
Alice (business owner), Harry (warehouse manager)		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Competition can use this data to outbid the business or impact the supply chain otherwise.
Integrity	Only authorized personnel can modify this information asset, as follows:	Only the warehouse manager or stand-in employee may modify the data.
Availability	This asset must be available for these personnel to do their jobs, as follows:	Only shop employees may access the data.
	This asset must be available for 8 hours, 5 days/week, 52 weeks/year.	The data needs to be available during business hours.
~~**Other**~~	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
Availability		

Information Asset Risk Environment Map (Technical)

Internal		
#	**Container Description**	**Owner(s)**
1	**Warehouse computer** stores data about warehouse stock	Harry (warehouse mgr)
2	**Front desk computer** stores financial records (sales and purchases), as well as accesses organization's emails	Cathy (store manager)
3	All devices in the shop are connected to the **shop network**	Alice (business owner)
4		
External		
#	**Container Description**	**Owner(s)**
1	**Mail server** is used for communication with customers	Unknown, an email provider
2		
3		
4		

Information Asset Risk Environment Map (People)

Internal Personnel		
#	**Name or Role/Responsibility**	**Department or Unit**
1	**Harry (warehouse manager)** knows suppliers' details as well as the organization of the stock	
2	**Cathy (store manager)** works with the customers and knows details of their orders	
3	**Andrea (assistant)** has similar experience	
4		
External Personnel		
#	**Contractor, Vendor, etc.**	**Department or Unit**
1		
2		
3		
4		

Information Asset Risk Example

Information asset risk

Threat

Information Asset	Warehouse records
Area of Concern	An employee can accidentally modify the warehouse records.
(1) Actor *Who would exploit the area of concern or threat?*	Any employee with access to the warehouse computer (all employees).
(2) Means *How would the actor do it? What would they do?*	The spreadsheet may be overwritten with incorrect data, thus preventing the intended use of the data.
(3) Motive *What is the actor's reason for doing it?*	Mistake
(4) Outcome *What would be the resulting effect on the information asset?*	
(5) Security Requirements *How would the information asset's security requirements be breached?*	The information is required for the normal operation of the business, and its modification may result in halting some of the operations or need to verify stocks.
(6) Probability *What is the likelihood that this threat scenario could occur?*	

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Normal business processes are interrupted, employees need to spend time on verifying and restoring the data integrity.	Reputation & Customer Confidence	Low	1
	Financial	Low	3
	Productivity	Med	4
	Safety & Health	Low	5
	Fines & Legal Penalties	Low	4
	User Defined Impact Area		
		Relative Risk Score	17

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
~~Accept~~	**~~Defer~~**	**Mitigate**	**~~Transfer~~**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Warehouse computer	The spreadsheet file may be backed up regularly (e.g. daily) to allow for quick recovery		

Appendix B — Summary risk assessment tables

Original before digitalisation

Asset	Scenario	Actor	Outcome	Probability	Reputation	Financial	Productivity	Safety	Fines	Score
Financial Records	Unauthorized access (competitor)	Competitor	Disclosure	Low	2	2	2	1	3	29
Financial Records	Unauthorized access (visitor)	Visitor	Disclosure	Medium	2	2	2	1	3	29
Financial Records	Accidental destruction (delete/corrupt file)	Employee	Destruction	Medium	1	2	2	1	3	28
Financial Records	Deliberate destruction	Employee	Destruction	Low	1	2	2	1	3	28
Financial Records	Natural/man-made disaster	Event	Destruction	Low	1	2	2	1	3	28
Financial Records	Accidental interruption (file inaccessible)	Employee	Interruption	Medium	1	2	2	1	3	28
Financial Records	Deliberate interruption (deny access)	Employee	Interruption	Low	1	2	2	1	3	28
Financial Records	Accidental modification (data entry error)	Employee	Modification	Medium	1	2	2	1	3	28
Financial Records	Deliberate modification	Employee	Modification	Low	1	2	2	1	3	28
Financial Records	Hardware defect	Technical	Interruption/Destruction	Low	1	2	2	1	3	28
Financial Records	Power outage	External	Interruption/Destruction	Low	1	2	2	1	3	28
Financial Records	Malicious code (virus, Trojan)	External	Disclosure/Modification/Interruption/Destruction	Medium	1	2	2	1	3	28
Financial Records	Software defect / system crash	Technical	Interruption/Disclosure/Destruction	Low	1	2	2	1	3	28
Email Orders	Unauthorized access (competitor)	Competitor	Disclosure	Low	2	2	1	1	3	27
Email Orders	Unauthorized access (visitor)	Visitor	Disclosure	Medium	2	2	1	1	3	27
Email Orders	Malicious code (phishing/malware)	External	Disclosure/Modification/Interruption/Destruction	Medium	2	2	1	1	3	27
Email Orders	Third-party email provider incident (breach/major outage)	External	Disclosure/Destruction	Low	2	2	1	1	3	27
Financial Records	Accidental disclosure (mis-sent/cc error)	Employee	Disclosure	Low	1	2	1	1	3	26
Financial Records	Deliberate disclosure (insider leak)	Employee	Disclosure	Low	1	2	1	1	3	26
Email Orders	Accidental disclosure (forwarding/cc error)	Employee	Disclosure	Low	1	1	1	1	3	23

