NAVIGATING RISKS IN BUSINESS DIGITALISATION AND INTERNATIONAL EXPANSION

A CASE STUDY OF PAMPERED PETS

This report presents a comprehensive risk assessment for Pampered Pets, a company undergoing digital transformation and international expansion. The study uses Monte Carlo simulations in Python and Excel to evaluate critical risks such as product quality issues, supply chain disruptions, and cybersecurity threats. Detailed analysis is conducted using Python's advanced capabilities to simulate thousands of potential scenarios, offering insights into the probability and impact of each risk factor. The findings highlight high-probability risks like logistical delays and cybersecurity attacks, proposing mitigation strategies through a multi-cloud disaster recovery (DR) solution involving AWS and Microsoft Azure. The report emphasises the importance of avoiding vendor lock-in by utilizing cloud-agnostic tools like Terraform and integrating third-party DRaaS providers like Veeam or Zerto. The recommended strategies aim to ensure business continuity, operational resilience, and data protection in a highly automated and internationalized business environment.

Word Count: 2160

David Abiodun

Navigating Risks in Business Digitalisation and International Expansion: A Case Study of Pampered Pets

Introduction:

As Cathy’s business embarks on its digitalisation journey, including adding an international supply chain and multiple automated warehouses, it presents opportunities and risks. While these changes offer efficiency and global reach, concerns regarding product quality, supply chain security, and overall operational continuity arise. High-profile customers such as HRH the King and Prince Albert II of Monaco have expressed concerns about potential disruptions. This executive summary assesses these risks using Monte Carlo simulations. It recommends mitigating them through disaster recovery (DR) strategies, leveraging AWS and Microsoft Azure to avoid vendor lockin.

Assumptions

The probabilities used in the Monte Carlo simulation were based on my 30 years of experience, current cybersecurity trends, and industry threat reports such as those from IBM, Symantec, and Verizon’s Data Breach Investigations Report. Known vulnerabilities like API exploits, phishing, and weak credentials were qualitatively assessed to estimate the likelihood of each risk event. Additionally, AI-generated insights informed the probability distributions without historical data. These assumptions allowed for a realistic risk assessment prioritising mitigation strategies based on observed and potential threats. (OpenAI, 2024).

Methods: Monte Carlo Simulation in Python

A Monte Carlo simulation was initially conducted in Excel for basic risk modelling, but I later transitioned to using Python in Jupyter Notebook for more advanced probabilistic analysis. This shift allowed for a more detailed and comprehensive risk evaluation, leveraging Python's capabilities to simulate thousands of potential scenarios and provide a deeper understanding of the risks involved. Combining both approaches ensured a thorough assessment, but the results were derived from the more advanced Jupyter simulation.

Monte Carlo Simulation in Python (Jupyter Notebook):

For more complex risk modelling, the NumPy library in Python was used to simulate and analyse thousands of potential outcomes. Using Jupyter Notebook, we created probability distributions for each risk factor and ran 10,000 simulations for each risk category.

Python’s ability to handle larger datasets allowed us to model more intricate relationships between risk factors, such as cybersecurity threats and supply chain disruptions, which could be modelled as correlated events.

How It Works in Python:

Using the numpy.random module, we generated random samples from probability distributions to simulate outcomes. Each simulation iterated through scenarios where different combinations of risks (e.g., delays, cybersecurity breaches) were triggered or not, allowing us to compute expected risk values and standard deviations.

The simulation results were visualised using Matplotlib to create detailed risk severity charts and bar graphs, helping visualise which risks are the most critical to Pampered Pets’ operations.

Justification for Method Used:

This report employed Monte Carlo simulation Python with Jupyter Notebook to model the risks associated with Pampered Pets' business expansion. This approach was chosen to ensure a robust and comprehensive analysis of the risks, capitalising on the tool's strengths while addressing the specific requirements of the case.

