1. Report Objective

A Risk Assessment for Pampered Pets.

Pampered pets is within the scope of GDPR. If GDPR is breached, then pampered pets could face financial penalties and damages to its reputation.

2. Current Business Review

2.1 Selection of a Risk Methodology

The Factor Analysis of Information Risk (FAIR) Methodology was selected for the risk assessment due to the following (Reciprocity, 2020) :

- The framework has a defined taxonomy and is compatible with other risk management frameworks.
- It is suited to small organizations where historical data information is lacking.
- It shows risk in terms of the potential financial impact.
- It is widely used, easy to understand, has no-cost and is scalable.
- A qualitative risk method was chosen, because historical data is not available.

2.2 Identified Risks

Below is a summary of the current high-risk threats (for detailed breakdown, see appendix A):

- Shared infrastructure.
- Data breach/leakage.
- Inability to determine or investigate malicious attack(s).
- No personal data categorization.
- Inability to identify employees' log-in credentials.
- Unauthorized access
- No regular patching.
- Lack of policies like: security policy
- Denial-of-service attack
- Man-in-the-middle attack
- Non-standard network architecture
- Physical injury

- Virus/Malware exposure

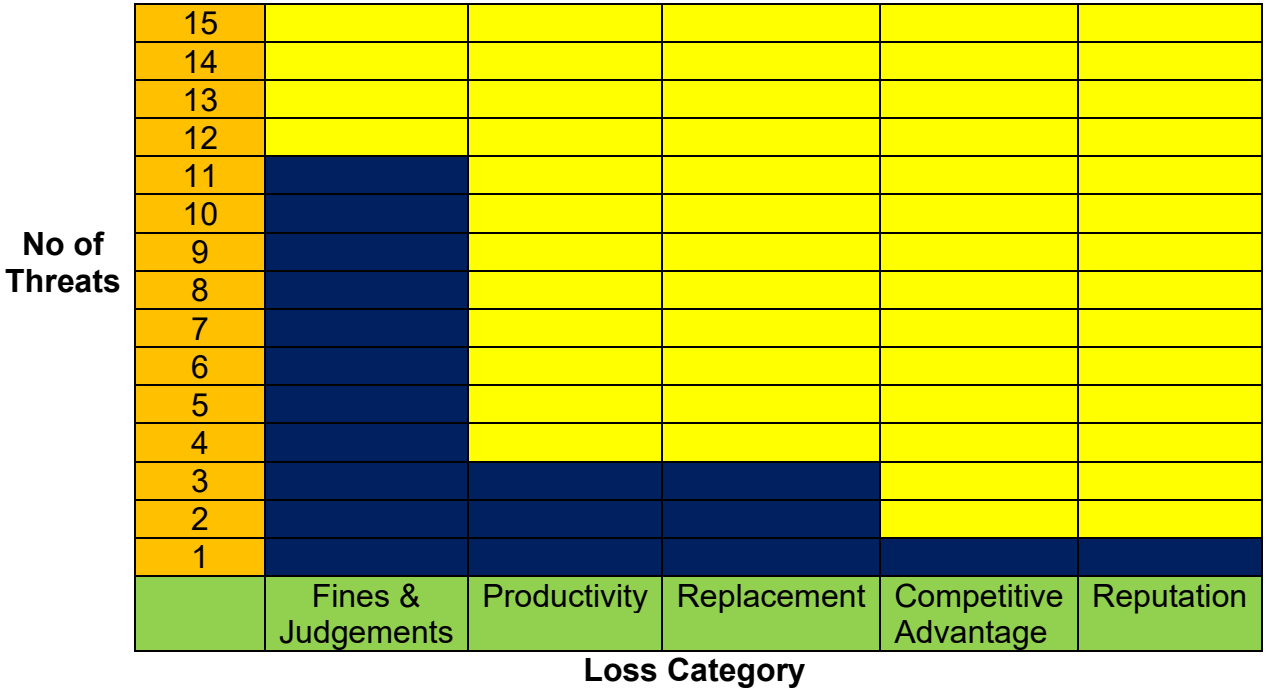
2.2 Risk Analysis Summary

- 73% of risks were categorized as high.
- Pampered pets is currently exposed to a high amount of regulatory risk.
- A detailed risk breakdown is in Appendix A.

