Development Team Project: Risk Assessment Executive Summary For Pampered Pets

SRM_PCOM7E

BY

GROUP 3

October 2023

Table of Content

Introduction……..…….....3

Executive Summary …….3

- Product Quality …….3
- Probability for Supply Chain Risk ……..4
- Summary Recommendation.……..…….…….…….4

Quantitative Analysis Justification……..…6

Monte Carlo simulation quality and supply chain risk categorisation ..……....7

- Random (Assumption) Data Collection and Preprocessing ..…..……..8
- Defining Parameters…… ……8
- Implementing the Monte Carlo Simulation..…….…….9
- Analysing the Simulation Results…… ……..……9
- Quality and Supply Chain using Monte Carlo simulation in Python…...9
- Visualising the distributions…….……10
- Monte Carlo Simulation Supporting Comments……..……..12

Summarised Cyber Risk Identification based on earlier report……..12

- Monte Carlo Simulation for Cyber Risk Assessment……13

Disaster Recover Choice……..14

Recommended Cloud Platform and Vendor Lock-in……15

Conclusion …….16

References …….18

Introduction

Following the ISO 31000 risk assessment model, we plan to align the business objectives with digitalisation technologies and enterprise risk management (ERM), automate the warehouse worldwide, coordinate and monitor the internal supply chain and balance the cost/benefit of IT security risks while ensuring proper disaster recovery plan (DRP) with available of 24/7/365 with a less than 1-minute changeover window. Monte Carlo Simulation is our chosen quantitative risk modelling approach for this exercise. Our presentation word count is 2,080.

Executive Summary

For the risk assessment of Pampered Pets (PP), we identified and evaluated the probabilities of potential changes to the operations of the business and supply chain that could endanger the quality and availability of PP's products.

We assumed dummy values and employed Monte Carlo probabilistic simulations to quantify the associated risks and several methodologies based on past works of literature on supply chain risk assessment.

Product Quality

We are working with the assumption that PP's products/materials are from a single source, the same production plant and distribution centres. Therefore, the probability of encountering product defects is relatively insignificant. We have considered factors such as potential financial losses per quality issue, the probability of encountering such issues, and standard deviations. The results show that the estimated mean potential

loss due to product quality issues is well below the threshold, demonstrating that the risk to product quality is effectively managed.

Probability for Supply Chain Risk

The supply chain risk assessment accounts for potential disruptions that could impact product availability. While the probability of such disruptions is relatively low (especially in the first 5 years), it is essential to maintain a strong focus on supply chain reliability. Our analysis considers factors like financial losses per disruption, service level, and standard deviations. The results indicate that the estimated mean potential loss due to supply chain disruptions is well within acceptable limits. However, if there are changes to Service Level (SL), it significantly affects the supply chain loss.

E.g if SL = 0.002, Supply_Chain_Reliability_Loss = £0

if SL = 0.02, Supply_Chain_Reliability_Loss = £ 5163.33 or £ 4975.68 (Probability changes).

We also noticed that the Mean Potential Loss due to Quality changes when there is a significant change in SL. Service Level is, therefore, a critical factor in ensuring customer perception of the quality and availability of the product.

Proactive management of risk, continued maturation, and implementation of the new GDPR directive to regulate the unlawful processing of data created by the Internet of Things (GDPREU, N.D.) will position PP for sustainable success while safeguarding product quality and availability.

Quick Recommendations

We recommend that the business does the following;