Monte Carlo Simulation in Python (Jupyter Notebook):

While Excel is excellent for basic modelling, Python with Jupyter Notebook offers greater flexibility, speed, and the capacity to handle more complex and larger-scale simulations. Using Python, we ran 10,000 iterations—far more than Excel's feasible range while modelling more intricate relationships between different risk factors.

<u>Scalability and Advanced Analytics:</u> Python’s NumPy library and random number generation functions enable more sophisticated simulations incorporating larger datasets and more complex dependencies between risks. Research by (Raschka et al., 2020) shows that Python’s computational capabilities make it particularly well-suited for high-dimensional risk simulations that require precision and scalability.

<u>Data Visualisation and Integration:</u> Python's Matplotlib library was utilised to generate clear and detailed charts, enabling better analysis and presentation of results. Jupyter Notebook allows for easy integration of these visualisations, making it an excellent tool for conducting in-depth risk assessments while maintaining transparency of the code and methods used (Allen et al., 2021).

Flexibility for Custom Models: Python allowed for creating custom probability distributions for each risk factor, making it possible to correlate risks such as cybersecurity threats and supply chain disruptions—a level of complexity that would be challenging to achieve in Excel. (Perez et al., 2011) Python's flexibility in modelling non-linear relationships between risk variables makes it indispensable for modern risk analysis.

Justification for Approach:

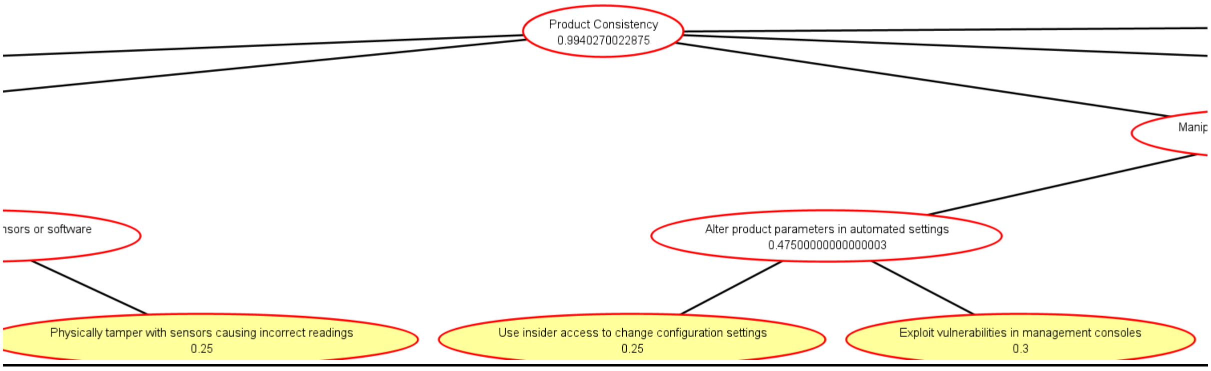
Python was chosen for the simulation because it efficiently handles complex, large-scale risk analysis. Its advanced libraries, like NumPy and SciPy, enabled the creation of detailed models, ensuring validation and accuracy by simulating thousands of scenarios and capturing dependencies between variables. The multi-level approach facilitated basic and granular risk assessments, offering a comprehensive view of potential outcomes. Python's computational power and flexibility, combined with visualisation tools like Matplotlib, allowed for high-precision analysis and consistent results, aligning with the project's analytical needs

