# Assessment 2: Executive Summary

**Course Name**: MSc Cyber Security

**Module Name**: Security and Risk Management

**Submission date: 13/10/2025**

**Word Count – 1993**

## Contents

# Executive Summary – Pampered Pets

## 1. Introduction

This report has two concerns. The first is to perform a quantitative risk assessment on the effects of digitalisation, moving to an international supply chain and adding global automated warehouses, on the quality and availability of Pampered Pet's products. This will be followed by mitigations for these risks and recommendations for future strategy. The second is to propose a business continuity and disaster recovery solution that will maintain an online presence for the company regardless of the situation, accompanied by implementation recommendations.

## 2. Quantitative Risk Analysis

### 2.1. Methodology

Initial consideration was given to performing an overview of the risk situation in the sector. This was achieved via literature review, combining academic papers, benchmarks and risk reports from industry leaders, and general risk reports from world bodies.

Several key impact areas emerged:

- Economic Uncertainty (World Economic Forum [WEF], 2025; Tovee, 2025)
- Geopolitical Tensions (WEF, 2025; Tovee, 2025)
- Cyber Attacks (WEF, 2025; Tovee, 2025)
- Data Issues (Rodríguez García, Betts and Ponce, 2025)
- Standards and Practices (Alicke, Foster and Trautwein, 2025; Tovee, 2025)

From here more specific risks related to pet food supply chains and storage companies were selected: Exchange rate fluctuation, supply delivery delays, product defects, automation failures, and differing global values on data and regulatory requirements.

Some assumptions about the company were made. It was determined that the country of origin for vendors should be between Germany, Thailand and the USA, as they are among the top exporters of pet food (Tendata, 2024). A contract showing £50,000 monthly orders, valued at £1,800,000, was set as the base for analysis.

Next, research was done to find statistics on possible risks. This proved to be challenging, as exact numbers on most risks were not available. One risk, exchange rate fluctuations, did have concrete data available.

Historical yearly averaged exchange rates were taken for all three potential supply regions for the past decade (OFX, 2025). The highest, lowest and mode rates were put into a Python program running a Monte Carlo Simulation with triangular distribution (Appendix A), adapted from a base code (Geeks for Geeks, 2025). The results returned a graph showing the mean, higher and lower boundaries, and returned values from the program were compared to the base contract to check probability of excess and the average excess (Appendices B, C and D).

Where precise data was not available, estimates were made based on assumptions on the literature review as to the probability and financial impact of selected risks, leading to an Expected Monetary Value (EMV). These individual EMV's were combined to give a total risk EMV.

Monte Carlo simulations were used as they are a method of testing severity and frequency of event occurrences; useful for risk management (Deleris and Erhun, 2005). However, the simulation will only produce useful results from accurate data (Velikova, Mileva and Naseva, 2024).

## 2.2. Results

### 2.2.1. Monte Carlo Simulation Results for Exchange Rate Fluctuations over whole contract.

| Currency | Mean | Higher | Lower | Probability of Exceeding Base | Average Excess |
|---|---|---|---|---|---|
| Euro | **£1,801,099** | **£1,853,062** | **£1,749,373** | **52%** | **£25,276** |
| US Dollar | **£1,804,363** | **£1,927,924** | **£1,681,628** | **52%** | **£60,073** |
| Thai Baht | **£1,807,546** | **£1,977,113** | **£1,639,156** | **53%** | **£82,606** |

### 2.2.2. Risk Chart with EMV for annual risk.

| Risk | Probability | Impact | EMV |
|---|---|---|---|
| Port / Customs Delays (Stockout issues, perishability) | **80%** | **£1000** | **£800** |
| Product Issues (Defect, Standards etc.) | **8%** | **£20,000** | **£1600** |
| Supply Chain Disruption (Conflicts, Strikes, Rerouting) | **2%** | **£50,000** | **£1000** |

| | | | |
|---|---|---|---|
| **Automated Warehouse Failure (Stockout, Perishability, Repairs)** | 10% | £10,000 | £1000 |
| Cyberattack (Ransomware, DoS, data breach) | **5%** | **£100,000** | **£5000** |
| GDPR Breach (Cloud migration across regions, improper data handling) | **5%** | **£100,000** | **£5000** |

