Executive Summary

As the pet food industry evolves, businesses like **Pampered Pets** are increasingly adopting digital transformation strategies to enhance operational efficiency and expand their market reach. However, this shift presents significant risks that could impact the quality and availability of products.

This executive summary analyses the risks associated with the digitalisation process, using quantitative risk modelling approaches, specifically **Monte Carlo (MC) simulation**. Further a **disaster recovery (DR) strategy** is developed for the business to ensure business continuity in the case of disruption.

Quantitative Risk Modelling

The MC simulation was selected, as this quantitative risk modelling approach is suitable to navigate complex risks and helps to fulfil the two new high-profile customer's needs. It allows the modelling of complex systems involving multiple variables and uncertainties. By simulating numerous scenarios, this method provides an understanding of how various factors could affect the business (Vose, 2008). Unlike traditional deterministic models, simulations produce probability distributions for various outcomes (Simon, 1996).
Lastly, the insights gained from MC simulations empower stakeholders to make informed decisions by evaluating the trade-offs between different risk management strategies (Hertz & Thomas, 1984).
While offering significant advantages, several critical points must be navigated:

- Reliance on the input data; prioritise the collection of accurate data and use benchmark data (Palisade, 2023)
- MC simulations can be resource intensive
- Stakeholders must understand unforeseen events may still occur (Gartner, 2021)

Steps to Implement a MC Simulation:

1. Identify the risk and make assumptions regarding the probability (see A.1).
2. Define an impact between 1 (low impact) and 5 (high impact) for the respective risks.
3. Simulate the impact of these risks over 1,000 iterations to estimate the potential combined effects of availability and quality risks.

Below is a snipped of the Python code for the MC Simulation (complete code in A.2):

```
iterations = 1000


risks = {
    "Supply_Delays": {"probability": 0.25, "impact": 4},
    "System_Downtime": {"probability": 0.15, "impact": 3},
    "Inaccurate_Forecasting": {"probability": 0.30, "impact": 4},
    "Transport_Disruptions": {"probability": 0.20, "impact": 3},
    "Supplier_Reliability": {"probability": 0.10, "impact": 2},
    "Data_Integrity_Issues": {"probability": 0.10, "impact": 3},
    "Product_Contamination": {"probability": 0.05, "impact": 5},
    "Defective_Packaging": {"probability": 0.05, "impact": 3},
    "Inconsistent_Ingredient_Quality": {"probability": 0.15, "impact": 4},
    "Cybersecurity_Threats": {"probability": 0.07, "impact": 5}
```

Figure 1: Python Code (Hamberger, 2024)

Python produced the following result for this MC simulation:

```
Average Availability Risk Impact: 3.61
Average Quality Risk Impact: 1.771

Availability Risk Impact Frequency Distribution:
Impact: 3, Frequency: 130
Impact: 7, Frequency: 110
Impact: 0, Frequency: 319
Impact: 2, Frequency: 32
Impact: 8, Frequency: 55
Impact: 4, Frequency: 227
Impact: 6, Frequency: 42
Impact: 5, Frequency: 20
Impact: 14, Frequency: 4
Impact: 11, Frequency: 25
Impact: 9, Frequency: 18
Impact: 10, Frequency: 13
Impact: 13, Frequency: 3
Impact: 12, Frequency: 2

Quality Risk Impact Frequency Distribution:
Impact: 0, Frequency: 623
Impact: 4, Frequency: 116
Impact: 5, Frequency: 96
Impact: 3, Frequency: 100
Impact: 8, Frequency: 14
Impact: 7, Frequency: 21
Impact: 9, Frequency: 15
Impact: 10, Frequency: 4
Impact: 6, Frequency: 7
Impact: 12, Frequency: 2
Impact: 13, Frequency: 1
Impact: 14, Frequency: 1
```

Figure 2: Result Monte Carlo Simulation (Hamberger, 2024)

Interpretation availability risk:

- The "Average Availability Risk Impact" value of 3.61 represents the average impact level of availability risks across the data analysed. 3.61 suggests a moderate to high overall impact of availability risks.
- The frequency distribution is somewhat right-skewed, with the highest frequency at impact level 2 (319 occurrences), followed by levels 1 and 3. This implies that most availability risks lead to relatively low-to-moderate impacts, but some can escalate to more severe disruptions (e.g., impact level 6 with 45 occurrences). This aligns with Olson and Wu (2010) suggestion that operational risks often follow non-normal distributions, with many low-impact events and fewer, but more significant, high-impact disruptions. A value of "0" occurs 319 times, indicating that no significant availability risks materialized in 319 out of 1,000 simulations.
- The skewed distribution indicates resilience in the system. Nevertheless, Olson and Wu (2010) highlight that the tail risk (extreme but rare events) can be particularly damaging in supply chains if not addressed.

Interpretation quality risk:

- The average quality risk impact is 1.771, it suggests that the quality risks identified are relatively low to moderate in severity.
- The most frequent values are "3" and "4," indicating low-to-moderate impacts.
- The extreme values in the quality risk distribution (e.g., impact level 14 with 1 occurrence) suggest that while infrequent, severe quality risks could lead to catastrophic consequences. Olson and Wu (2010) emphasize the importance of continuous quality control mechanisms to prevent these events. The large number of zero-impact events (“0" occurs 623 times, meaning in over 62% of the simulations, no significant quality risks) may reflect strong preventative measures, but the presence of higher impacts indicates that when these systems fail, the consequences can be severe.

Further, Olson and Wu (2010) propose a dual approach in enterprise risk management: managing frequent, moderate risks through operational resilience and supply chain diversification, and preparing for rare, high-impact events through strategic buffers, such as quality audits and supplier evaluation.

From the above simulated risk impacts, it is possible to calculate the likelihood of different risk levels occurring.

Risk Type	Likelihood post-digitalisation	Likelihood pre-digitalisation	Difference
Availability Issues	68.1%	30-50% (Tang, 2006)	+18.1% to +38.1%
Quality Loss	37.7%	20-35% (Ivanov et al., 2019)	+2.7% to +17.7%

Table 1: Risk Level Comparison Digitalisation (Hamberger, 2024)

This comparison highlights the increasing complexity and risk associated with the digitalisation of supply chains, underscoring the importance of adapting risk management strategies. The table can be interpreted in the following way:

- In 68.1% of the MC simulations, at least one supply chain risk was realized (resulting in a non-zero impact). This means that the simulation suggests a very high likelihood of experiencing some form of risk in the supply chain.
- In 37.7% of the MC simulations, at least one quality risk was realized. This means that the simulation suggests a moderate likelihood of experiencing risk in the overall product quality.
- Compared to local suppliers it shows that availability issues are at a significantly higher risk (+18.1% to +38.1%) while the risk of quality loss is moderate (+2.7% to +17.7%) compared to sourcing from local suppliers.

By knowing which impact levels occur most frequently, it is possible to prioritise the risk management efforts. For rare but severe impacts, Pampered Pets should develop emergency procedures. Other possible **countermeasures** could be:

- Establishing multiple suppliers (Ivanov et al., 2019)
- Regular system maintenance and backup systems (Birkel & Hartmann, 2020)
- Use of AI-driven predictive analytics to improve accuracy in forecasting
- Partnering with multiple logistics companies to avoid transport disruptions and introduce penalties for late delivery (Ivanov et al., 2019)
- Establish KPIs for supplier digital readiness
- Contracts with suppliers that enforce quality standards and introduce penalties for quality issues
- Invest in cybersecurity solutions and regular vulnerability assessments

To sum it up, the MC simulation provides an essential starting point for assessing the risks related to the digitalisation of Pampered Pets operations. However, there are also critical points to consider when evaluating the MC simulation:

- Further risks, such as global catastrophes could heavily impact both global and local suppliers. These events could lead to delays, higher costs, and shortages (Ivanov et al., 2019).
- Financial costs of mitigating these risks can be substantial. Diversifying suppliers, enhancing quality control, or investing in backup logistics networks will require investment (Birkel & Hartmann, 2020).
- The accuracy is highly dependent on the underlying assumptions and input data. If the probability distributions are inaccurately defined, the outputs may not reflect real-world risks. Olson and Wu (2010) stress the importance of verifying assumptions in any simulation-based risk model to avoid under- or overestimating risks.
- The MC simulation might not account for the correlations between availability and quality risks. For example, a disruption in the supply chain could simultaneously increase both availability and quality risks (e.g., a sudden supplier change leading to quality control issues). Monte Carlo simulations often assume independent risks unless specifically modelled otherwise (Vose, 2008).
- The occurrence of high-impact events is likely based on assumptions about their probability, which may not be realistic. Olson and Wu (2010) emphasize the importance of stress testing for extreme cases ("black swan events") that lie outside the normal distribution predictions.

In conclusion, while Monte Carlo simulations are powerful tools, the results for Pampered Pets should not be accepted as 100% accurate without considering potential errors. Olson & Wu (2010) provide critical guidance on validating assumptions, ensuring data accuracy, and accounting for extreme events in enterprise risk management models.

Disaster Recovery Strategy

In the following a Disaster Recovery (DR) strategy is outlined. The solution ensures high availability (24/7/365) by meeting the Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) of less than 1 Minute, as specified by Cathy's investor. The DR plan is based on the transition to an e-commerce platform, ensuring the business's digital components are resilient to outages or disasters.

Explanation of the designed architecture:

- The arrow in the diagram shows **continuous data replication** between the two environments. It ensures that both environments have up-to-date data in near real-time, which is essential for achieving an RPO under 1 minute. This means minimal data loss in the event of a failure (Jouini, Rabai & Aissa, 2014).
- The inclusion of a **traffic manager** suggests that traffic can be dynamically rerouted between the two environments. In a DR situation, the traffic manager should automatically switch traffic to the secondary environment (on the right) if the primary environment (on the left) fails. If properly configured, this can happen almost instantaneously, meeting the 1-minute RTO requirement (Ali, Khan & Vasilakos, 2015).
- Both environments are **cloud-based,** which generally allows for quick failover due to the high availability of cloud resources. If failover mechanisms are automated, this would also support a very low RTO (Toosi et al., 2016).

- The secondary environment has **redundancy** in terms of databases, storage, and servers, which is excellent for fault tolerance. This will ensure high availability and minimize downtime in case of component failures (Jouini, Rabai & Aissa, 2014).
- The presence of an **automated DevOps pipeline** helps to maintain both environments in sync and ensures that updates are deployed efficiently.