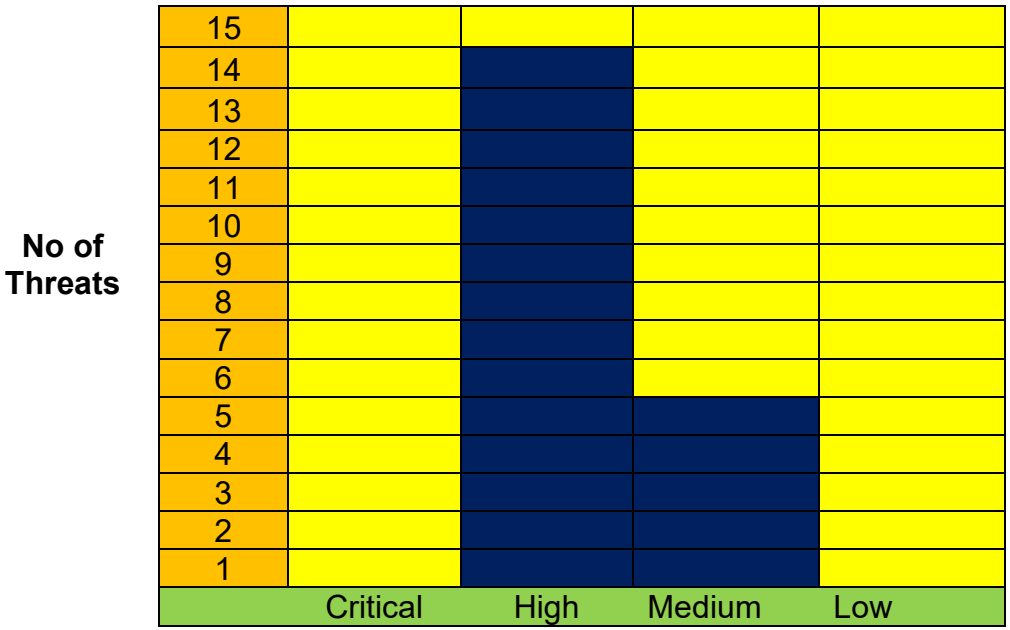
Financial Loss Analysis

Rating	Likely Annualized Loss Exposure Range		Number of threats
Critical	$1M	Or More	0
High	$500K	$1M	14
Medium	$250K	$500K	5
Low	$0	$250K	0

Threats by Loss Category



Threats by Risk Severity



2.4 Proposed Mitigations for High-Risk Threats

- Implement VLAN segregation and prioritize network traffic.
- Daily data back-up.
- Implement a detailed audit trail, which is backed-up off line and analysed.
- Categorise customer data (GDPR).
- Restrict use of USB/CD-ROM.
- Remove generic log-in credentials
- Segregate employee roles
- Enforce logout of computer sessions
- Enforce strict password format, multi-factor authentication and regular passwords expiration.
- Enforce monthly patching
- Implement security, password and incident management policies.
- Cybersecurity Insurance.
- Encrypt data.
- Set-up wireless router with Personal/Pre-Shared Key encryption mode.
- Implement firewall, antivirus and antimalware in the system.

3. Proposed Digitalisation Risk Assessment

3.1 A selection of a risk methodology

To ensure consistency, the FAIR risk methodology was used for the digitalisation process.

3.2 Proposed changes

- Implementation of SaaS (Software as a Service) solution, which has the integration between an ERP and E-commerce platform, such as Oracle's NetSuite.
- An ERP system provides inventory management and financial forecasting, and not the user experience of e-commerce systems.
- The vendor solution needs to include a well-known payments engine.
- Below are the reasons for selecting a SaaS solution (McCue , 2020):
    - Reduction in IT costs.
    - No need for in-house IT/Cybersecurity expertise.
    - Enforces software upgrades.
    - Real-time reporting and analytics.
    - There is no need to invest in and support additional IT infrastructure.