**Yearly Total Risk EMV = £14,400.**

## 2.3 Mitigations

| Risk | Mitigation |
|---|---|
| **Exchange Rate Flux** | Multiple suppliers to balance risk of one currency.<br>Negotiate a contract unaffected by positive or negative fluctuations. |
| **Port Delays** | Stock buffer in initial order.<br>Compliance officer for customs regulation adhereance. |
| **Product Issues** | Due diligence checks on suppliers, including on-site, with regular checks.<br>Strict Service and Licensing Agreements (SLAs). |
| **Supply Chain Disruption** | Multiple suppliers.<br>Multiple supplier regions.<br>Consider multiple delivery methods (e.g. sea and air) |
| **Automated Warehouse Failure** | Use an automated Warehouse Management System (WMS).<br>Regular maintenance and equipment checks. |
| **Cyberattack** | Defined and comprehensive cybersecurity strategy.<br>Proper data storage. |
| **GDPR Breach** | Defined and Comprehensive Data Storage and Handling strategy. |

## 2.4. Recommendations

- **Hire a dedicated cybersecurity officer –** Source of high potential risk. Responsible for implementing cybersecurity strategy, conducting security training.
- **Hire a dedicated regulatory compliance officer –** Source of high potential risk. Regulations change regularly, and the company will move into new territories with new regulations.
- **Adopt a multi-supplier strategy across regions –** Proactively guard against problems. In this case, if the company has a low-risk appetite it should select Germany, and US-based suppliers on contracts that eliminate the risk of fluctuations in exchange rates. If a high-risk appetite, then Germany and Thailand based suppliers on contracts with no provisions for limiting currency changes.
- **Develop a standard SLA and Operating Requirements for Partners –** Set minimum expectations from all companies with links to the business. These agreements should cover delivery times, quality controls, meeting regulations etc.
- **Implement a WMS system –** tracks inventory, gives real time updates, leading to better efficiency, reliability and reducing cost (Odeyinka and Omoegun, 2024).
- **Focus on quality –** Reports show quality of products and digitalisation affects customer satisfaction and retention rates, above brand awareness and availability (Kim and Yang, 2025).

# 3. Business Continuity and Disaster Recovery (BC/DR) Plan

## 3.1. Requirements

The BC/DR solution has been based around keeping Pampered Pets online shop operating despite the physical business premises being affected by a disaster. The Recovery Time Objective (RTO) and the Recovery Point Objective both need to be less than 1 minute.

## 3.2. Solution Considerations

To achieve this, several factors were considered:

### 3.2.1. Location

Backup systems can be in one or many other physical locations with most or all the setup of the primary premises. They receive backups of the data and applications and can be set to varying stages of readiness. These systems can exist in the cloud and is generally more flexible, faster and cheaper (Oluwasanmi, 2023).

As speed of recovery is paramount, a cloud-based solution is recommended. This will add geographic redundancy, something that will be increasingly important, given WEF (2025) warnings of increased risk of state-based armed conflict and adverse weather events. The solution should be a multi-cloud system, in case of primary backup failure, and multi-vendor in case of primary vendor failure.

### 3.2.2. Redundancy Type

Both active-active and active-passive redundancy types were considered. Active-active is constantly on and in the same state as the primary system, which means two or more systems operate concurrently. Active-passive is updated regularly but only becomes active when the original system fails. The constantly on feature of active-active makes for very low recovery time and extremely low data loss, although it comes with higher complexity and cost (Yadav, 2023).

### 3.2.3. Data Replication

Two types of data replication were considered – synchronous and asynchronous. Synchronous replication guarantees near zero data loss, matching RPO requirements, but latency can cause performance issues over longer distances. Asynchronous replication performs at higher speeds but can have some data loss (Natanzon and Bachmat, 2013).

Given our RPO and RTO requirements synchronous replication would be the most suitable choice. However, a hybrid of the two replications could be used, with flexible management. Synchronous could be used for all data that is deemed critical and asynchronous could be used for data that would not cause issues in case of a slower than required RTO. Geographical placement of the primary location could also lower the impact of latency. Having the primary data centre centralised between backup centres can avoid slow replication in more remote centres (Mendonca et al., 2019). The location of automated warehouses also must be strategized.