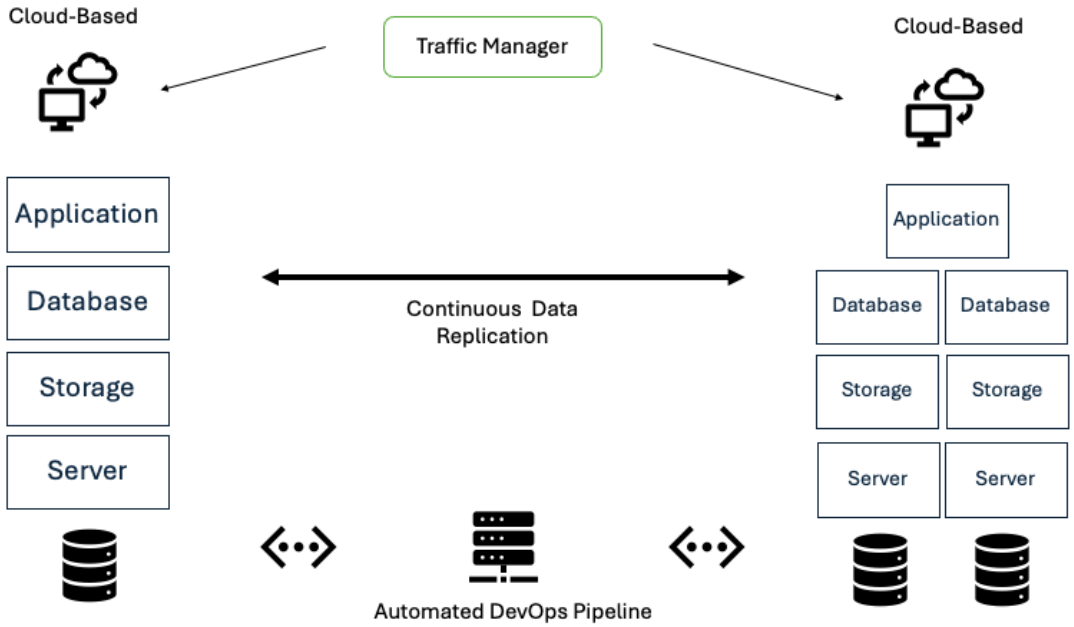

Figure 3: DR architecture for Pampered Pets (Hamberger, 2024)

The solution of **DraaS (Disaster Recovery as a Service)** is preferred due to the ability to meet the stringent RTO and RPO requirements, ease of scalability, and resilience (Ali, Khan & Vasilakos, 2015).For Pampered Pets the below Platforms are recommended:

Component	Cost Estimate (Monthly)	Platform
Cloud-Based DRaaS	$500 - $3,000 (Jamsa, 2013)	AWS Elastic Disaster Recovery, Azure Site Recovery
Continuous Data Replication	$200 - $500 Buyya et al., 2013)	AWS RDS Multi-AZ, Azure Geo-Replication
DR Automation	$300 - $2,500 (Gupta et al., 2013)	AWS Cloud Endure, Azure Site Recovery
Containerisation	$500 - $1,500 (Pahl et al., 2019)	Docker, Kubernetes
Total Cost	$1,500 - $7,500	

Table 2: Recommended DR Platforms including cost overview (Hamberger, 2024)

After implementation Pampered Pets must also ensure that there are enough security protocols, they work GDPR compliant, and they avoid vendor lock-in:

To ensure GDPR compliance, all data in transit and at rest will be encrypted, safeguarding against unauthorized access. The cloud provider must also offer data

storage in GDPR-compliant regions, such as EU-based data centers from AWS or Azure. Additionally, robust access control will be enforced through Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), ensuring only authorized users can access critical systems and data (*Art. 32 GDPR*, 2016).

To avoid vendor lock-in, Pampered Pets should adopt several strategies and best practices that enhance flexibility and mitigate dependency on any single provider. A multi-cloud or hybrid cloud strategy can distribute services, enhancing resilience and minimizing switching costs (Hashizume et al., 2013). Utilizing containerization technologies allows applications to decouple from their underlying infrastructure, enabling the same application to run across different cloud environments with minimal changes (Turnbull, 2014). Additionally, adopting open standards and open-source solutions promotes interoperability and minimizes dependence on proprietary systems. Choubey et al. (2011) highlight that open-source platforms are critical in maintaining operational independence from single providers.

Furthermore, implementing a robust data portability and backup strategy is crucial. By storing data in widely supported formats, migrating between cloud services becomes easier. Bohn et al. (2011) emphasize that data portability practices significantly reduce risks associated with switching vendors. Lastly, contract negotiations should include exit clauses that provide migration assistance and data retrieval options, addressing potential future challenges related to vendor dependency (Armbrust et al., 2010).

Critical Points to be reviewed regularly:

- According to Subashini and Kavitha (2011), cloud services increase exposure to cyber threats. Ensuring robust encryption and access controls is essential, yet these measures can introduce management complexities and performance bottlenecks.
- Reliance on continuous data replication can be risky. While it helps achieve low RPO and RTO, disruptions in the replication process could lead to data inconsistencies, contradicting the purpose of a DR strategy (Chen & Zhao, 2012). Organizations must prioritize network reliability to ensure uninterrupted replication, though this may increase operational costs (Zissis & Lekkas, 2012).
- While traffic management aims to enhance performance and availability, improper configuration or system failures can cause significant disruptions (Rittinghouse & Ransome, 2016).