Email Orders	Deliberate disclosure (insider leak)	Employee	Disclosure	Low	1	1	1	1	3	23
Email Orders	Accidental destruction (delete emails)	Employee	Destruction	Medium	1	2	2	1	1	20
Email Orders	Deliberate destruction	Employee	Destruction	Low	1	2	2	1	1	20
Warehouse Records	Accidental destruction (delete/corrupt file)	Employee	Destruction	Medium	1	1	2	1	1	17
Warehouse Records	Accidental destruction (visitor)	Visitor	Destruction	Medium	1	1	2	1	1	17
Warehouse Records	Deliberate destruction	Employee	Destruction	Low	1	1	2	1	1	17
Warehouse Records	Deliberate destruction (competitor)	Competitor	Destruction	Low	1	1	2	1	1	17
Warehouse Records	Natural/man-made disaster (fire, flood)	Event	Destruction	Low	1	1	2	1	1	17
Email Orders	Deliberate interruption (lockout)	Employee	Interruption	Low	1	1	2	1	1	17
Warehouse Records	Accidental interruption (misplaced file)	Employee	Interruption	Medium	1	1	2	1	1	17
Warehouse Records	Accidental interruption (visitor)	Visitor	Interruption	Medium	1	1	2	1	1	17
Warehouse Records	Deliberate interruption (competitor)	Competitor	Interruption	Low	1	1	2	1	1	17
Warehouse Records	Deliberate interruption (deny access)	Employee	Interruption	Medium	1	1	2	1	1	17
Warehouse Records	Accidental modification (overwrite)	Employee	Modification	Medium	1	1	2	1	1	17
Warehouse Records	Accidental modification (visitor)	Visitor	Modification	Medium	1	1	2	1	1	17
Warehouse Records	Deliberate modification	Employee	Modification	Low	1	1	2	1	1	17
Warehouse Records	Deliberate modification (competitor)	Competitor	Modification	Low	1	1	2	1	1	17
Warehouse Records	Hardware defect	Technical	Interruption/Destruction	Low	1	1	2	1	1	17
Warehouse Records	Power outage	External	Interruption/Destruction	Low	1	1	2	1	1	17
Warehouse Records	Malicious code (virus, Trojan)	External	Disclosure/Modification/Interruption/Destruction	Medium	1	1	2	1	1	17
Warehouse Records	Software defect / system crash	Technical	Interruption/Disclosure/Destruction	Low	1	1	2	1	1	17
Warehouse Records	Accidental disclosure (mis-sent/cc error)	Employee	Disclosure	Low	1	1	1	1	1	15
Warehouse Records	Deliberate disclosure (insider leak)	Employee	Disclosure	Low	1	1	1	1	1	15
Warehouse Records	Unauthorized access (competitor)	Competitor	Disclosure	Low	1	1	1	1	1	15
Warehouse Records	Unauthorized access (visitor, accidental)	Visitor	Disclosure	Medium	1	1	1	1	1	15
Email Orders	Accidental interruption (lost password)	Employee	Interruption	Low	1	1	1	1	1	15
Email Orders	Natural/man-made disaster (affecting shop → access)	Event	Interruption	Low	1	1	1	1	1	15

Email Orders	Telecom outage	External	Interruption	Low	1	1	1	1	1	15
Email Orders	Software defect / system crash (client PC)	Technical	Interruption/Destruction	Low	1	1	1	1	1	15