1. To ensure compliance with data privacy regulations, PP must conduct a comprehensive data mapping exercise, documenting all collected PII by PP's AI systems. Data collection must adhere to legal standards and be regularly updated. Minimise data collection to the essentials and follow GDPR's privacy-by-design principles (GOV UK, 2021). Continued training for employees and users is also vital.
2. Upgrade PP’s Warehouse Management System to a secure supply chain solution from Oracle, integrate the E-commerce Platform, and introduce a Mobile Application for operational efficiency and customer engagement. Strengthen physical security with CCTV, fencing, and safeguard IT equipment in a restricted access cupboard. Ensure comprehensive security features throughout the Software Development Life Cycle (SDLC), including dedicated Web Application Firewall, DMZ, Identity and Access Management, Log monitoring, load balancing, IDS/IPS etc.
3. Improve baseline security for all critical infrastructures
4. Implement a Business Continuity Plan (BCP) and Data Recovery Plan (DRP) to ensure data and system resilience. In ensuring 24/7/365 availability, there should be a Target RTO < 1hr; and Target RPO < 1m changeover window. A Blue-Green deployment should be implemented to easily invoke DR.
5. Automated Warehouse Worldwide prioritises quality, scalability, and compatibility using robotics, AI, and ML/Big data. Maintaining cybersecurity is essential. Adherence to the Security Policies and Guidelines is crucial, including technology systems and dependencies like APIs (Oracle WMS Cloud Product Team, 2023).

Robotic systems are prone to vulnerabilities impacting connectivity, productivity, operations, and accuracy (Yaacoub, et al., 2022).

6. Implement Quality Assurance measures to ensure that product quality remains world-famous and meets PP’s customers' expectations.
7. Adopt AWS cloud technologies (e.g. Identity and Access Management, VPC, Auto-scaling etc.) and ensure that industry standards for security are maintained by the DevOps engineering team with dedicated security personnel to carry out all the required testing and checks (DevSecOps).
8. Secure digital payment gateways following PCI-DSS guidelines. And yearly tests to verify that all systems and procedures are still complaints.
9. Regularly back up data and test the recovery process for business continuity and disaster recovery using the active-active availability solution to achieve PP’s DR Target RTO < 1hr; Target RPO < 1m.
10. Always on Executive stakeholders' buy-in at every stage of the digitisation process.

Quantitative Analysis Justification

Monte Carlo simulation is a powerful technique used in supply chain management (Ghafoor, R. (2023).) In our analysis, we believe this technique is robust enough to assess product quality and supply chain risks for PP due to its ability to model complex, probabilistic scenarios, providing insights into potential financial impacts and enhancing decision-making.

Additionally, we believe Cyber security risk probability calculation is critical for PP because if there is any risk of financial loss, disruption to operations, or damage to the reputation of PP due to the failure of its information technology (IT) systems (Shevchenko, et al., 2023) will affect the supply chain availability and even result in product defect.

Monte Carlo simulation quality and supply chain risk categorisation for Pampered Pet

We are considering the below risk factors (which are broadly divided into Product Quality and Supply Chain Reliability (Availability);

Category	**Input**
Product Quality	Product Defect
Distribution Centers	Demand distribution information Number of weeks' worth of finished goods inventory held
Service Level	The desired probability of meeting customer demand (SL)
Plants	Production time per product Maximum capacity for production Number of weeks' worth of pre-processed material inventory held

	Number of weeks' worth of post-processed inventory stored
Cost Component (Transportation)	Time to ship between plants or DCs Maximum capacity for shipments

Schmitt, A.J., & M. Singh (2009).

Random (Assumption) Data Collection and Preprocessing

All data used in this calculation will be based on assumptions over a given period. Our assumptions from the Risk Identification Report anticipate a 10% annual business growth and a 50% total increase in 5 years. Data preprocessing identifies patterns, trends, and seasonality, with a focus on technology and security.

Defining Parameters

Determine the key parameters for inventory management:

a. Service Level (SL): The desired probability of meeting customer demand. For example, SL = 98% indicates a target fill rate of 98%. The probability of Supply chain disruption = SL x 0.002
b. Product Quality (PQ): The desired quality of ensuring that the products are defect-free and meet PP's high-profile customers' world-famous quality securely. PQ = 99% indicates a target quality of 99%
c. Lead Time (LT): The time taken for customers to receive an order after placing it.

d. Demand Distribution: Analyse the historical demand data to determine the distribution that best represents the demand pattern (e.g., normal, Poisson, or empirical distribution).
e. Supply chain loss: Consider holding costs (H) associated with DC/Production Cost (PS) and average financial loss per disruption.