### 3.2.4. Monitoring and Automated Failover

Effective monitoring of business systems is a key aspect of the process. Having automated systems to monitor the network of on premises and warehouse activity will allow for early detection of problems requiring action. An automated failover would allow the recovery system to immediately take over operations. This would add resilience to the system, a core aspect of business continuity practices (Ali, Hanafiah and Mogindol, 2023).

### 3.2.5. Compliance

Providing the company does backup data in the cloud, at distributed locations, data protection rules and regulations must be considered.  Primarily this means being aware of United Kingdom General Data Protection Regulation (UK GDPR) standards, based on the Data Protection Act of 2018, however, with the company goes digital in general, and having global warehousing, the regulations of other jurisdictions must also be considered, as orders can come from any region.   This means that the GDPR standards of the European Union (EU) must be considered if customers are from the EU, or the Australia's Privacy Act of 1988 if they are from Australia.

Practiacally, for UKGDPR and GDPR, where most customers will be based, the primary concern with the solution is making sure the backups are in regions deemed acceptable.  Data flow between the UK and the EU is freely allowed (ICO, 2025), however for data transfer to outside those regions safeguards must be put in place (United Kingdom, 2018; European Union, 2016).

Therefore, the company must ensure that the backups are regionalised.  A compliance officer position should be created to evaluate the company's position and compliance processes as expansion continues.

### 3.2.6. Analysis

The overall BC/DR solution is a multi-cloud, active-active system, with synchronous, or hybrid backup.  This would allow the solution to meet the requirements on RPO and RTO.  The company should set up an automated monitoring system for immediate implementation.  A compliance officer should be hired to ensure data storage meets regulations.

The proposed infrastructure would be to have a Disaster Recovery as a Service (DRaaS) managed on premises set up, that can failover into the provider's cloud network.  A third tier of failure could be added to have a secondary DRaaS provider in case of failure in the primary provider.

## 3.3. Disaster Recovery as a Service Provider Recommendation

DRaaS is a solution offered by various companies that alleviates some of the burden on individual companies to manage all its own BC/DR systems.  There are various levels of service that are offered and a broad range of vendors.

Given the solution's requirements, Nutanix DRaaS service would be a good fit for the company.  It advertises effectively zero recovery time and data loss and has active-active setups across multiple sites or clouds (Nutanix, 2025).

The service was given a customer choice award by Gartner (2024), showing positive experiences from clients. Importantly, with the optimal solution requiring more than one vendor, Nutanix has a history of utilising software that lessens vendor lock-in and allowing platform integration (Bigelow, 2024). This should mean that adding a second provider would be simpler than with other companies.

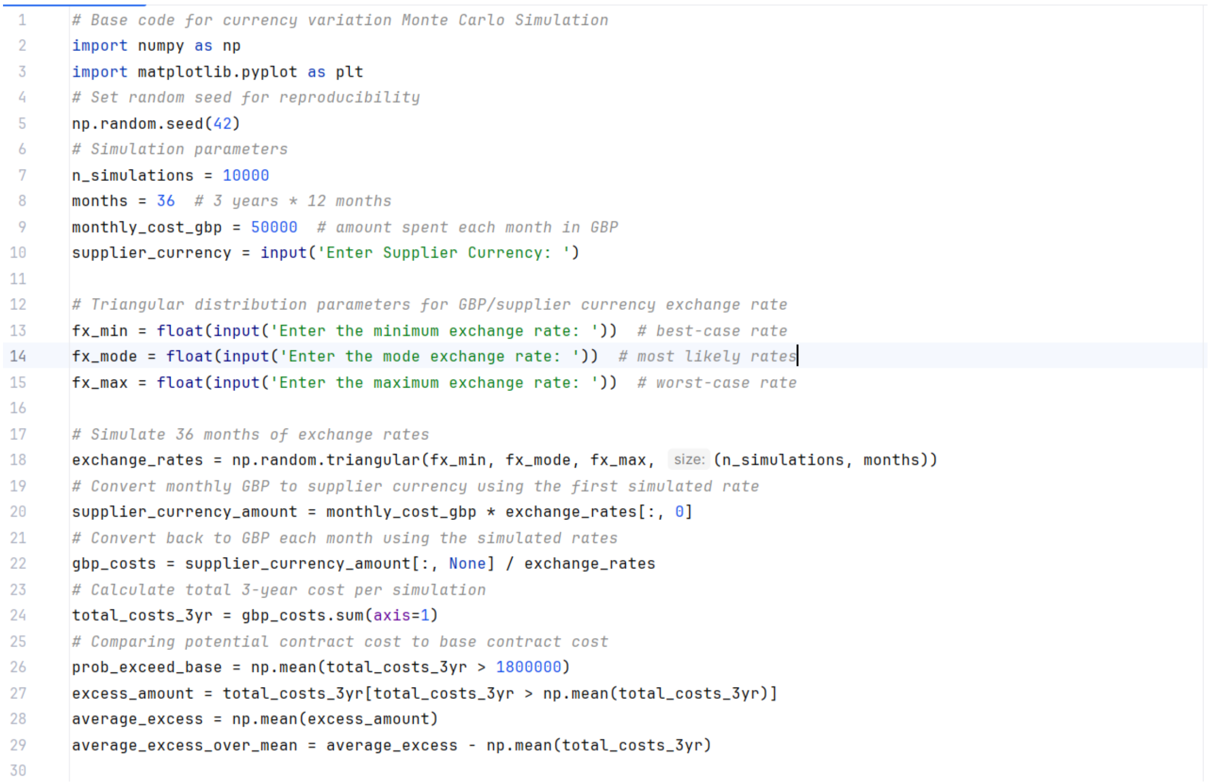
Nutanix partners with Amazon Workspaces (AWS), allowing customers to utilise many AWS features (Nutanix, 2024). This link makes AWS would be a good secondary backup DRaaS provider. However, many AWS features are proprietary and do contribute to vendor lock-in. This is an important factor in utilising the AWS solution; users should take care to limit use of these features.

