1. Report Objective

The objective of this report is to detail the risks and the associated risk probability, for the proposed digitalisation changes, in terms of product quality and the performance of the supply chain.

2. Risk Analysis

2.1 Risk Modelling Approach

Monte Carlo was selected because:

- Monte Carlo simulations have been used in many different scenarios from stock prices, sales forecasting, project management and pricing, and it is a proven model.
- It provides a number of advantages over predictive models, with fixed inputs, by providing output based on an estimated range of values. It uses random numbers between the minimum and maximum range to calculate results, and simulates a huge number of possible scenarios (IBM, 2020).
- The results are averaged to provide a probability, so risks are expressed in terms of probabilities (Gisslen et al, 2016).
- It is very flexible, and easily understood.

- The Monte Carlo simulation caters for uncertainty in terms of variables, which would apply to the analysis of risk for a supply chain and product quality risk.
- There are also multiple risk factors which can impact supply chain performance, and some of those risks, such as natural disasters, are likely to occur very rarely and so fixed variable models will not be able to model the risk accurately.

2.2 Risk Calculation and Data – Supply Chain Management

In supply chain management, the impact of risk is manifested by a lack of stock or by holding too much stock. The primary concern of stakeholders was stock not being available. Any of the below risks could impact the availability of stock.

The Monte Carlo simulation for the supply chain risks was based on the following :

- 10 risk categories, broken down into specific risks.
- The number of occurrences of each risk category over the previous 12 months, using historical data from Pampered Pets and insurance data from the Pet Supply industry.
- The predicted number of occurrences of each risk category based on expert opinion for the next 12 months.
- For Cyber security risks, historical data from the Cyber Security Breaches survey 2022 (GOV.UK, 2022), and threat reports from the National Cyber Security Centre (NCSC, 2022) were used.

- The Monte Carlo simulation was run 100 times using Yasai and excel, to predict the probability of a risk occurring over the next 12 months.

2.3 Risk Priority Approach

- A heatmap was created to analyse risk priority for Pampered Pets, and to ensure that the highest risks are those that are a priority to the business and meet its' commercial needs.
- The heatmap includes the probability of a risk occurring, the impact of the risk and whether the risk could have a regulatory impact.
- The impact of the risk was based on expert opinion.
- A potential regulatory breach automatically makes the risk a high priority, regardless of the risk probability or risk impact.
- **This approach will provide risk priorities according to the business's commercial needs.**

2.4 **Supply Chain Risks and Risk Probability**

The risks detailed in the table below are derived from (Rauniyar, et al., 2022), (Rodriguez, 2019) and (Bailey et al, 2019)

Table Key :

*Probability of Risk Occurring Over a 12 Month Period, derived from Monte Carlo Simulation:

High probability – 10 and above (Red), Medium probability – 5 to 9 (yellow), Low probability – 1 to 4 (green)

**Risk Impact (disruption to the supply chain):

High - Red, Medium - yellow, Low – Green

***Risk Prioritization:

1 = highest priority

Risk Prioritization***	Top Priority Risks***	Risk Category	Underlying Risks	Probability of Risk %*	Risk Impact**	GDPR Regulatory impact
2	4	Financial	1) Budget overruns 2) Additional funding due to missed milestones 3) Bankruptcy 4) Incomplete project	4.6	High	No

Risk Prioritization***	Top Priority Risks***	Risk Category	Underlying Risks	Probability of Risk %*	Risk Impact**	GDPR Regulatory impact
			5) Reputation damage			
2	3	Scope of schedule	1) Change of schedules	13.8	Medium	No
3		Legal	1) Misuse of intellectual property, 2) Violation of laws 3) Civil lawsuits and fines 4) Not meeting the regulations, standards or requirements included in the terms and conditions,	3.7	High	No (excludes security regulations)
3		Environmental	1) Negative impact on global environment	1.8	Low	No
2	5	Socio-political	1) Corruption 2) Ethics	4.6	High	No

Risk Prioritization***	Top Priority Risks***	Risk Category	Underlying Risks	Probability of Risk %*	Risk Impact**	GDPR Regulatory impact
			3) Issues of trust, 4) Bureaucracy			
3		Project organizatio n	1) Project delivery delays	7.3	Medium	No
3		Human behaviour	1) Lack of training 2) Change of schedules 3) Negative impact on the budget, project/business continuity	3.7	High	No
3		Reputation	1) Loss in demand 2) Loss in investment and morale	0	High	No
1	1	Cybersecur ity	1) Reputation damage 2) Hacking of BYOD and IoT	51.4	High	Yes