Ghafoor, R. (2023).

Implementing the Monte Carlo Simulation

We will generate random demand scenarios and random quality scenarios.

Repeat the simulation for a sufficient number of iterations to obtain reliable results.

Analysing the Simulation Results

a. Product Defect Rate (PD) = Number of Quality Products/Total Sold

b. Plant or DC Reliability (PR) = Supply chain reliability

c. Average Costs (AC) = Holding Costs + Production Costs

Below is an assumption and example of how the case study distributes potential risk to

Quality and Supply Chain using Monte Carlo simulation in Python:

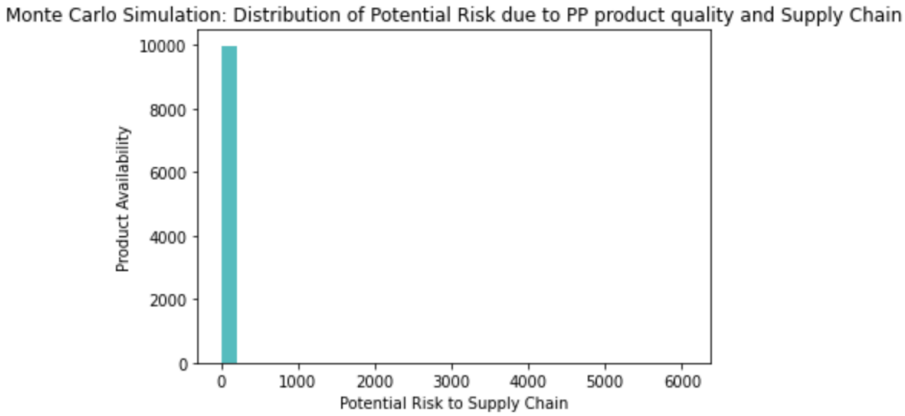
```python
import matplotlib.pyplot as plt
import random
import numpy as np

# Step 1: Forcast Data Preprocessing (Dummy values)
demand_data = [600, 710, 858, 681, 980, 890, 1001, 99, 1123, 900, 670, 809]  # monthly demand data

# Step 2: Defining quality parameters for Product Quality Issues (Dummy values)
product_quality_prob = 0.01  # Probability of product quality issues
product_quality_loss = 5000  # Average financial loss per quality issue in pounds
product_quality_std_dev = 1000  # Standard deviation for quality issues

# Step 3: Defining parameters for Supply Chain Disruptions/Inventory Cost Component (Dummy values)
service_level = 0.002  # Probability of supply chain disruptions leading to failed SL
supply_chain_reliability = 65000  # Average financial loss per disruption
supply_chain_std_dev = 13000  # Standard deviation for disruptions

# Step 4: Implementing the Monte Carlo simulation
num_iterations = 10000

# Step 5: Lists to store total losses for each iteration

total_losses = []

for _ in range(num_iterations):
    # Simulate Product Quality Issues
    product_quality_loss_sample = np.random.normal(product_quality_loss, product_quality_std_dev)
    product_quality_loss_total = product_quality_loss_sample if random.random() < service_level else 0

    # Simulate Supply Chain Disruptions
    supply_chain_loss_reliability = np.random.normal(supply_chain_reliability, supply_chain_std_dev)
    supply_chain_loss_total = supply_chain_loss_reliability if random.random() < service_level else 0

    # Calculate total loss for this Reliability iteration
    total_loss = product_quality_loss_total + supply_chain_loss_total * service_level
    total_losses.append(total_loss)

# Calculate statistics
mean_loss = np.mean(total_losses)
std_deviation = np.std(total_losses)
supplychain_reliability_10 = np.percentile(total_losses, 10)
supplychain_reliability_99 = np.percentile(total_losses, 99)
```

Group 3 assumption on product quality is highly positive, assuming that PP will not shift to an international supply but source all its raw materials from one point, and control the product manufacturing plants as well as the Distribution Centers. It is important to note that, PP is not a multi-vendor platform or one which allows products they do not control. Based on these assumptions, we strongly believe the foreseeable risks are minimal.