# 4. Conclusion

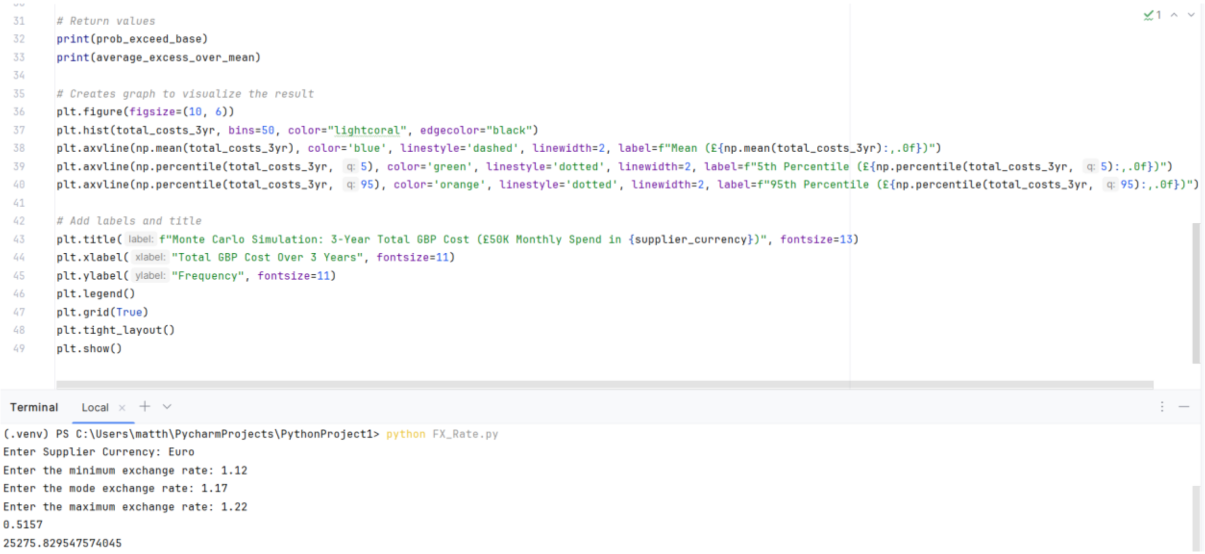
This report quantifies several risks of implementing an international supply chain with global automated warehousing and proposes a business continuity and disaster recovery solution. The risk report was conducted using Monte Carlo simulations and EMV, to give financial predictions. It recommends that a layered approach: multiple vendors and from different geographical areas should be used as mitigation, with the combination determined by the risk appetite of the company. Hiring cybersecurity and regulatory compliance officers was regarded as essential. The BC/DR plan followed a similar structure, with a multiple vendor, multiple backup cloud solution proposed. Nutanix was proposed as the primary vendor due to advertised metrics and positive reputation. AWS was proposed as the backup vendor due to its infrastructure and links to Nutanix. The need for the business to hire a compliance officer was repeated due to the expected increase in international customers and the need to handle their data across cloud backup systems.