Risk Assessment Approach

Risk Identification and Quantitative Modelling

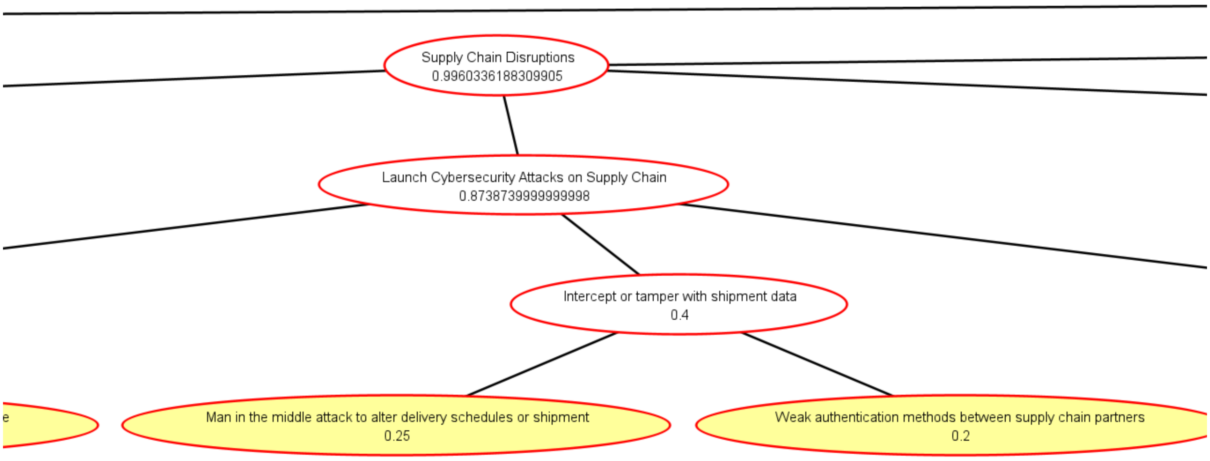
We have identified two critical areas of risk: product quality risks due to automation and supply chain risks resulting from international operations. Quantitative modelling techniques, including Failure Modes and Effects Analysis (FMEA) and Risk Based Supply Chain Management (RBSM), are used to assess these risks comprehensively.

Product Quality Risks:

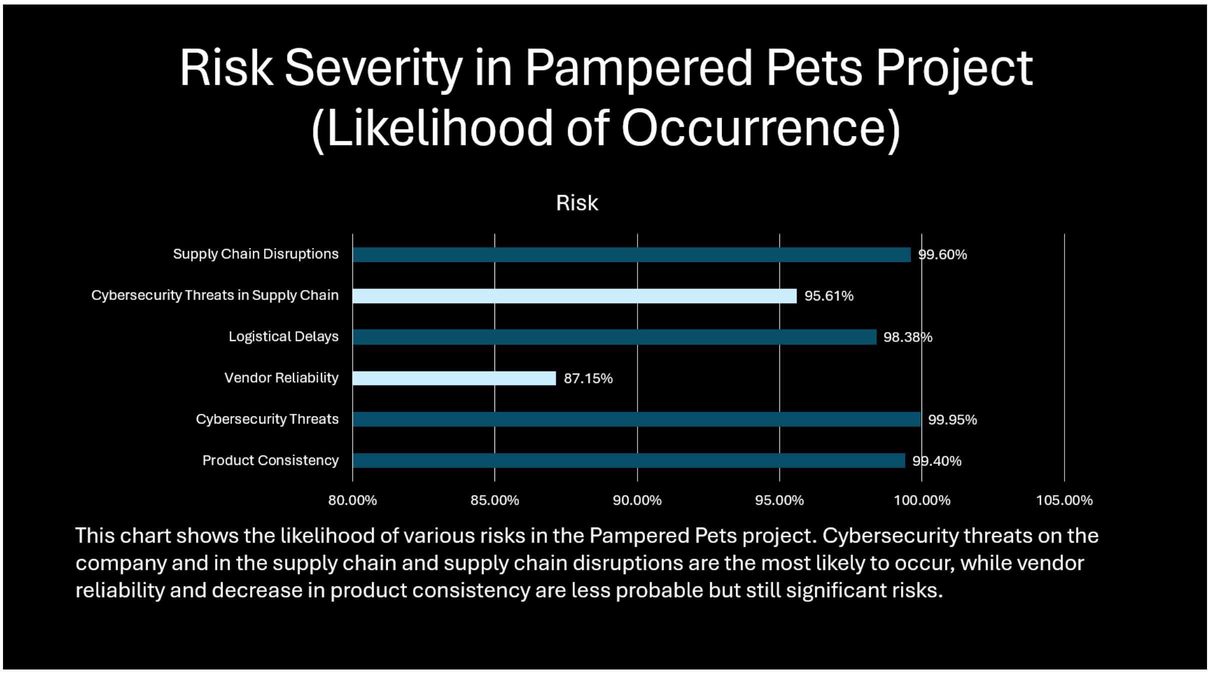

Product Consistency
0.9940270022875
Manip
nsors or software
Alter product parameters in automated settings
0.47500000000000003
Physically tamper with sensors causing incorrect readings
0.25
Use insider access to change configuration settings
0.25
Exploit vulnerabilities in management consoles
0.3

Automation presents a substantial risk to product consistency due to vulnerabilities in quality control systems and software. The FMEA model assesses these risks by assigning a Risk Priority Number (RPN) based on severity, occurrence, and detectability. According to the attack tree analysis, tampering with quality control systems carries a 70.9% likelihood, while modifying quality monitoring algorithms poses a 51% risk. Additionally, exploiting vulnerabilities in automated processes, such as altering product parameters, has a 73.12% likelihood. While automation increases operational efficiency, these risks could lead to significant product inconsistencies that would negatively affect a company's premium reputation, particularly in industries that rely on high product quality and reliability standards. These risks, highlighted in enterprise risk management literature, emphasise the importance of robust controls and monitoring systems to safeguard product quality (Fraser and Simkins, 2016).

Supply Chain Risks:


Supply Chain Disruptions
0.9960336188309905
Launch Cybersecurity Attacks on Supply Chain
0.8738739999999998
Intercept or tamper with shipment data
0.4
e
Man in the middle attack to alter delivery schedules or shipment
0.25
Weak authentication methods between supply chain partners
0.2

International supply chains face various risks, including customs delays, shipping disruptions, and political instability. Based on Monte Carlo simulation and attack tree analysis, logistical delays were found to have a 98.38% likelihood, indicating a high probability of occurrence in the supply chain risk landscape, with cybersecurity threats contributing to a 99.96% likelihood of disruption, the risk posed by malicious cyber activities is nearly specific within the supply chain risk landscape. Spoofing attacks targeting the supply chain have a 71.2% likelihood of success, with the most common vector being phishing emails targeting supply chain personnel (40% likelihood). Additionally, threats like man-in-the-middle attacks on delivery schedules (25%) and exploiting weak authentication methods between supply chain partners (20%) further contribute to the overall risk of disruption. These findings align with established literature on supply chain vulnerabilities, emphasising the need for robust cybersecurity measures (Cagliano et al., 2012).



Risk Severity in Pampered Pets Project (Likelihood of Occurrence)

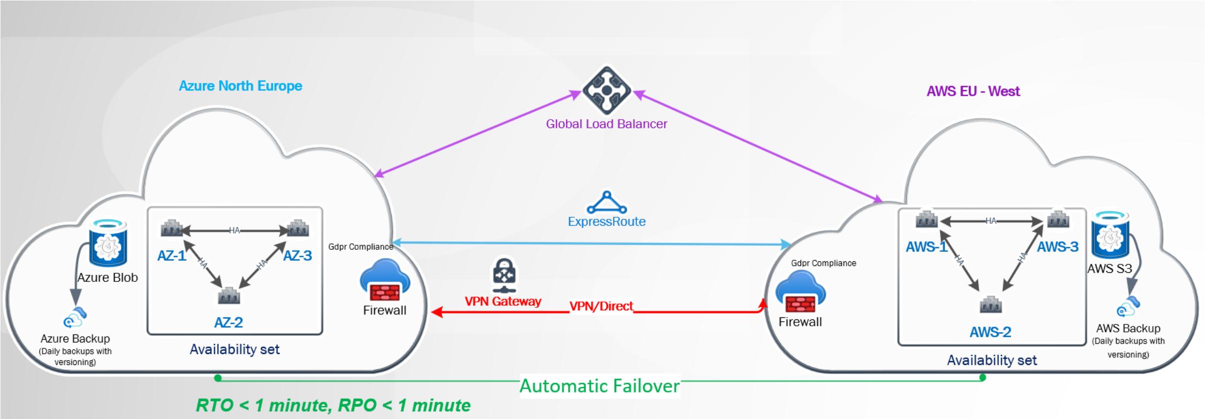
This chart shows the likelihood of various risks in the Pampered Pets project. Cybersecurity threats on the company and in the supply chain and supply chain disruptions are the most likely to occur, while vendor reliability and decrease in product consistency are less probable but still significant risks.

