Tom Smith Unit 11 Assignment

Individual Project: Executive Summary

Introduction

Pampered Pets has chosen to implement digitalisation improvements to build their brand and streamline their business operations. As recommended by our previous assessment, e-commerce capabilities, online marketing and blogging, and an ERP will streamline business processes and provide new revenue streams.

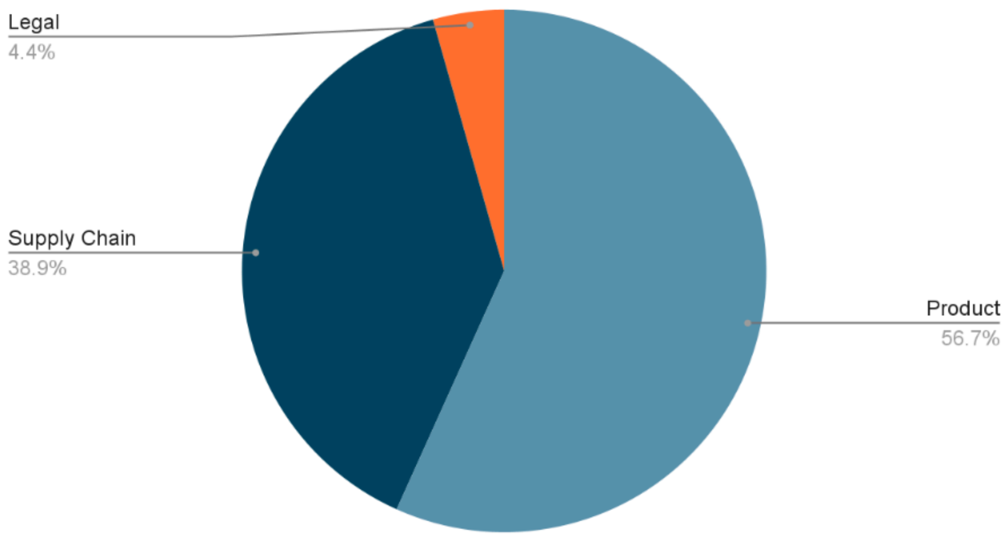
Furthermore, the business has taken initiatives to expand to an international supply chain to lower costs and diversify market reach, and utilise automated warehouses to increase efficiency.

The risks associated with these initiatives will be mapped to strong mitigation strategies, and will be supplemented by a robust business continuity plan.

Risk Summary

The table below summarises the financial outcomes of the quantitative analysis performed. There are more risks during the initial period of digitisation and this has been reflected in the summary.

Type	Year 1 Cost	Year 2 Onward Cost
Product Quality Risks	£122 200	£97 000
Supply Chain Security Risks	£86 500	£66 500
Legal Risks	£7 500	£7 500



Product Quality risks make up a slight majority of the overall risk costing which is expected as this is a key priority of the business. The most expensive risk is the cost of data synchronisation issues which is due to the critical RPO requirement of 1 minute. The least costly risk is the cost of physical security breaches which are both low impact and low probability.

Risk Analysis

Annualised Loss Expectancy (ALE)

Method

The risks have been quantified by using the Annualised Loss Expectancy (ALE) model (Blakely et al., 2001) as it performs well as an indicator of budget required to mitigate risks (De Bruyn, 2019). Furthermore, Kuzminykh et al. (2021) calls this assessment method “business-friendly” which is suitable for an executive summary for business stakeholders, and Taylor (2013) explains that it is useful to decide whether a risk is worth its cost.

Other methods of analysis were considered such as Monte Carlo simulations analysis. Monte Carlo simulations are very good at making predictions based on historical data, but as this is a new endeavour with very limited data available, it has limited applicability here (Bonate, 2001). A simulation can be carried out based on assumptions, but Monte Carlo is very sensitive to assumptions and so a small misjudgement can give dramatically different results (Kanade, 2023).

ALE is calculated as follows:

$$ALE = SLE \times ARO$$

Where SLE is the Single Loss Expectancy: the loss to the company in the case that the risk occurs once, and ARO is the Annualised Rate of Occurrence: how many times the risk is likely to actually occur in a year (De Bruyn, 2019).

SLE is calculated as:

$$SLE = AV \times EF$$

Where AV is the Asset Value (in this case the business has been assumed as a single asset as the digitalisation is company-wide - see assumption A-01), and EF is the Exposure Factor: the percentage of the business that is affected by each risk event (Krutz, 2001).

Data

The table below outlines the key risks associated with the mentioned digitalisation. Risks are organised into the categories of ‘product quality’, ‘supply chain security’, and ‘legal’.