Risk Prioritization***	Top Priority Risks***	Risk Category	Underlying Risks	Probability of Risk %*	Risk Impact**	GDPR Regulatory impact
			3) Denial of Service attacks 4) Malware and virus infesting the system(s) and end user devices 5) Software security vulnerabilities in supply chain management 6) Counterfeit hardware			
1	2	Information	1) Data breaches 2) Lawsuits and Fines 3) Reputation damage 4) Bankruptcy 5) Third party data banks	9.2	High	Yes

2.5 Assumptions – Supply Chain

- Pampered pets will be using an international supplier for the manufacturing of pet food.

2.6 Summary of Results – Supply Chain

- The top two risks with a 51.4 and a 9.2 probability of occurring over the next 12 months, are cyber security and information risks.
- Both of these risk categories have the potential to breach GDPR, and both have been classified as high impact.
- The next category of risks which should be addressed are where the heatmap, is showing a red and yellow combination (financial, scope of schedule and socio-political categories).
- A priority number has been assigned to each risk category, based on the regulatory impact, the risk probability and the risk impact (non-regulatory).
- If a risk could have a regulatory impact then it is automatically classified as top priority.
- The top two risks below increase the probability of a breach of GDPR and the potential associated fines.
- The recommendation is that the following risks are addressed by order of priority:

Priority	Risk Category	Probability	Impact	Regulatory impact	Proposed Risk Mitigation
1	Cybersecurity	51.4	High	Yes	Create a cyber security policy and associated remediation plan Regular audits Ensure that suppliers adhere to their own cyber security policy
2	Information	9.2	High	Yes	Monitor Information security policies of suppliers Ask to review suppliers audit findings
3	Scope of Schedule	13.8	Medium	No	Regular supplier manufacturing status reports
4	Financial	4.6	High	No	Ensure suppliers are on schedule and within budget Suppliers to provide monthly budget updates Monitor financial stability of the supplier

Priority	Risk Category	Probability	Impact	Regulatory impact	Proposed Risk Mitigation
5	Socio-political	4.6	High	No	Ensure that the supplier has in place an anti-bribery policy and procedures

2.7 Risk Calculation and Data – Product Quality

- The risk probability was determined by using historical data gathered through quality sampling of pet food, plus customer returns over a 12 month period.
- Sampling of pet food takes place weekly, so over a 12 month period there are 52 samples taken for quality analysis.
- The number of risks will have increased with a new international supplier, and included in this are the additional transport or logistics risks.
- The number of individual risks per risk category was a parameter in the simulation.
- Expert opinion on the number of issues which could be encountered over the next 12 months was also used in the formula.
- The simulation results are shown in terms of the probability of the number of weekly sampling checks which will fail, over a 12 month period, due to product quality issues.

- The Monte Carlo simulation was run 100 times using Yasai and excel.

2.8 Product Quality Risks

Table Key :

*Probability of Risk Occurring Over a 12 month period represented as the number of weekly quality samples which fail (percentage):

- High probability – 30 and above (Red), Medium probability – 11 to 29 (yellow), Low probability – 1 to 10 (green)

**Risk Impact - High - Red, Medium - yellow, Low – Green

*** Risk Prioritization – 1 = highest priority

Risk*** Prioritization	Risk*** Prioritization	Risk Category	Underlying Risks	Probability of Risk*	Risk Impact**	GDPR Regulatory Impact
1	2	Improper Storage	1) Insufficient refrigeration at supplier	36.3	High	No

Risk*** Prioritization	Risk*** Prioritization	Risk Category	Underlying Risks	Probability of Risk*	Risk Impact**	GDPR Regulatory Impact
			2) Insufficient hygiene at the supplier 3) Transportation hygiene issues 4) Warehouse hygiene issues 5) Water damage at warehouse impacts quality 6) Rodent infestation at supplier 7) Rodent infestation at warehouse 8) Product recall 9) Regulatory fine			
2	3	Animal Feed Quality	1) Poor quality raw materials 2) Contamination of food 3) Poor hygiene	14.9	High	No

Risk*** Prioritization	Risk*** Prioritization	Risk Category	Underlying Risks	Probability of Risk*	Risk Impact**	GDPR Regulatory Impact
			4) Product recall 5) Regulatory fine			
1	1	Packaging	1) Labelling of ingredients not correct 2) Damaged packaging 3) Quality of packaging 4) Product recall 5) Regulatory fine	43.3	High	No
3	4	Out of date stock	1) Out of date stock	5.5	Medium	No

2.9 Assumptions – Product Quality

Pampered pets will be using a different international supplier.