    - Lower upfront cost, which reduces the risk if the company profits don’t grow as expected.
    - Offers scalability.
- Upgrade of desktop computers.
- Implementation of a private network, firewall and separate wireless network for employee’s.
- Cyber Security training.
- Social media presence and on-line marketing that gives a competitive advantage for Pampered pets.

3.3 Identified Risks

High category threats are summarized below (for detailed breakdown, see Appendix B):

No	Threat Summary	Proposed Mitigation
1	Cyber-attacks/data leakages compromises Customers' data.	Data encryption.
2	Software release impacting the system.	Change management process.
3	SaaS is based on web delivery (internet failure results in unavailability of the system).	Implement VLAN segregation and QOS to prioritise network traffic.
4	Lack of transparency.	The SaaS vendor should be externally audited regularly.
5	An incident occurs which is not managed and reported correctly	Vendor Incident Response plan.
6	Unauthorized access to data	Implement Multi-Factor Authentication, Authorizations and strong password policy

3.4 Risk Analysis Summary

The high category risk has been reduced to 7% from 73% of the total number of threats.

When adopting a SaaS model, the regulatory risk is significantly reduced because a well-known cloud provider such as Oracle has multiple existing controls.

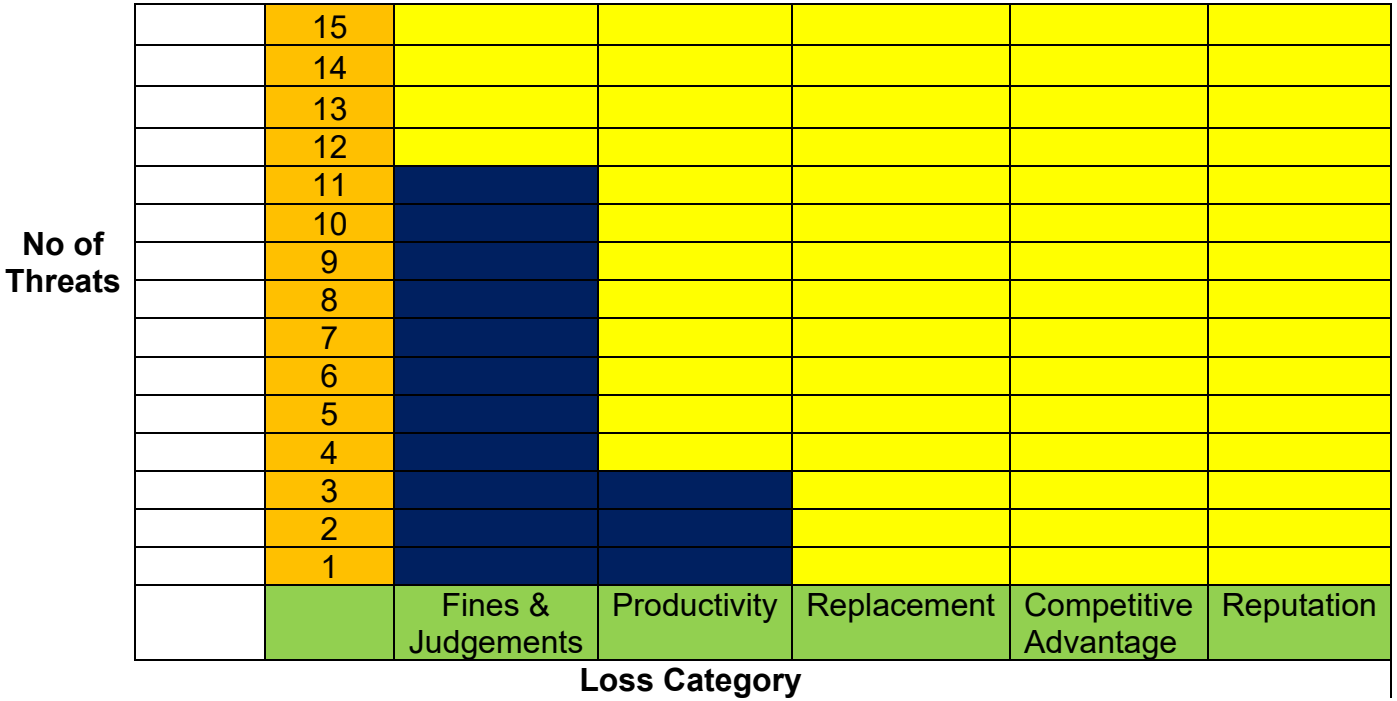
Comparison of the below graphs, for the current state and post digitalisation shows the shift in risk.