Organization after digitalisation

Asset	Scenario	Actor	Outcome	Probability	Reputation	Financial	Productivity	Safety	Fines	Score
Corporate Email Data	Outsider hacking	Outsider	Disclosure	Medium	3	3	2	1	3	33
Customer Accounts	Outsider deliberate disclosure (account breach)	Outsider	Disclosure	Medium	3	3	2	1	3	33
E-Commerce Store Data	Outsider disclosure (web breach)	Outsider	Disclosure	Medium	3	3	2	1	3	33
Financial Records	Outsider disclosure (hacking)	Outsider	Disclosure	Medium	3	3	2	1	3	33
Order & Inventory Records	Deliberate disclosure (hacking, brute force)	Outsider	Disclosure	Medium	3	3	2	1	3	33
Backup Data	Disclosure of backups	System	Disclosure	Low	3	3	1	1	3	31
Order & Inventory Records	Accidental disclosure (unprotected endpoint)	Outsider	Disclosure	Low	3	3	1	1	3	31
Corporate Email Data	Malware	System	Disclosure/Modification/Interruption/Destruction	Medium	2	2	2	1	3	29
Financial Records	Malware	System	Disclosure/Modification/Interruption/Destruction	Medium	2	2	2	1	3	29
Customer Accounts	Outsider modification (account tampering)	Outsider	Modification	Medium	2	2	2	1	3	29
Financial Records	Employee accidental modification	Employee	Modification	Medium	1	2	2	1	3	28
Financial Records	Employee deliberate modification	Employee	Modification	Low	1	2	2	1	3	28
Corporate Email Data	Employee accidental disclosure	Employee	Disclosure	Low	2	2	1	1	3	27
Customer Accounts	Employee accidental disclosure	Employee	Disclosure	Low	2	2	1	1	3	27
E-Commerce Store Data	Employee accidental disclosure	Employee	Disclosure	Low	2	2	1	1	3	27
Financial Records	Employee accidental disclosure	Employee	Disclosure	Low	2	2	1	1	3	27
Financial Records	Employee deliberate disclosure	Employee	Disclosure	Low	2	2	1	1	3	27
Order & Inventory Records	Accidental disclosure (mis-sent email, unlocked screen)	Employee	Disclosure	Low	2	2	1	1	3	27

Order & Inventory Records	Deliberate disclosure (insider leak)	Employee	Disclosure	Low	2	2	1	1	3	27
Order & Inventory Records	Natural disaster (shop destroyed)	Event	Interruption	Low	1	3	3	1	1	25
Order & Inventory Records	Deliberate destruction (delete records)	Outsider	Destruction	Low	3	2	3	1	1	24
Order & Inventory Records	Malware affecting records	System	Disclosure/Modification/Interruption/Destruction	Medium	2	1	2	1	2	22
E-Commerce Store Data	Outsider DDoS	Outsider	Interruption	Medium	1	2	2	1	1	20
Order & Inventory Records	Deliberate interruption (DDoS)	Outsider	Interruption	Medium	1	2	2	1	1	20
Order & Inventory Records	Software defect disclosure	System	Disclosure	Low	2	1	1	1	2	20
Order & Inventory Records	Employee knowledge accidental disclosure	Employee	Disclosure	High	2	1	1	1	2	20
Order & Inventory Records	Employee knowledge intentional disclosure	Employee	Disclosure	Low	2	1	1	1	2	20
Order & Inventory Records	IT contractor accidental disclosure	Contractor	Disclosure	Low	2	1	1	1	2	20
Order & Inventory Records	IT contractor deliberate disclosure	Contractor	Disclosure	Low	2	1	1	1	2	20
Backup Data	Modification of backups	System	Modification	Low	2	1	3	1	1	20
Order & Inventory Records	Accidental modification (wrong field)	Employee	Modification	Medium	1	2	2	1	1	20
Order & Inventory Records	Deliberate modification	Employee	Modification	Low	1	2	2	1	1	20
Order & Inventory Records	Accidental destruction (delete records)	Employee	Destruction	Low	2	1	2	1	1	18
Order & Inventory Records	Deliberate destruction	Employee	Destruction	Low	2	1	2	1	1	18
Backup Data	Interruption of backups	System	Interruption	Low	1	1	2	1	1	17
Order & Inventory Records	Employee absence (sickness)	Employee	Interruption	Medium	1	1	2	1	1	17
Order & Inventory Records	Supplier intentional disclosure	Supplier	Disclosure	Low	1	1	2	1	1	17

Order & Inventory Records	Software defect modification/loss	System	Disclosure/Modification/Interruption/Destruction	Low	1	1	2	1	1	17
Backup Data	Loss of backups	System	Destruction	Low	1	1	2	1	1	17
Order & Inventory Records	Accidental interruption (lost password)	Employee	Interruption	Low	1	1	1	1	1	15
Order & Inventory Records	Deliberate interruption (disconnect network)	Employee	Interruption	Low	1	1	1	1	1	15
Order & Inventory Records	Local power outage	Infra	Interruption	Medium	1	1	1	1	1	15
Order & Inventory Records	Network outage	Infra	Interruption	Medium	1	1	1	1	1	15
Order & Inventory Records	Supplier accidental disclosure	Supplier	Disclosure	Low	1	1	1	1	1	15