# 5. Appendices

## 5.1. Appendix A



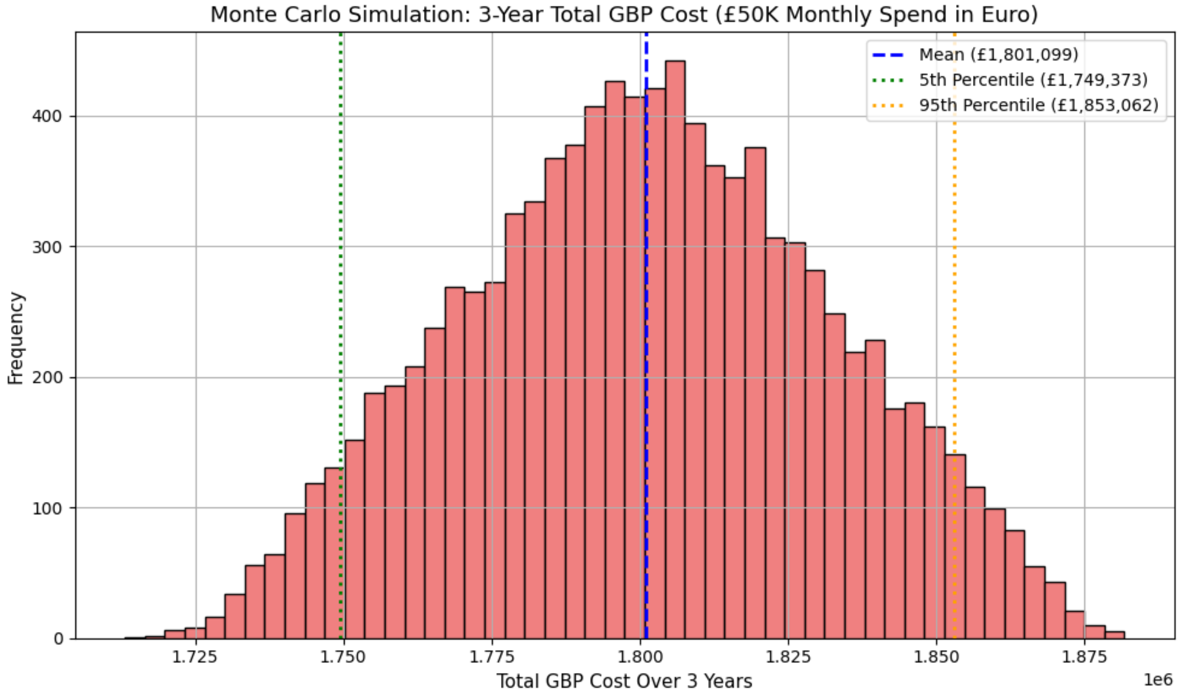
```
# Base code for currency variation Monte Carlo Simulation
import numpy as np
import matplotlib.pyplot as plt
# Set random seed for reproducibility
np.random.seed(42)
# Simulation parameters
n_simulations = 10000
months = 36  # 3 years * 12 months
monthly_cost_gbp = 50000  # amount spent each month in GBP
supplier_currency = input('Enter Supplier Currency: ')

# Triangular distribution parameters for GBP/supplier currency exchange rate
fx_min = float(input('Enter the minimum exchange rate: '))  # best-case rate
fx_mode = float(input('Enter the mode exchange rate: '))  # most likely rates
fx_max = float(input('Enter the maximum exchange rate: '))  # worst-case rate

# Simulate 36 months of exchange rates
exchange_rates = np.random.triangular(fx_min, fx_mode, fx_max,  size: (n_simulations, months))
# Convert monthly GBP to supplier currency using the first simulated rate
supplier_currency_amount = monthly_cost_gbp * exchange_rates[:, 0]
# Convert back to GBP each month using the simulated rates
gbp_costs = supplier_currency_amount[:, None] / exchange_rates
# Calculate total 3-year cost per simulation
total_costs_3yr = gbp_costs.sum(axis=1)
# Comparing potential contract cost to base contract cost
prob_exceed_base = np.mean(total_costs_3yr > 1800000)
excess_amount = total_costs_3yr[total_costs_3yr > np.mean(total_costs_3yr)]
average_excess = np.mean(excess_amount)
average_excess_over_mean = average_excess - np.mean(total_costs_3yr)