Appendix B contains a detailed risk breakdown.

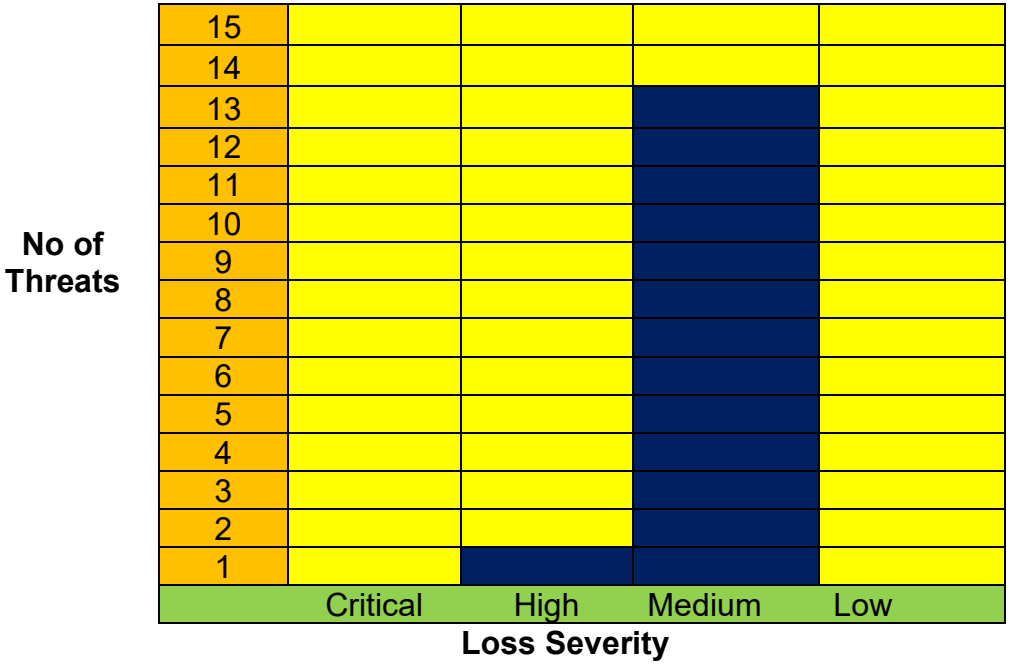
Financial Loss Analysis

Rating	Likely Annualized Loss Exposure Range		Number of threats
Critical	$1M	Or More	0
High	$500K	$1M	1
Medium	$250K	$500K	13
Low	$0	$250K	0

Threats by Loss Category



Threats by Risk Severity



3.5 Proposed Timeline

Phase 1 – Vendor due-diligence (4 weeks)

Phase 2 – Vendor pilot (4 weeks)