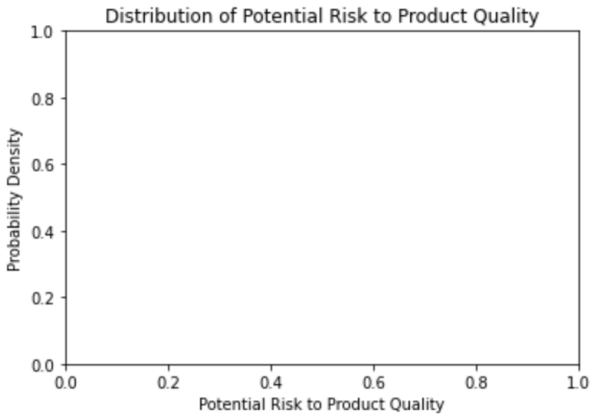
Visualising the distributions

```
# Print results
print("Monte Carlo Simulation Results:")
print("Mean Potential Loss due to Quality: £", round(mean_loss, 2))
print("Standard Deviation: £", round(std_deviation, 2))
print("10th_supplychain_reliability_loss: £", round(supplychain_reliability_99, 2))
print("99th_supplychain_reliability_loss: £", round(supplychain_reliability_99, 2))

#Plotting a histogram of supply chain Reliability and potential financial loss

plt.hist(total_losses, bins=30, color='c')

# Print the result
plt.xlabel('Potential Risk to Supply Chain')
plt.ylabel('Product Availability')
plt.title('Monte Carlo Simulation: Distribution of Potential Risk due to PP product quality and Supply Chain')
plt.show()


quality_losses = [loss for loss in total_losses if loss < 10000]

# Plotting a histogram of potential risk to product quality
plt.xlabel('Potential Risk to Product Quality')
plt.ylabel('Probability Density')
plt.title('Distribution of Potential Risk to Product Quality')
```

```
Monte Carlo Simulation Results:
Mean Potential Loss due to Quality: £ 9.38
Standard Deviation: £ 214.16
10th_supplychain_reliability_loss: £ 0.0
99th_supplychain_reliability_loss: £ 0.0
```



: Text(0.5, 1.0, 'Distribution of Potential Risk to Product Quality')



The probabilistic simulation was performed using Jupyta Notebook (python3) on Codio. This simulation, conducted for 10,000 iterations, considered the probability of occurrence and potential financial impact for each risk.

- Probability of Loss of Quality: 1%
- Probability of Supply Chain Issues: 0.2%

The Monte Carlo Simulation helps

- Forecast the potential loss expectancy.
- Focus on mitigating the risk of supply chain issues as it presents a higher financial impact.
- Implement quality assurance measures to reduce the probability of quality loss.

Summarised Cyber Risk Identification based on earlier report.

#	Cyber Risk Assessment	Frequency Distribution	Parameter 1
1	**Unauthorised access**	Binomial	20
2	**Elevation of privilege attack**	Poisson	12
3	**Insider threat**	Poisson	7
4	**Phishing/vishing attack**	Poisson	20
5	**Distributed Denial of Service (DDoS)**	Poisson	22
6	**Password attack**	Binomial	10
7	**Man-in-the-middle attack**	Poisson	5
8	**Web application and in-app attacks**	Poisson	15
9	**Advanced persistent threat attack**	Binomial	12
10	**Privacy compromise (PII exposure)**	Poisson	12
11	**Disaster (Fire in Datacenter (DC))**	Binomial	4
12	**Cloud vendor disaster**	Poisson	8
13	**Legal issues/sanctions**	InterUniform	10
14	**Third-party failure attack**	InterUniform	22
15	**Accidental data breach/leakage**	Poisson	13
16	**Sensitive data disclosure (Customers credit card compromise)**	Poisson	8
17	**Sales losses (Automated warehouse and supply chain software failures)**	Binomial	9

The parameters above are dummy values. We chose 'poisson' for events where success could occur at any point within the IT system (events in which the average rate

is known based on previous findings within cyberspace). Binomial frequency is for events that can experiment with two possible outcomes: success or failure (e.g., unauthorised access could succeed but not lead to the compromise of either Confidentiality, Integrity or Availability). InterUniform implies a combination of Binomial or Poisson since those Cyber risks depend on external factors or third parties.