```



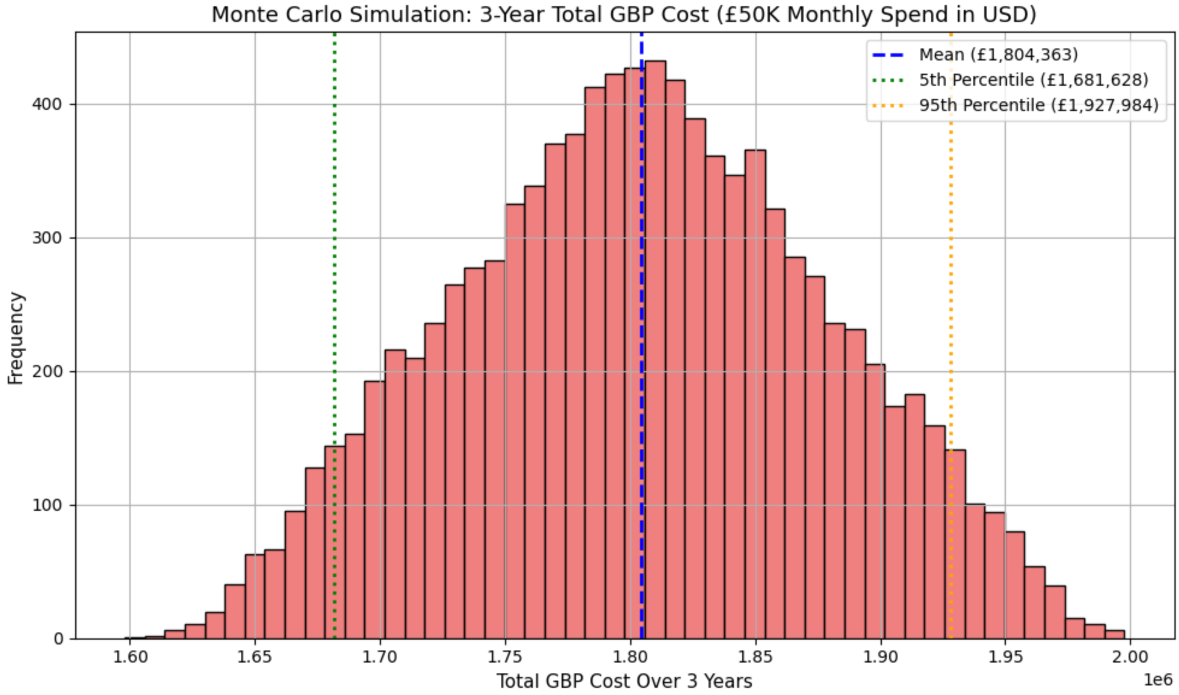
```
# Return values
print(prob_exceed_base)
print(average_excess_over_mean)

# Creates graph to visualize the result
plt.figure(figsize=(10, 6))
plt.hist(total_costs_3yr, bins=50, color="lightcoral", edgecolor="black")
plt.axvline(np.mean(total_costs_3yr), color='blue', linestyle='dashed', linewidth=2, label=f"Mean (£{np.mean(total_costs_3yr):,.0f})")
plt.axvline(np.percentile(total_costs_3yr,  q: 5), color='green', linestyle='dotted', linewidth=2, label=f"5th Percentile (£{np.percentile(total_costs_3yr,  q: 5):,.0f})")
plt.axvline(np.percentile(total_costs_3yr,  q: 95), color='orange', linestyle='dotted', linewidth=2, label=f"95th Percentile (£{np.percentile(total_costs_3yr,  q: 95):,.0f})")

# Add labels and title
plt.title( label: f"Monte Carlo Simulation: 3-Year Total GBP Cost (£50K Monthly Spend in {supplier_currency})", fontsize=13)
plt.xlabel( xlabel: "Total GBP Cost Over 3 Years", fontsize=11)
plt.ylabel( ylabel: "Frequency", fontsize=11)
plt.legend()
plt.grid(True)
plt.tight_layout()
plt.show()
```

```
(.venv) PS C:\Users\matth\PycharmProjects\PythonProject1> python FX_Rate.py
Enter Supplier Currency: Euro
Enter the minimum exchange rate: 1.12
Enter the mode exchange rate: 1.17
Enter the maximum exchange rate: 1.22
0.5157
25275.829547574045
```