Risk	SLE	SLE Justification	ARO	ARO Justification	ALE
Product Quality					
Data corruption within ERP system	30 000 (A-02)	Product specifications, production processes, and resource planning compromised leads to reduction in product quality.	0.8	A study by Bairavasundaram et al. (2008) found that the average disk experiences 0.08 corruptions per year (A-12, A-13).	24 000
Errors in automated warehouse	500 (A-03)	Machinery or configuration faults can lead to lower quality,	44	Tsarouhas & Fourlas (2015) found that the average operating time of robotic	22 000

systems		damaged or incorrect products reaching clients.		systems is 88%.	
Integration issues between new and existing systems	30 000 (A-04)	Critical processes may not be compatible or may need adapting which can affect the end product or cause delays.	0.84	Forbes found that 84% of digital transformations experience integration issues (Rogers, 2016) - although this is likely to be a one off issue at the beginning of the digitisation process.	25 200
Reduced human oversight and intervention	500 (A-05)	Defects and quality issues may be missed by automated systems, or affect larger batches before being found.	22	As above for ‘errors in automated warehouse systems’. Assume that half of the errors are worsened by lack of oversight (A-15).	11 000
International supply chain affects quality or availability of raw materials	20 000 (A-06)	Inconsistent material supply can affect the reliability of product quality or the amount of product that is able to be manufactured.	2	See assumption A-14.	40 000
Supply Chain Security					
Cyber attacks	20 000	Unauthorised access can	0.5	Cyber Security Breaches	10 000

target supply chain systems	(A-07)	lead to operational disruption, data breaches, and reputational damage.		Survey 2024 found that half of UK businesses experienced a cyber attack over 12 months (DIST, 2024).	
International supply chain creates logistical complexities	20 000 (A-06)	Implementation of an international supply chain will take time and research to set up.	1	Organisation of the supply chain is likely to occur at the beginning of the digitisation process and then further issues will be absorbed in other risk categories.	20 000
Inaccurate or delayed data synchronisation between ERP, e-commerce and supply chain	100 (A-08)	Discrepancies in inventory can or cause supply chains to be inefficient. Orders may need checking to be completed properly.	525	The 1 minute RPO requested means 525 600 synchronisation per year and a failure rate of 0.1% is assumed (A-15).	52 500
Physical security of geographically diverse supply chain	80 000 (A-09)	Theft, tampering or sabotage can ruin large batches of products or cause delays.	0.05	One-in-ten small businesses were victims of crime which cost in excess of £10 000 in a two year period (Downes, 2023).	4 000
Legal					

Non-compliance with GDPR in online marketing, e-commerce or ERP system	16 000	Fines and legal implications as well as brand reputational damage and loss of custom (Vaidya, 2018).	0.47	47% of small businesses were subjects of a breach in a 12 month period (Vaidya, 2018).	7 520
Non compliance with PCI-DSS through e-commerce sales	120 000 (A-10)	Payment fraud, data breaches and theft can have catastrophic results for customers and the business.	-	Fines are based on non-compliance and vary depending on severity and length of time (GoCardless, 2023).	-

Mitigation Recommendations

In order to mitigate these risks and sustain product quality, the following recommendations are provided in priority order:

#	Recommendation	Justification
1	Supply chain diversification	As the largest likely cost per year, having multiple supply chains across multiple geographical regions to improve product resilience is paramount (Li et al., 2022). This is a trade-off with logistical complexities (also modelled), but as that is more of a one off cost, pay-off

		is likely to be seen over time.
2	Use a cloud provided datacenter infrastructure	Dixit et al. explain how compiler optimisation, protected datapaths, and architectural priority can mitigate data corruption (2021), but a non-technical team should abstract this strategy to a specialist provider. This is particularly key due to the expected RPO of 1 minute. This solution is also key to reducing the cost of data synchronisation issues between key systems.
3	Automation Monitoring	Due to the impact of automation errors, and the exacerbation from uncaught errors, monitoring is integral to the success of automated warehouses. This may include IoT quality scanning devices and predictive maintenance via AI and big data analytics - beware these come with their own cyber security risks (Ani et al., 2024).
4	Data management policies and audits	A company-wide data management policy should be implemented to counter the likelihood of cyber breaches, as well as reduce synchronisation error occurrence. This should be enforced on the e-commerce site, ERP system, online blog, and throughout the in-store customer experience. Clear incentives and sanctions should be embedded into the

		policy to ensure that people comply with the policy (Janssen, 2020).
5	Hire an Information Security Officer	An Information Security Officer can implement measures and processes to protect you from cyber crime, physical thefts. The byproduct of the good practices they would introduce is that you are more likely to avoid GDPR and PCI-DSS fees and fines. Although this has many benefits, it is a lower priority as it is a greater consideration.