Monte Carlo Simulation for Cyber Risk Assessment

We also tried using the Monte Carlo Simulation for the cyber risk assessment, and below is our result.

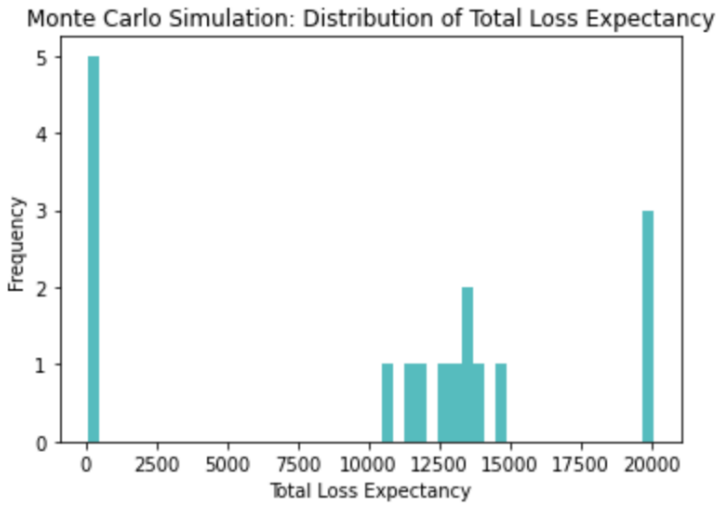
```
import numpy as np
import matplotlib.pyplot as plt

# List of risks
risks = [
    "Unauthorised access", "Elevation of privilege attack", "Insider threat", "Phishing attack",
    "DDoS", "Password attack", "Man-in-the-middle attack", "Web application and in-app attacks",
    "Advanced persistent threat attack", "Privacy compromise", "DC Disaster",
    "Cloud vendor disaster", "Legal issues", "Third-party failure attack", "Accidental data breach",
    "Sensitive data disclosure", "Sales losses"]

# Parameters for frequency and severity distributions
binomial_params = (40, 0.002)  # Number of trials and probability of success
poisson_params = (12,)  # Mean (average) occurrence rate
interuniform_params = (10, 30, 20)  # Lower bound, upper bound, and mode

# Number of iterations for Monte Carlo simulation
num_iterations = 1000

# Lists to store total losses for each risk
total_losses = []

# Simulate risk events
for risk in risks:
    if risk in ["Unauthorised access", "Password attack", "Advanced persistent threat attack", "DC Disaster", "Sales
        # Binomial distribution
        frequency = np.random.binomial(binomial_params[0], binomial_params[1], num_iterations)
    elif risk in ["Elevation of privilege attack", "Phishing attack", "Web application", "Insider threat", "DDoS", "
        # Poisson distribution
        frequency = np.random.poisson(poisson_params[0], num_iterations)
    else:
        # Interuniform distribution
        frequency = np.random.triangular(interuniform_params[0], interuniform_params[2], interuniform_params[1], num

    # Severity distribution
    severity = np.random.normal(1000, 5000, num_iterations)

    # Calculate total loss for each iteration
    total_loss = frequency * severity
    total_losses.append(total_loss)
```

The mean severity is 1000, representing the average or expected financial impact of a risk event. The standard deviation is 5000, indicating a relatively high degree of variability or dispersion in the severity of cyber risk events. Some events may result in

relatively small losses, while others may lead to significantly larger losses. The high standard deviation suggests a wide range of potential outcomes.