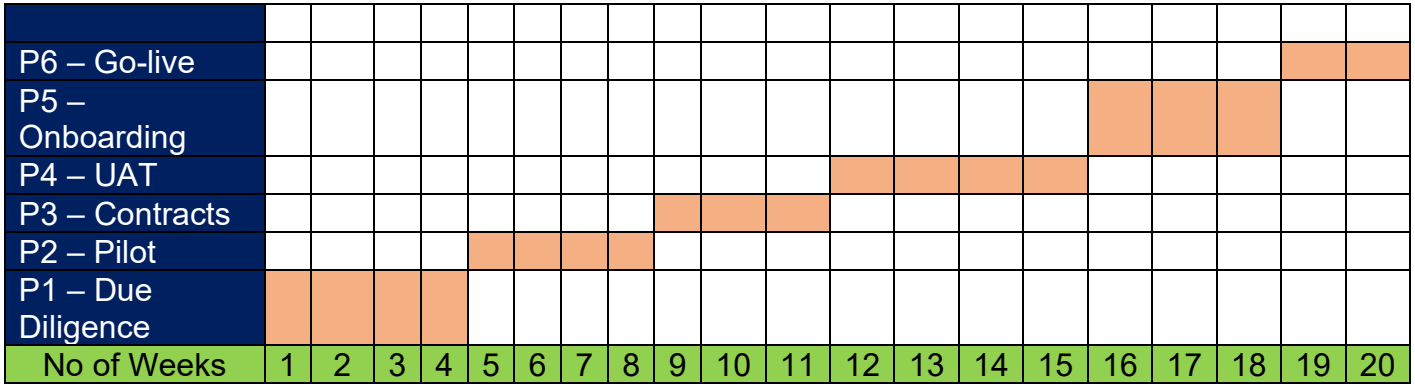
Phase 3 – Contractual Negotiations (3 weeks)

Phase 4 – User acceptance testing (4 weeks)

Phase 5 – Data Onboarding (3 weeks)

Phase 6 – Phased go-live (2 weeks)

Total duration – 20 weeks



4. Summary and Recommendations

1) The recommendation is to have an on-line presence because:

- The business could grow by 50%
    - In 2020, 93% of consumers used the internet to find a local business (Murphy, 2020), so it is realistic to expect that the business would grow by 50% with an on-line presence and without an on-line presence, **pampered pets could lose up to 33% of its current client base.**

2) Changing to an international supply chain will reduce costs by up to 24%

- The advantage of an international supply chain is that there are lower operating and labour costs during manufacturing which will reduce costs (Anon, N.D.)

3) The recommendation is to digitalize the current business due to:

- The growth potential (i.e. the business can grow by 50%).
- Pampered pets will lose customers and market share without digitalization
- The current infrastructure cannot support the required growth.

- If the status quo is maintained then pampered pets is subject to significant regulatory risk, (resulting to significant fines and reputational damage).

References

Anon, N.D.. *Global supply chains.* [Online]

Available at: https://www.cips.org/intelligence-hub/supply-chain-management/global-supply-chains

[Accessed 5 September 2022].

Anon, N.D. *10 Data Security Standards.* [Online]

Available at: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-policy/

[Accessed 1 July 2022].

Department of Health and Social Care, 2020. *New health data security standards and consent/opt-out model.* [Online]

Available at: https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

[Accessed 20 July 2022].

Lees, S., 2021. *GDPR – understanding personal data in the healthcare sector.* [Online]

Available at: https://www.gl.law/insight/news/gdpr-understanding-personal-data-in-the-healthcare-sector/

[Accessed 20 July 2022].

McCue , I., 2020. *SaaS ERP Explained.* [Online]

Available at: https://www.netsuite.com/portal/resource/articles/erp/saas-erp.shtml#:~:text=SaaS%20ERP%20is%20an%20enterprise,the%20software%20over%20the%20internet

[Accessed 5 September 2022].

Meier, J. D. et al., 2010. *Chapter 2 – Threats and Countermeasures.* [Online]

Available at: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648641(v=pandp.10)?redirectedfrom=MSDN

Murphy, R., 2020. *Local Consumer Review Survey 2020.* [Online]

Available at: https://www.brightlocal.com/research/local-consumer-review-survey-2020/

[Accessed 12 September 2022].