Business Continuity

Disaster Recovery Strategy

Requirements

RTO: 1 minute

RPO: 1 minute

Availability: 24/7/365

Strategy

The DR requirements are typical of a highly critical system and so an active-active DRaaS (Disaster Recovery as a Service) solution is most appropriate (Necat, 2022). DRaaS uses cloud technology providers to emulate systems remotely so that they can be initiated when the original system experiences a disaster (Andrade et al., 2017). Although using an on-site solution provides higher synchronisation rates (due to the shorter distance for the data to travel), this advantage is offset by the risk of any geographical disaster - which warrants the need for cloud based geographical diversification (Alhazmi & Malaiya, 2013).

To meet the 1 minute Recovery Time Objective and ‘always on’ availability, two data centres must be running at all times with a traffic manager able to instantly change to the secondary system in case of failure. Both systems must be active at all times which will mean higher utilisation costs (Wood et al., 2010).

To meet the 1 minute Recovery Point Objective, data should be copied synchronously between the two sites to guarantee data consistency, although due to geographical distancing, additional latency means there may be a slight delay (Alhazmi & Malaiya, 2013). This may work favourably, however, as a small delay can eliminate the impact of data corruption (Necat, 2022).

Regular failover testing is essential to ensure that these measures are operating effectively. Periodic drills and simulations should be scheduled to ensure that the RTO and RPO are being met.

Platform

Recommended Provider: Zerto

Secondary Recommended Provider: Amazon Web Services

Feature	AWS	Zerto
Deployment Model	Public cloud	On-premises, Hybrid, Multi-cloud
RTO (Recovery Time Objective)	Near-zero to minutes	Near-zero to minutes
RPO (Recovery Point Objective)	Near-zero to seconds	Near-zero to seconds
Data Replication	Asynchronous and synchronous replication	Continuous Data Protection (CDP)
Failover Automation	Automated failover and failback	Automated failover and failback
Disaster Recovery Testing	Yes	Yes
Cost Model	Pay-as-you-go or Reserved Instances	Subscription-based pricing
Integration with Other Tools	Integrates with AWS Backup, AWS CloudWatch, AWS Security Hub	Integrates with VMware vSphere, Nutanix Prism, AWS, Azure

(AWS, 2024; Wilson, 2022; Zerto, 2022)

AWS is easy to get started, and is suitable for SMEs such as Pampered Pets. Zerto is also very user friendly and supports a variety of cloud options, as opposed to AWS which only works within its own ecosystem (Zerto, 2022). Zerto is likely to be more expensive, although this cost is offset by the variety of compatible hosting options which helps to avoid vendor lock-in (Rawool et al., 2020).

Vendor lock-in happens when providers make their service incompatible with alternative providers to make any transition difficult and so the customer is dependent (Opara-Martins, 2016). The lock-in might not be purely cost related as system differences may require new staff to be hired to gain suitable resources. AWS Lambda functions, for example, are known to require specialist knowledge to transfer to other cloud providers (Alhosban et al., 2024).

Although Microsoft Azure is a common provider with equivalent capability to those recommended above, it is considered more difficult to use and requires more IT knowledge to set up solutions (Rawool et al., 2020).

Assumptions

#	Assumption
A-01	The current annual revenue of Pampered Pets represents the value of the business and is £500,000, as given in the previous assessment.
A-02	Data corruption of key information on products and processes could take roughly 3 weeks to rectify.
A-03	An error in machinery could take a few hours for a configuration fault or a day for a repair.

A-04	Integration issues between complex systems may take several weeks to resolve if multiple parties need to communicate and implement fixes.
A-05	Reduced human oversight may mean that a day's worth of batches are generated without quality control.
A-06	International reshipping of a large order may take multiple weeks to organise and receive.
A-07	Cyber attacks may limit services for a few weeks.
A-08	Inaccurate data could take a few hours to be noticed and rectified.
A-09	Sabotage and theft could affect up to 2 months worth of production.
A-10	PCI-DSS fine is £60,000 but reputational damage is equal (GoCardless, 2023).
A-11	Revenue is earned uniformly throughout the year.
A-12	Corruption rates have not improved since 2008.
A-13	10 HDDs/SSDs are used in the ERP system.
A-14	Supply chains experience availability issues twice per year due to extreme weather.
A-15	Half of automated machinery errors have reduced impact as they are noticed by human intervention before damage can occur.

References

Alhazmi, O. H. & Malaiya, Y. K. (2013) ‘Evaluating disaster recovery plans using the cloud’, *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*. Orlando, 28-31 January. New York: IEEE. 1-6.

Alhosban, A., Pesingu, S. & Kalyanam, K. (2024) CVL: A Cloud Vendor Lock-In Prediction Framework. *Mathematics* 12(3): 387.

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing* 99(10): 929-954.

Ani, E. C., Olu-lawal, K. A., Olajiga, O. K., Montero, D. J. P. & Adeleke, A. K. (2024) Intelligent monitoring systems in manufacturing: current state and future perspectives. *Engineering Science & Technology Journal* 5(3): 750-759.