Visualising the distributions

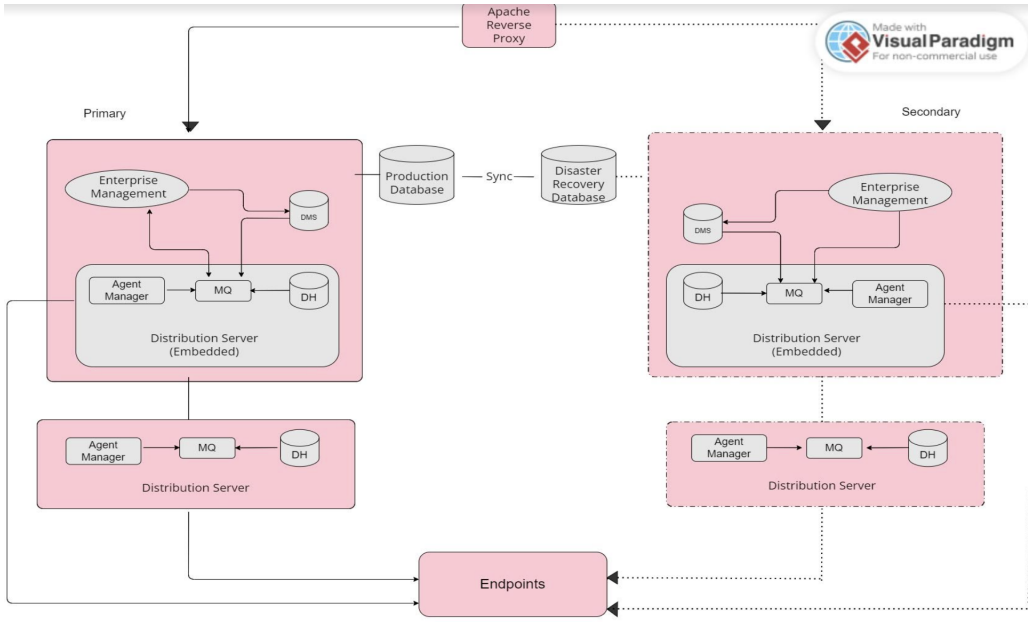
```
# Calculate mean total loss
mean_total_losses = np.mean(total_losses, axis=1)

# Plot distribution graph
plt.hist(mean_total_losses, bins=50, color='c')
plt.xlabel('Total Loss Expectancy')
plt.ylabel('Frequency')
plt.title('Monte Carlo Simulation: Distribution of Total Loss Expectancy')
plt.show()
```



Disaster Recover Choice

Implementing a Disaster Recovery Plan is vital for 24/7/365 online shop availability while ensuring a 1-minute changeover window. This guarantees seamless Business Continuity with the flexibility to switch sites as needed. We recommend ongoing DR site testing, including yearly or bi-annual tests. Real-world scenarios like pandemics, fires,

floods, or power grid failures should be simulated to evaluate DR and BC readiness, revealing any weaknesses.



ACTIVE-ACTIVE SITE For DR Solution.

To address Ms. O'dour's request, we propose an active-active DR failover setup. Both production and DR sites will mirror each other, featuring multiple data centres, storage, server clustering, and synchronous operation for maximum reliability. This configuration ensures high availability across the two sites. Simultaneously, two systems will run, ideally in different regions, one on-premise and one in the cloud. Code deployment will occur concurrently, but a blue-green deployment strategy is also available for testing new code while retaining the older version on the second site. (Lecturecast 6, Unit 11, 2023)

Recommended Cloud Platform and Vendor Lock-in

For an optimal Active-Active DR solution, we recommend a single cloud Service Provider (CSP) in different availability zones since multiple CSPs can be costly, pose

integration challenges, and demand more technical know-how. Given assumed budget constraints, AWS Cloud and the use of DynamoDB are advised for its high availability, scalability, global reach, and serverless NoSQL capabilities (Pelumi, N.D.).

The following factors are important in selecting a vendor:

- Cost & Flexibility
- Data portability
- Interoperability: it is critical to ensure the vendor's infrastructure has the interoperability to link with other vendors/platforms.
- Standardisation
- Continuous support from the provider

GeeksforGeeks, 2023

Service Level Agreement (SLA): PP needs to pay attention to all the terms and conditions in the vendor's SLA, especially on service availability of 24/7/365, smooth exit in the event of dissatisfaction and exclusivity service clauses to avoid vendor lock-in challenges (GeeksforGeeks, 2023).