The Risk Severity Chart shows the most significant risks facing Pampered Pets, with supply chain disruptions (99.6%), cybersecurity threats (99.96%), Cybersecurity threats in supply chains (95.61%) and logistical delays (98.38%) being the most critical. These findings indicate that mitigating these risks should be prioritised.

Business Continuity and Disaster Recovery Strategy

Ms. O'dour's requirements for a DR plan necessitate 24/7 availability of the online shop with a changeover window of less than 1 minute in the event of a disaster. Additionally, the business must not lose more than 1 minute of data during a disruption.

Cloud-Based Disaster Recovery Solution

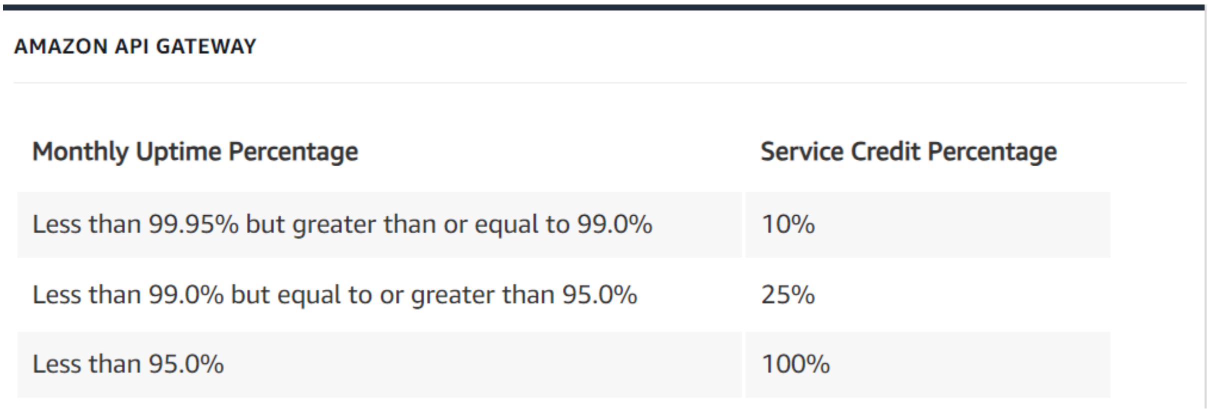


Multi-Cloud Approach

The proposed disaster recovery (DR) plan for Pampered Pets uses a multi-cloud approach with AWS and Azure to meet Ms. O'dour's strict requirements. For a 1-minute RTO, real-time data replication across geographically distributed data centres ensures immediate failover. Load balancing and automated failover via AWS Elastic Load Balancer and Azure Traffic Manager allow seamless transitions with minimal downtime.

To meet the 1-minute RPO, continuous backups and real-time synchronisation using AWS RDS Multi-AZ and Azure SQL Failover Groups ensure data is replicated instantly, minimising the risk of data loss. Both platforms provide cross-region replication and frequent snapshots, ensuring up-to-date data is always available.