National Cyber Security Centre, 2018. *GDPR security outcomes.* [Online]

Available at: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

[Accessed 20 July 2022].

Reciprocity, 2020. *Pros and Cons of the FAIR Framework.* [Online]

Available at: https://reciprocity.com/pros-and-cons-of-the-fair-framework/

[Accessed 5 September 2022].

Appendix A – Current Threats and Mitigations Analysis

Evaluation of current threats and risks, and proposed mitigations

Below is a summary of the analysis which was carried out for the present state of risk for pampered pets, and uses the FAIR risk methodology. Proposed risk mitigations are also included.

The below table structure is taken from the Open Group Guide Risk Analysis Process for FAIR:

Valuation of Loss Key:

Rating	Most Likely Annualized Loss Exposure (ALE) Falls Between…	
Critical	$1M	Or More
High	$500K	$1M
Medium	$250K	$500K
Low	$0	$250K

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
1	Computers	Shared Infrastructure.	Employees	Human Error	Productivity	High	Implement VLAN segregation and QOS (Quality of Service) to tag and prioritize network traffic based on business needs.
2	Customer data	Data Loss - Losing or failing to back up data	Employees	Error	Fine Judgements	High	Backup data on a daily basis
3	Customer data	Not able to determine or	Cyber Criminals	Malicious	Fine Judgements	High	Implement a detailed audit trail, which is backed-up off line and

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
		investigate a malicious attack					analysed for malicious activity on a regular basis
4	Customer data	Data Categorization	Cyber Criminals	Malicious	Fine Judgements	High	Categorise customer data which is personal data under GDPR
5	Customer data	Data breach - data leaked or unintentionally exposed	Cyber Criminals	Malicious	Fine Judgements	High	Encrypt customer data in transit and while persisted. Use of USB/CD-ROM on network devices can be restricted. Encrypt passwords

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
6	Data and stock	Generic privileges and so the user cannot be identified	Cyber Criminals Employees	Malicious	Fine Judgements	High	Remove generic login id's and enforce individual login id's
7	Data	Unauthorized access – There is no standard password format Passwords do not expire No multi-factor authentication	Cyber Criminals Employees	Malicious	Fine Judgements	High	Segregate roles so that not every employee has access to required inventory and client data Enforce logout of computer sessions Enforce strict password format Enforce passwords to expire on a regular basis

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
							Implement multi factor authentication
8	Customer Data	There is no regular patching of the two computers or the wireless hub	Cyber Criminals	Malicious	Fine Judgements	High	Enforce monthly patching
9	Stock	Loss Prevention - no active monitoring for malicious behaviour	Cyber Criminals Employees	Malicious	Replacement (stolen assets)	Medium	Reconcile stock regularly to identify any ‘missing stock’

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
10	Customer Data	Regulatory fine because there is no security policy, no password policy, no incident management policy	Cyber Criminals	Malicious	Fine Judgements	High	Implement a security policy, password policy, incident management policy
11	Computers	Denial of service attack	Cyber Criminals	Malicious	Productivity	High	Implement Security solutions like WAF, Network Firewalls. Update and patch firewalls and network security programs.

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
12	Computer	Man-in-the-Middle (MIM) Attack	Cyber Criminals	Malicious	Replacement	High	Encrypt data, implement TLS (Transport Layer security)
13	Wireless router	Non-standard network architecture	Cyber Criminals	Malicious	Fines Judgements	High	Set wireless router with PSK (Personal/Pre-shared key) mode of WPA or WPA2 encryption
14	Stock	Theft / Loss/Property Damage	Thieves	Malicious	Replacement	Medium	Install a monitored alarm for the warehouse and CCTV. Buy insurance for stock damage
15	Employee	Physical Injury	Thieves	Natural	Fines Judgements	High	Ensure health and safety checks are carried out

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
							and documented on regular basis. Have adequate insurance coverage in place
16	Pampered Pets	Competitive rivalries	Competitor	Human	Competitive Advantage	Medium	Monitor competitors Have a strategy of growth for the company
17	Pampered Pets	Negative Reputation	Competitor Customers	Human	Reputation	Medium	Monitor social media closely, have a social media presence and strategy, respond to comments left by customers

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
18	Employees	Key staff are off sick	N/A	Human	Productivity	Medium	Have a contingency plan if more than one member of staff is off sick
19	Data	Viruses & Worms	Cyber Criminals	Malicious	Fine Judgements	High	Install and maintain antivirus and antimalware software on user's systems and networked devices.