Conclusion

In conclusion, key findings from the analysis encompass product quality and supply chain risks, as well as cybersecurity considerations. The assessment highlights that the risk to product quality is effectively managed, with minimal estimated mean potential

loss. Supply chain risk is also within acceptable limits, but service level (SL) changes significantly impact supply chain loss and, consequently, the perception of product quality and availability.

The quantitative analysis is justified, considering the potential impact on supply chain availability and product quality. The Monte Carlo Simulation, supported by Python, provides insights into financial impacts, risk probabilities, and mitigations. Risk assessment for cyber risks is presented, with parameters and probabilities established for each risk category.

The assessment emphasises the importance of a proactive approach to risk management, digitalisation, adherence to GDPR directives and effective management of risks relating to quality, supply chain, and cybersecurity.

References

1. GDPREU (N.D.). What's on the horizon for privacy and data in 2023?. Available from: https://www.gdpreu.org/whats-on-the-horizon-for-privacy-and-data-in-2023. [Accessed 20 October 2023].
2. Ghafoor, R. (2023). Monte Carlo Simulation in Supply Chain Management: A Case Study on Inventory Optimization. Available from: https://medium.com/@zainabghafoor7866/monte-carlo-simulation-in-supply-chain-management-a-case-study-on-inventory-optimization-c4fbb064d84. [Accessed 21 October 2023].
3. GOV UK (2021.). Make privacy integral. Available from: https://www.gov.uk/guidance/make-privacy-integral. [Accessed 22 October 2023].
4. Oracle WMS Cloud Product Team (2023). Oracle Warehouse Management Cloud. Available from: https://docs.oracle.com/en/cloud/saas/warehouse-management/23b/owsec/security-guide.pdf [Accessed 20 October 2023].
5. Schmitt, A.J., & Singh, M. (2009). Quantifying supply chain disruption risk using Monte Carlo and discrete-event simulation. [Accessed 22 October 2023].
6. Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. P., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. Available from: https://academic.oup.com/cybersecurity/article/9/1/tyac016/7000422. [Accessed 20 October 2023].

7. University of Essex Codio (Jupyter notebook: python3). [Accessed 21 October 2023].
8. Yaacoub, J. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Available from: https://link.springer.com/article/10.1007/s10207-021-00545-8 [Accessed 20 October 2023].
9. Pelumi (2023). Cosmos DB vs DynamoDB: What Are The Similarities? Available from: https://www.pulumi.com/what-is/database-comparison-cosmos-db-vs-dynamodb [Accessed 20 October 2023].
10. University Essex Lecture Cast unit 9. Business Continuity and Disaster Recovery, Available from: https://www.my-course.co.uk/mod/scorm/player.php?scoid=23630&cm=853366&currentorg=articulate_rise&display=popup [Accessed 17 October 2023]
11. Microsoft Ignite Article 04/14/2023.Azure Virtual Desktop disaster recovery concepts. Available from: https://learn.microsoft.com/en-us/azure/virtual-desktop/disaster-recovery-concepts[access [Accessed 10 October 2023].
12. Geeks (Jan 27, 2023). Vendor Lock-in in Cloud Computing. Available from:https://www.geeksforgeeks.org/vendor-lock-in-in-cloud-computing/. [Accessed 05 October 2023].

13. Morrow. el at (2021), Carnegie Mellon University Software Engineering Institute, Cloud Security Best Practices Derived from Mission Thread Analysis. Available from: https://apps.dtic.mil/sti/pdfs/AD1139951.pdf[Accessed 08 October 2023].
14. Opera-Martins et al (2014). International Conference on Information Society (i-Society 2014) Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. Available from:https://eprints.bournemouth.ac.uk/22467/1/Critical%20Review%20of%20Vendor%20Lock-in%20and%20Its%20Impact%20on%20Adoption%20of%20Cloud%20Computing.pdf [Accessed 04 October 2023]