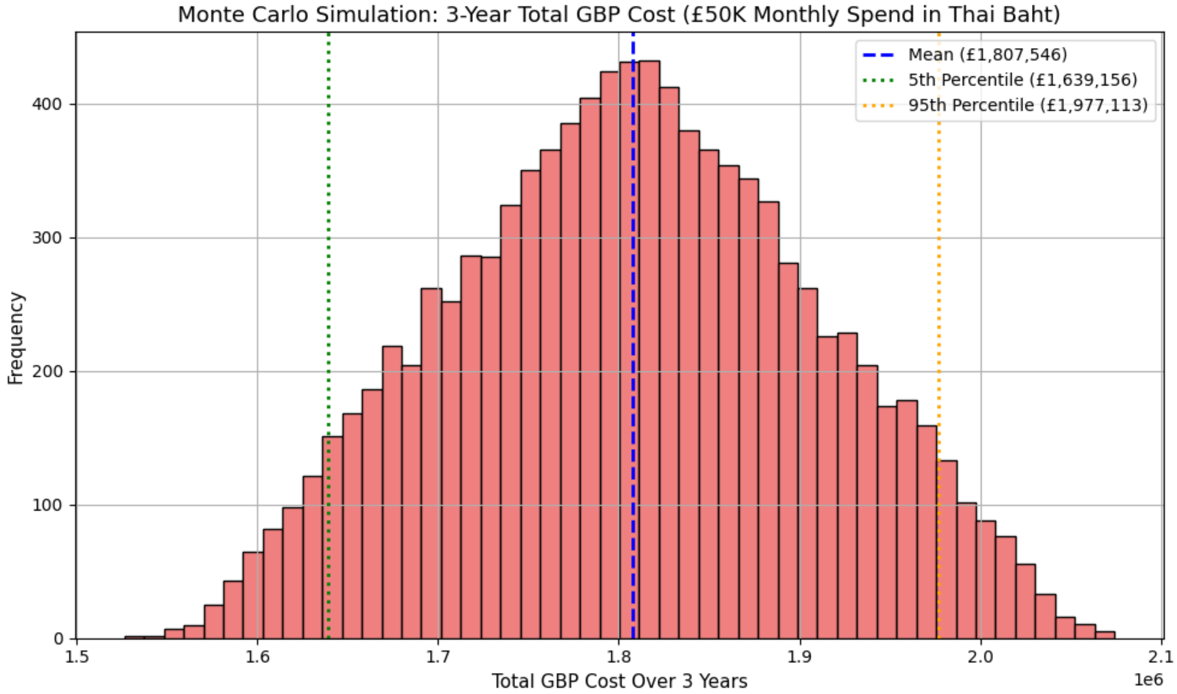
## 5.2. Appendix B



## 5.3. Appendix C



## 5.4. Appendix D



# 6. References

Ali, Q. S. A., Hanfiah, M. H. and Mogindol, S. H. (2023) ‘Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework’, *International Journal of Disaster Risk Reduction,* 99. Available at: https://doi.org/10,1016/j.ijdrr.2023.104135

Alicke, K., Foster, T. and Trautwein, V. (2024) *Supply Chains: Still Vulnerable*. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-risk-survey (Accessed 11 October 2025).

Bigelow, S. J. (2024) *What is hyperconverged infrastructure? Guide to HCI*. Available at: https://www.techtarget.com/searchdatacenter/definition/What-is-hyper-converged-infrastructure-Guide-to-HCI (Accessed 12 October 2025).

Deleris, L., A. and Erhun, F. (2005) ‘Risk management in supply networks using monte-carlo simulation’, *WSC '05: Proceedings of the 37th conference on Winter simulation,* Orlando, Florida, 4-7 December. Pp. 1643-1649. Available at: https://doi.org/10.5555/1162708.1162994

European Union. (2016) ‘Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation’, *Official Journal of the European Union,* L119. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed 12 October 2025).