Appendix B – Strategic Proposal – Risk Assessment and Proposed Risk Mitigations

The below risk assessment is for the digitalization changes proposed.

A SaaS implementation will generate third party risk. The risk mitigations are also included.

The below table structure is taken from the Open Group Guide Risk Analysis Process for FAIR:

Valuation of Loss Key:

Rating	Most Likely Annualized Loss Exposure (ALE) Falls Between…	
Critical	$1M	Or More
High	$500K	$1M
Medium	$250K	$500K
Low	$0	$250K

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
1	Client orders	The system is unavailable to process client orders due to a new version of software being released which was not tested sufficiently by pampered pets	Employees	Error	Productivity	Medium	Agree a testing schedule with the vendor Allow sufficient time for testing new releases plus contingency
2	Customer Data	Customer personal data is compromised, due to a cyber attack	Cyber criminals	Malicious	Fines/Judgements	Medium	Ensure strong encryption is in place for data to transit and when persisted

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
3	Customer Data	Customer personal data is compromised due to a data leakage	Employees	Error	Fines/Judgement	Medium	Ensure strong encryption is in place for data in transit and when persisted
4	Client orders	SaaS is based on web delivery and if the internet fails there is no access to the system	Employees	Error	Fines/Judgement	High	Implement VLAN segregation and QOS (Quality of Service) to tag and prioritize network traffic based on business needs
5	Client Orders	SaaS may run at lower speeds than on-	N/A	Error	Productivity	Medium	Agree performance SLA's with the vendor

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
		premise client or server					Ensure that the internet speed is sufficient
6	Client Orders	Limited customization of the system	N/A	Error	Productivity	Medium	Perform a pilot to assess the system functionality as an initial phase, before any contracts are signed
7	Payments	There could be an error when processing payments	Employees	Error	Fines/Judgement	Medium	Ensure that the SaaS vendor uses a well known payments engine Include a review of payments processing in a regular vendor audit

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
8	Customer Data	Customer data is compromised as it transits over the internet	Cyber criminals	Malicious	Fines/Judgements	Medium	Ensure that in transit data is encrypted
9	Data	Insufficient data to respond to or investigate an incident	Cyber criminals Employees	Malicious Error	Fines/Judgement	Medium	Ensure that the vendor has an incident management process Ensure that the vendor keeps detailed logs and has log analysis tools
10	Data	Legal implications because data is hosted outside of the UK	Employees	Error	Fines/Judgement	Medium	The vendor needs to confirm where the data is physically stored

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
							The location of data storage should be included in the vendor contract
11	Data	Pampered pets is unable to prove that it meets the regulatory requirements such as GDPR	N/A	Error	Fines/Judgement	Medium	The vendor needs to be audited on a regular basis and provide evidence that regulatory obligations are being met Routine security questionnaires should also be completed by the vendor

Threat No	Asset at Risk	Threat	Threat Community	Threat Type	Forms of Loss	Valuation of Loss	Threat Action (Mitigation)
12	Data	An incident occurs which is not managed and reported correctly	Employees Cyber criminals	Multiple	Fines/Judgement	Medium	The vendor should have a detailed incident response plan which covers multiple scenarios
13	Data	Data is not retained for the period required by regulators	Employees	Error	Fines/Regulatory	Medium	Within the contract the vendor needs to state what the cloud retention policy is and how it is enforced
14	Data	Unauthorized access to data	Cyber criminals	Malicious	Fines/Regulatory	Medium	Ensure that multi-factor authentication exists