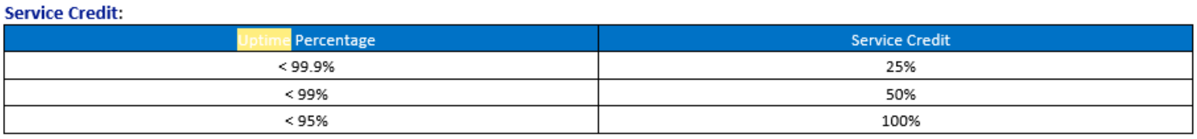
This strategy avoids vendor lock-in by using cloud providers and cloud-agnostic tools like Terraform, ensuring resilience and scalability while maintaining compliance with strict uptime and data protection standards.



AMAZON API GATEWAY

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but greater than or equal to 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

AWS provides a service credit if uptime falls below 99.9%, offering 25% credit for uptime between 99% and 99.9% and 100% credit for uptime below 95%.



Service Credit:

Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Similarly, Azure guarantees a 99.9% uptime, ensuring service credits are available even in rare cases of downtime as compensation for unfulfilled SLAs (as shown in the image).

Combining these two providers ensures a reliable, highly available infrastructure, maximising operational uptime.

<u>Service Allocation</u>

AWS will manage the active data storage and handle the bulk of user traffic, while Azure will be responsible for real-time data replication and disaster recovery. This setup ensures that even in the event of a failure in one service, the other can immediately take over with less than 1 minute of downtime.

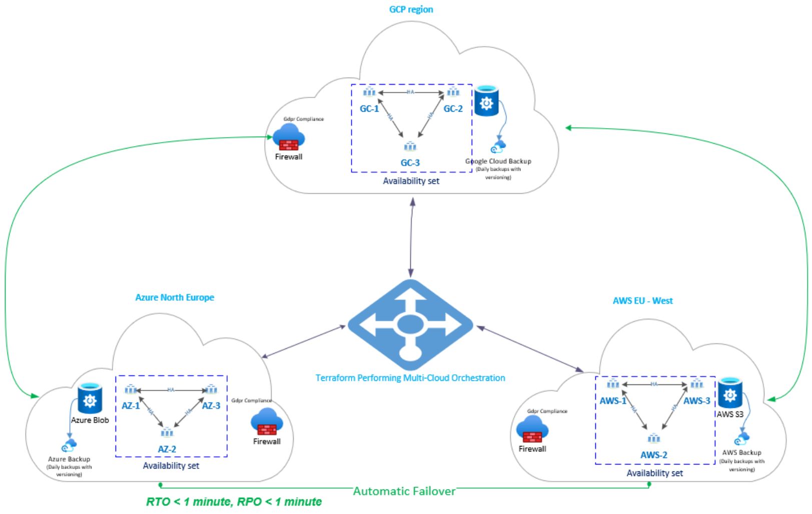
Avoiding Vendor Lockin

Using both AWS and Azure avoids vendor lockin by distributing services across providers. This reduces the risks associated with depending on a single provider and allows for competitive pricing.

Critical analysis

Multi-cloud solutions provide flexibility and resilience but come with added complexity and costs. Cloud-agnostic tools like Terraform help businesses minimise lock-in risks while managing multiple providers. However, organisations must balance cost efficiency, security, and ease of management based on their disaster recovery (DR) needs (de Carvalho and de Araujo, 2020).

A multi-cloud strategy with cloud-agnostic tools offers a mix of resilience and flexibility. Incorporating Google Cloud Platform (GCP) alongside AWS and Azure diversifies infrastructure. GCP provides scalable storage, robust security, and real-time performance suited for high availability, though it may trail AWS in RAM speed and performance. GCP remains a competitive option for high-demand applications due to its pricing and ability to handle HTTP requests (Kaushik et al., 2021).



Google Cloud’s backup and DR tools, cross-region replication, and support for Terraform further enhance its appeal for comprehensive DR strategies. While AWS is generally cheaper, GCP remains competitive, especially for general-purpose instances (Kaushik et al., 2021).