<u>Summary</u>

Pampered Pets is undergoing a digital transformation that presents significant risks to product availability and quality. To assess these risks, a MC simulation was used.

The results showed that availability risks pose a moderate to high impact, with the most frequent outcomes falling within mid-range impact levels (between 3 and 7). While more severe disruptions were less common, they remain possible. Quality risks, on the other hand, showed a relatively low-to-moderate impact, with no significant quality issues occurring in over 60% of the simulations. However, while

MC simulation offer a robust way to understand the range of potential risks, it is not all-embracing and cannot account for unpredictable global events (Vose, 2008).

To complement this risk analysis, a DR strategy was developed to ensure business continuity. The DR strategy focuses on achieving an RTO and RPO of less than 1 minute, using a cloud-based DRaaS. This includes continuous data replication between two cloud environments and dynamic traffic management to minimize downtime (Wallace & Webber, 2017).

Finally, Pampered Pets must regularly update its MC simulations and refine its DR strategy to mitigate new risks as the business grows. Enhancing data quality, strengthening cybersecurity measures, and developing alternative supplier networks will be critical to maintaining resilience in the face of digital transformation challenges (Vose, 2008).

Wordcount: 2196

Appendix

A.1 Potential risk assumptions regarding the probability and respective impact

1. Supply Delays: Probability = 0.25, Impact = 4

Supply chain delays are common in businesses with complex supply chains, such as pet food manufacturing, where ingredients are often sourced from various regions. Research shows that disruptions in global supply chains, whether due to transportation delays or supplier issues, occur in approximately 20-30% of supply chains (Ivanov, 2021). The high impact (4) reflects the dependency of pet food manufacturers on timely delivery of ingredients to maintain production schedules and meet demand, particularly for premium, perishable products (Stevenson & Spring, 2007).

2. System Downtime: Probability = 0.15, Impact = 3

The digitalization of pet food businesses increases their reliance on IT systems for operations, including e-commerce platforms and ERP systems. While the probability of a full system failure may be relatively low (15%), the impact on operations can be moderate, leading to disruptions in order processing, inventory management, and logistics ((Harland, Brenchley & Walker, 2003).

3. Inaccurate Forecasting: Probability = 0.30, Impact = 4

Forecasting demand in the pet food industry is challenging due to fluctuating consumer preferences and seasonal variations. Research indicates that forecasting errors occur in up to 30% of inventory planning cases, particularly in industries with complex product lines and high SKU counts (Makridakis, Wheelwright & McGee, 1993). The impact of inaccurate forecasting (4) is significant as it can lead to overproduction or stockouts, which affect customer satisfaction and profitability.

4. Transport Disruptions: Probability = 0.20, Impact = 3

Transportation is a critical element in pet food logistics, and disruptions—such as strikes, extreme weather, or fuel shortages—are relatively common, with probabilities around 20% in supply chain operations (Christopher, 2016). The impact (3) is moderate, as transportation delays can lead to temporary stock shortages, particularly for premium products, without immediate catastrophic effects.

5. Supplier Reliability: Probability = 0.10, Impact = 2

In the pet food industry, supplier reliability tends to be relatively stable due to long-term contracts and stringent quality control mechanisms (Trent, 2004). However, issues such as financial instability or production shortfalls can affect 10% of suppliers, leading to minimal to moderate impacts on the business (impact = 2), as suppliers can typically be replaced or alternative solutions found.

6. Data Integrity Issues: Probability = 0.10, Impact = 3

The rise of digitalized systems makes data integrity issues a significant risk, though they tend to occur in about 10% of cases, especially where there are weaknesses in data management and quality control (Staff, 2005). The impact of compromised data can be moderately disruptive (impact = 3), particularly in logistics and inventory management, leading to operational inefficiencies.