2.10 Summary of Results – Product Quality

Insufficient quality control can result in liability claims, product recall and reputational damage. The probability of a risk occurring which impacts product quality, is represented as the probability of a failed weekly product quality test over a 12 month period.

The recommendation is to remediate the three risks below, which have the highest probabilities and also the highest impact.

Priority	Risk Category	Probability	Impact	Proposed Risk Mitigation	Regulatory Impact
1	Packaging	43.3	High	Weekly sampling for quality, to check: • The packaging has the correct product • The quality of the product is correct • The correct packaging materials were used	No

Priority	Risk Category	Probability	Impact	Proposed Risk Mitigation	Regulatory Impact
				• Barcodes, labelling and ingredients are correct The supplier should have a quality assurance process QA checks should be automated Supplier to provide a weekly QA status report	
2	Improper Storage	36.3	High	Use storage facilities which have automated the checking of refrigeration temperature There needs to be a hygiene policy in place and there should be regular documented checks to ensure that these standards are being met.	No

Priority	Risk Category	Probability	Impact	Proposed Risk Mitigation	Regulatory Impact
3	Animal Feed Quality	14.9	High	The manufacturer should have an automated process for checking the quality of animal feed, and a quality assurance process to ensure that the automated process is working	No

2.11 Executive Summary and Recommendations

Through the Monte Carlo simulations we have identified the top risks, in terms of probability, for the supply chain and also for product quality. The five top supply chain risks and the three top product quality risks need to be addressed and the proposed risk mitigations implemented.

Out of the eight priority risks identified, the supply chain cybersecurity and information risks could cause a breach of GDPR, so these two risks are the top priority risks which need to be addressed first out of the eight.

The risk assessment should be run on an on-going basis, we propose monthly, because the probability and priority of risks may change, if the underlying data inputs change. New risks may also be identified.

3.0 Business Continuity and Disaster Recovery Strategy

- In the previous risk assessment for Pampered Pets, the proposal was to implement a SaaS solution (Oracle's NetSuite product).
- A SaaS solution will impact the BCP/DR strategy and Pampered Pets will be dependent on the SaaS provider for BCP/DR.
- The requirements are that the online shop should be available for 24/7/365 with less than a minute changeover window and that the business cannot afford to lose more than 1 minute of data.
- The SaaS provider needs to provide the following to meet the DR requirements :
    - The system needs to run live/live, this means that there needs to be two data centres which host the data and application which are duplicates of each other and run in an active-active mode. So they operate concurrently to share service loads. In the event of failure of one data centre, the system provides automatic failover with zero downtime and zero loss of data.
    - The storage, compute, application, network, transmission, and security layers must all be designed to support an active-active architecture (see appendix A).
    - There should be regular DR tests, where one DC is out of action.

- The vendor should also back up data off-line daily, so if there is data corruption which impacts both DC's then back-ups will be available, for example if there is a cyber attack.

- In addition, in terms of BCP, in the event of a natural disaster at the warehouse or shop, then there needs to be a contingency plan to use alternative premises and a DR site which is not in the near vicinity, all employees should also have the technology in place to work from home.

4.0 Vendor Lock-in

In order to avoid vendor lock-in, then the following measures can be taken :

- Ensure that the original vendor contract includes a clause to support a data migration.
- Vendor lock-in risk is increased with a cloud solution, however a big cloud provider, will have a process for supporting clients who want to move onto a different platform/vendor and also automated tools to support a data migration.
- Vendors and platforms should be selected that provide more standardised formats and protocols based on standard data structures, and ensure that there is sufficient portability (Opara-Martins et al, 2016).