Third-party DRaaS providers like Veeam and Zerto offer specialised disaster recovery services that automate failover and replication processes. Though they may add costs and complexity, integrating DRaaS with a multi-cloud strategy, including GCP, AWS, and Azure, creates a flexible and resilient DR environment tailored to organisational needs.

Recommendations

1. Enhanced Cybersecurity Measures:

Phishing Attacks: Attackers deceive employees into revealing sensitive information via emails or messages.

Mitigation: Implement email filtering solutions and conduct regular phishing awareness training.

Ransomware: Cybercriminals encrypt critical data and demand a ransom.

Mitigation: Ensure frequent data backups and deploy patch management to address vulnerabilities.

DDoS Attacks: Attackers flood systems with traffic to cause downtime.

Mitigation: Use cloud-based DDoS protection and traffic monitoring tools to prevent service disruptions.

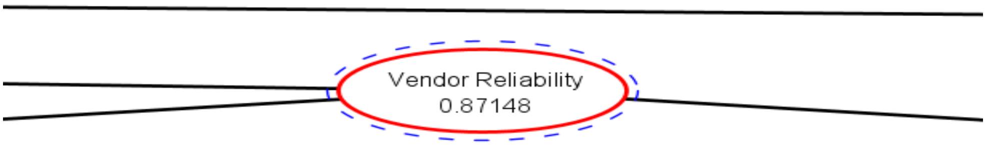
Advanced Persistent Threats (APTs**):** Long-term attacks aimed at stealing sensitive data while remaining undetected.

Mitigation: Deploy real-time monitoring and adopt a zero-trust security framework to detect anomalies.

Zero-day Exploits: Attackers exploit unknown vulnerabilities in software or hardware.

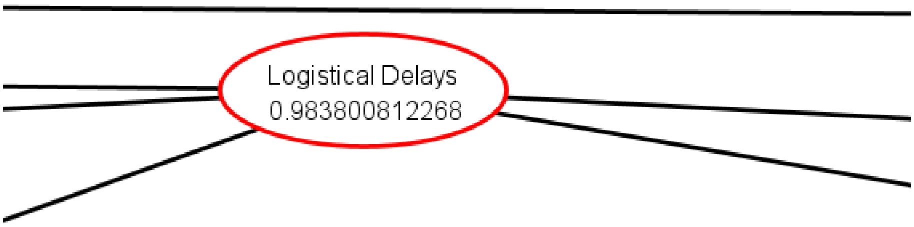
Mitigation: Strengthen patch management and invest in threat intelligence for early vulnerability detection.

2. Diversification of Suppliers:



Pampered Pets should diversify its supplier base across multiple geographic regions to mitigate the 12.85% risk of vendor unreliability, as indicated by the 87.15% reliability score. Mitigation: By sourcing from multiple vendors, especially in different locations, Pampered Pets can reduce its dependence on any single supplier and minimise the impact of regional disruptions, ensuring consistent operations.

3. Logistics Partnerships:



Pampered Pets should partner with logistics providers experienced in handling potential challenges to address the 1.62% probability of logistical delays, as indicated by the 98.38% reliability score.

Mitigation: By establishing preferred customs clearance processes and contingency plans, Pampered Pets can further reduce the already low risk of delays, ensuring smoother and more efficient shipment handling.

4. Continuous Data Replication:

Pampered Pets should ensure real-time data replication across AWS and Azure datacentres to minimise the risk of data loss and reduce recovery time in disaster situations.

Mitigation: Real-time replication allows for quick failover to secondary data centres, ensuring business continuity and minimising downtime, even during data centre outages or regional failures.

Conclusion

Pampered Pets' digital transformation and international expansion bring inherent risks, particularly in product quality and supply chain disruptions. However, these risks can be effectively managed through robust business continuity planning, utilising a multi-cloud disaster recovery strategy across AWS and Azure, and implementing enhanced cybersecurity protocols. The quantitative analysis demonstrates that Pampered Pets can continue delivering high-quality products while expanding its global footprint with the appropriate risk mitigation strategies.