AWS (2024) AWS Elastic Disaster Recovery. Available from: https://aws.amazon.com/disaster-recovery/?nc=sn&loc=1 [Accessed 27 May 2024].

Bairavasundaram, L. N., Arpaci-Dusseau, A. C., Arpaci-Dusseau, R. H., Goodson, G. R. & Schroeder, B. (2008) An analysis of data corruption in the storage stack. *ACM Transactions on Storage (TOS)* 4(3): 1-28.

Blakley, B., McDermott, E., & Geer, D. (2001) ‘Information security is information risk management’, *Proceedings of the 2001 workshop on New security paradigms.* Cloudcroft, New Mexico, 10-13 September. New York: ACM. 97-104.

Bonate, P. L. (2001) A brief introduction to Monte Carlo simulation. *Clinical pharmacokinetics* 40: 15-22.

De Bruyn, I. (2019) *The Influence Of Annualized Loss Expectancy On IT Risk Management And Cybersecurity In Belgian SMEs*. Belgium: Ghent University.

Downes, R. (2023) Organised shoplifting among most common types of crime affecting small businesses. Available from https://www.fsb.org.uk/resources-page/organised-shoplifting-among-most-common-types-of-crime-affecting-small-businesses.html [Accessed 25 May 2024].

DIST (2024) Cyber security breaches survey 2024. Available from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 [Accessed on 24 May 2024].

Dixit, H. D., Pendharkar, S., Beadon, M., Mason, C., Chakravarthy, T., Muthiah, B. & Sankar, S. (2021) Silent data corruptions at scale. *arXiv* (2102): 11245.

GoCardless (2023) PCI fines and penalties. https://gocardless.com/guides/posts/pci-fines-penalties/ [Accessed on 24 May 2024].

ICO (2018) UK GDPR guidance and resources. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/enforcement-of-this-code/ [Accessed on 24 May 2024].

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S. & Janowski, T. (2020) Data governance: Organizing data for trustworthy Artificial Intelligence. *Government information quarterly* 37(3): 101493.

Kanade, V. (2023) What Is a Monte Carlo Simulation? Working, Applications, Pros, and Cons. Available from: https://www.spiceworks.com/tech/tech-general/articles/what-is-a-monte-carlo-simulation/ [Accessed on 26 May 2024].

Krutz, R. L., Vines, R. D., & Stroz, E. M. (2001) *The CISSP prep Guide: Mastering the ten domains of Computer Security*. 1st ed. New York: Wiley.

Kuzminykh, I., Ghita, B., Sokolov, V. & Bakhshi, T. (2021) Information security risk assessment. *Encyclopedia* 1(3): 602-617.

Li, G., Liu, M. & Zheng, H. (2022) Subsidization or diversification? Mitigating supply disruption with manufacturer information sharing. *Omega* 112: 102670.

Necat, B. (2022) *Business Continuity and Disaster Recovery* [Lecturecast]. SRM_PCOM7E March 2024. University of Essex Online.

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* 5(4): 1-18.

Rawool, A., Joshi, A. & Sayyed, S. (2020) Comparison Between Disaster Recovery As A Service Providers. *International Research Journal of Modernization in Engineering Technology and Science* 2(12): 1116-1120.

Rogers, B. (2016) Why 84% Of Companies Fail At Digital Transformation. Available from: https://www.forbes.com/sites/brucerogers/2016/01/07/why-84-of-companies-fail-at-digital-transformation/?sh=5bf4f1ad397b [Accessed on 24 May 2024].

Taylor, L. P. (2013) 'Performing the Business Risk Assessment', in: Taylor, L. P. (eds) *FISMA Compliance Handbook.* Oxford: Syngress. 201-220.

Tsarouhas, P. H. & Fourlas, G, K. (2015) Reliability and Maintainability Analysis of a Robotic System for Industrial Applications: A Case Study. *Int J Performability Eng* 11(5): 453-462.

Vaidya, R. (2018) *Cyber Security Breaches Survey 2018: Statistical Release.* Available from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018 [Accessed on 25 May 2024].

Wilson, M. (2022) Establishing RPO and RTO Targets for Cloud Applications. Available from: https://aws.amazon.com/blogs/mt/establishing-rpo-and-rto-targets-for-cloud-applications/ [Accessed on 27 May 2024].

Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van der Merwe, J. & Venkataramani, A. (2010) 'Disaster recovery as a cloud service: Economic benefits & deployment challenges', *2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10)*. Boston, 22-25 June. 1-7.

Zerto (2022) DRaaS eBOOK 101. Available from:
https://www.zerto.com/wp-content/uploads/2022/09/DRaaS-101_eBook.pdf [Accessed on 27 May 2024].