- Port data out of the cloud on a daily basis, and reconcile it back to the cloud daily. The data should be held in a data model which represents the business. The data should also be held in WORM storage, in order to provide a layer of protection, and to ensure that the data cannot be altered.

References

Bailey, T., Barriball, E., Dey, A., Sankur, A. (2019). *A practical approach to supply-chain risk management.* McKinsey & Company.

Rauniyar, K. et al., (2022). *Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology.* Industrial Management & Data Systems.

Gisslen, L., Horndahl, A. (2016). *A Quantitative Approach to Risk and Cost Assessment in Supply Chain Management.* 2016 European Intelligence and Security Informatics Conference.

GOV.UK (2022). Cyber Security Breaches Survey 2022. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[Accessed 20th October 2022]

IBM (2020). Monte Carlo Simulation. Available from:

https://www.ibm.com/cloud/learn/monte-carlo-simulation

[Accessed 15th October 2022]

National Cyber Security Centre (2022). Threat Reports. Available from:
https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc

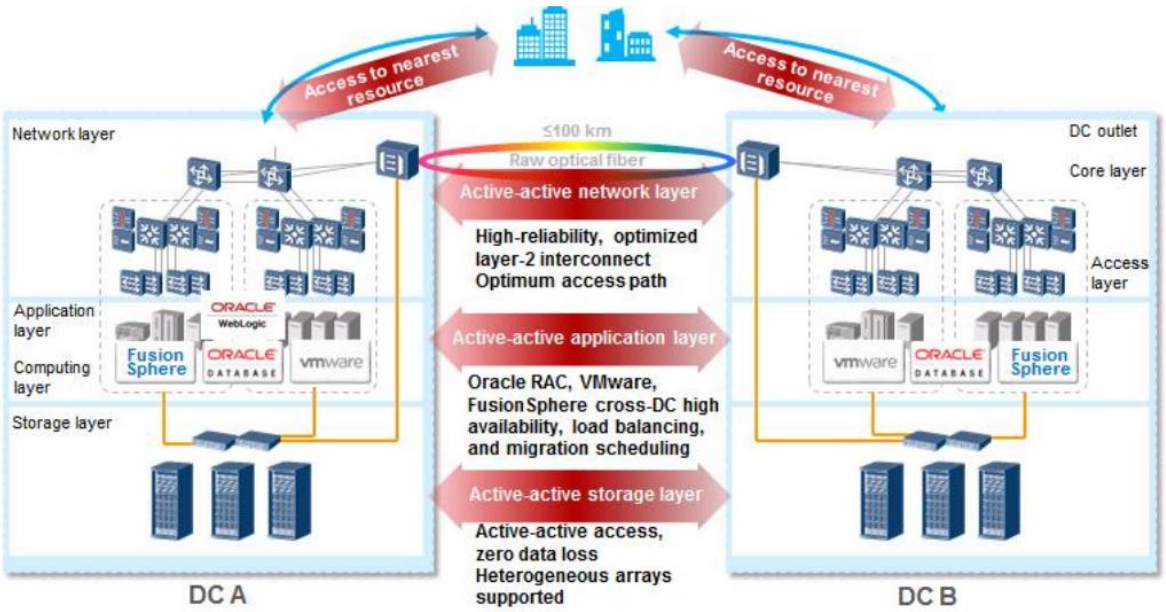
[Accessed 15th October 2022]

Opara-Martins, J., Sahandi, R., Tian, F. (2016). *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective.* Journal of Cloud Computing: Advances, Systems and Applications.

Rodriguez, D. (2019). 7 Basic Types of Supply Chain Risks. Available from:
https://precoro.com/blog/7-basic-types-of-supply-chain-risks/
[Accessed 5 October 2022].

Appendix A

The below diagram is sourced from Huawei (2017) from the 'Active-Active Data Center Solution Technical White Paper', which is anonymous :


Access to nearest resource
Access to nearest resource
Network layer
≤100 km
Raw optical fiber
Active-active network layer
High-reliability, optimized layer-2 interconnect
Optimum access path
DC outlet
Core layer
Access layer
Application layer
Computing layer
Storage layer
Active-active application layer
Oracle RAC, VMware, FusionSphere cross-DC high availability, load balancing, and migration scheduling
Active-active storage layer
Active-active access, zero data loss
Heterogeneous arrays supported
DC A
DC B