Bibliography:

Anderson, J.A., Glaser, J. and Glotzer, S.C. (2020) HOOMD-blue: A Python package for high-performance molecular dynamics and hard particle Monte Carlo simulations. *Computational Materials Science*, *173*,109363 https://doi.org/10.1016/j.commatsci.2019.109363 [Accessed 06/10/2024].

Farrance, I., & Frenkel, R. (2014) Uncertainty in measurement: a review of monte carlo simulation using Microsoft Excel for the calculation of uncertainties through functional relationships, including uncertainties in empirically derived constants. *The Clinical Biochemist. Reviews*, *35*(1), 37–61.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3961998/ [Accessed 06/10/2024].

Raschka, S., et al. (2020) Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence. *Information*, 11(4),193. Available at: [Accessed 04/10/2020].

Gedam, S.G. and Beaudet, S.T. (2000) *Monte Carlo simulation using Excel® spreadsheet for predicting reliability of a complex system*. Motorola Satellite Communications Group. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=816305 [Accessed: 07/10/2024].

Allen, M., Poggiali, D., Whitaker, K., Marshall, T.R., van Langen, J. and Kievit, R.A. (2021) Raincloud plots: a multi-platform tool for robust data visualisation [version 2; peer review: 2 approved]. Wellcome Open Research, 4:63. Available at: https://doi.org/10.12688/wellcomeopenres.15191.2 [Accessed 07/10/2024].

Perez, R.E., Jansen, P.W. and Martins, J.R.R.A. (2011) pyOpt: a Python-based object-oriented framework for nonlinear constrained optimization. Structural and Multidisciplinary Optimization, 45(1),101-118. https://link.springer.com/article/10.1007/s00158-011-0666-3 [Accessed 04/10/2024].

Matthews, J., Love, P.E.D., Porter, S.R., & Fang, W. (2022) Smart data and business analytics: A theoretical framework for managing rework risks in mega-projects. International Journal of Information Management, 62, 102495. Available at: https://doi.org/10.1016/j.ijinfomgt.2022.102495 [Accessed 04/10/2024].

Fraser, J.R.S. and Simkins, B.J. (2016) The challenges of and solutions for implementing enterprise risk management. Business Horizons, 59(6), 689-698. Available at: https://www.sciencedirect.com/science/article/pii/S000768131630057X [Accessed 07/10/2024].

Cagliano, A.C., De Marco, A., Grimaldi, S. and Rafele, C. (2012) An integrated approach to supply chain risk analysis. Journal of Risk Research, 15(7), 817-840. Available at: https://doi.org/10.1080/13669877.2012.666757 [Accessed 07/10/2024].

AWS Service Level Agreements https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=*all [Accessed 06/10/2024].

Microsoft Service Level Agreement for online services https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services [Accessed 06/10/2024].

de Carvalho, L.R. and de Araujo, A.P.F. (2020) Performance Comparison of Terraform and Cloudify as Multicloud Orchestrators. *IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*, 380-389. doi:10.1109/CCGrid49817.2020.00-55. [Accessed 06/10/2024].

Kaushik, P., Vashisht, S., Rao, A.M., Gupta, S. and Singh, D.P. (2021) Cloud computing and comparison based on service and performance between Amazon AWS, Microsoft Azure, and Google Cloud. *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 268-273. DOI: 10.1109/ICTAI53825.2021.9673425. [Accessed 06/10/2024].

OpenAI (2024) ChatGPT. Available at: https://www.openai.com [Accessed: 12 October 2024].

Appendices

Monte Carlo Simulations (Zipped file)

Attack Tree ADT file

Attack Tree PDF

DR for Pampered pets Visio file

DR for Pampered pets Critical Review Visio File