Gartner. (2025) *Disaster Recovery as a Service Reviews and Ratings*. Available at: https://www.gartner.com/reviews/market/disaster-recovery-as-a-service (Accessed 12 October 2025).

Geeks for Geeks. (2025) *What is Monte Carlo Simulation?* Available at: https://www.geeksforgeeks.org/artificial-intelligence/what-is-monte-carlo-simulation/ (Accessed 13 October 2025)

Information Commissioner’s Office (ICO). (2025) *International Data Transfers.* Available at: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/ (Accessed 12 October 2025).

Kim, S. H. and Yang, Y. R. (2025). ‘The Effect of Digital Quality on Customer Satisfaction and Brand Loyalty Under Environmental Uncertainty: Evidence from the Banking Industry’, *Sustainability*, 17(8), 3500. Available at: https://doi.org/10.3390/su17083500

Mendonca *et al*. (2019) ‘Evaluating Database Replication Mechanisms for Disaster Recovery in Cloud Environments’, *2019 IEEE International Conference on Systems, Man* *and Cybernetics (SMC),* Bari, Italy. Pp. 2358-2363. Available at: https://doi.org/10.1109/SMC.2019.8914069

Natanzon, A. and Bachmat, E. (2013) 'Dynamic Synchronous/Asynchronous Replication', *ACM Transactions on Storage (TOS),* 9(3), pp. 1-19. Available at https://doi.org/10.1145/2508011

Nutanix. (2024) Nutanix Expands Partnership with AWS. Available at: https://www.nutanix.com/press-releases/2024/nutanix-expands-partnership-with-aws (Accessed 12 October 2025).

Nutanix. (2025) *Disaster Recovery Solutions*. Available at: https://www.nutanix.com/en_gb/products/nutanix-cloud-infrastructure/disaster-recovery?utm_medium=redirect#features (Accessed 12 October 2025).

Odeyinka, O. F. and Omoegun, O. G. (2024). 'Warehouse Operations: An Examination of Traditional and Automated Approaches in Supply Chain Management', In T. Banyai (ed) *Operations Management - Recent Advances and New Perspectives*. IntechOpen. Available at: http://dx.doi.org/10.5772/intechopen.113147

OFX. (2025) *Yearly Average Rates*. Available at: https://www.ofx.com/en-gb/forex-news/historical-exchange-rates/yearly-average-rates/ (Accessed 11 October 2025).

Oluwasanmi, R, A. (2023) 'Cloud vs Traditional Disaster Recovery Techniques: A Comparative Analysis', *International Advanced Research Journal in Science, Engineering and Technology,* 10(4). Available at: http://doi.org/0.17148/IARJSET.2023.10430

Rodríguez García, M., Betts, K. and Ponce, E. (2025*) Identifying the Key Vulnerabilities in the Warehouses of the Future*. Cambridge MA: MIT Center for Transportation and Logistics. Available at: https://ctl.mit.edu/pub/report/identifying-key-vulnerabilities-warehouses-future (Accessed 10 October 2025).

Tendata. (2024) *Global Pet Food Exports Countries*. Available at: https://www.tendata.com/blogs/insight/5996.html (Accessed 11 October 2025).

Tovee, E. (2025) *The Biggest Global Supply Chain Risks of 2025*. Available at: https://www.xeneta.com/blog/the-biggest-global-supply-chain-risks-of-2025 (Accessed 10 October 2025).

United Kingdom, (2018) *Data Protection Act 2018 c.12*. Available at: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/ (Accessed 11 October 2025).

Velikova, T., Mileva, N. and Naseva, E. (2024) 'Method "Monte Carlo" in healthcare', *World Journal of Methodology*, 14(3). Available at: https://doi.org/10.5662/wjm.v14.i3.93930

World Economic Forum. (2025) *The Global Risks Report 2025*. Available at: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf (Accessed 11 October 2025).

Yadav, G. (2023) ‘Architectural Approaches to Disaster Recovery and High Availability in SAP HANA Cloud’, *International Journal of Scientific Research and Modern Technology (IJSRMT),* 2(8). Available at: https://doi.org/10.38124/ijsrmt.v2i8.854