7. Product Contamination: Probability = 0.05, Impact = 5

Although the probability of contamination in pet food manufacturing is low (5%), the impact is severe (impact = 5) because it directly threatens animal health and consumer trust. Recalls due to contamination can result in significant financial losses, legal repercussions, and long-term damage to the brand's reputation (Redmond & Griffith, 2004).

8. Defective Packaging: Probability = 0.05, Impact = 3

Defective packaging is relatively rare, occurring in about 5% of production runs, but it has a moderate impact (3) on the business as it affects product shelf life and consumer satisfaction (Smith, 1993). Poor packaging can lead to product spoilage or safety concerns, particularly for perishable items.

9. Inconsistent Ingredient Quality: Probability = 0.15, Impact = 4

Ingredient quality inconsistencies are a moderate risk in pet food manufacturing, particularly for premium products that require specific nutritional standards. Approximately 15% of ingredient suppliers may provide inconsistent quality due to supply chain variability (González-Benito, 2007). This has a significant impact (4), as inconsistent quality can lead to product recalls or consumer dissatisfaction.

10. Cybersecurity Threats: Probability = 0.07, Impact = 5

As pet food businesses increasingly rely on digital systems, cybersecurity threats such as data breaches, ransomware, and hacking pose a growing concern. Although the likelihood of a severe attack is relatively low (7%), the impact of such events is substantial (impact = 5), given the potential for operational disruption, financial losses, and damage to customer trust (OCR of the Document, 2018).

A.2 Python Code for the Monte Carlo Simulation

```python
import random
from collections import Counter

iterations = 1000


risks = {
    "Supply_Delays": {"probability": 0.25, "impact": 4},
    "System_Downtime": {"probability": 0.15, "impact": 3},
    "Inaccurate_Forecasting": {"probability": 0.30, "impact": 4},
    "Transport_Disruptions": {"probability": 0.20, "impact": 3},
    "Supplier_Reliability": {"probability": 0.10, "impact": 2},
    "Data_Integrity_Issues": {"probability": 0.10, "impact": 3},
    "Product_Contamination": {"probability": 0.05, "impact": 5},
    "Defective_Packaging": {"probability": 0.05, "impact": 3},
    "Inconsistent_Ingredient_Quality": {"probability": 0.15, "impact": 4},
    "Cybersecurity_Threats": {"probability": 0.07, "impact": 5}
}


availability_risks = ["Supply_Delays", "System_Downtime", "Inaccurate_Forecasting", "Transport_Disruptions", "Supplier_Reliability"]
quality_risks = ["Data_Integrity_Issues", "Product_Contamination", "Defective_Packaging", "Inconsistent_Ingredient_Quality", "Cybersecurity_Threats"]

availability_results = []
quality_results = []

for i in range(iterations):
    availability_impact = 0
    quality_impact = 0


    for risk in availability_risks:
        if random.random() < risks[risk]["probability"]:
            availability_impact += risks[risk]["impact"]


    for risk in quality_risks:
        if random.random() < risks[risk]["probability"]:
            quality_impact += risks[risk]["impact"]


    availability_results.append(availability_impact)
    quality_results.append(quality_impact)


def calculate_mean(results):
    return sum(results) / len(results)


def frequency_distribution(results):
    return dict(Counter(results))


availability_mean_impact = calculate_mean(availability_results)
quality_mean_impact = calculate_mean(quality_results)

print(f"Average Availability Risk Impact: {availability_mean_impact}")
print(f"Average Quality Risk Impact: {quality_mean_impact}")


print("\nAvailability Risk Impact Frequency Distribution:")
availability_dist = frequency_distribution(availability_results)
for impact, freq in availability_dist.items():
    print(f"Impact: {impact}, Frequency: {freq}")

print("\nQuality Risk Impact Frequency Distribution:")
quality_dist = frequency_distribution(quality_results)
for impact, freq in quality_dist.items():
    print(f"Impact: {impact}, Frequency: {freq}")
```

References:

Hamberger, G. (2024) Executive Summary Pampered Pets. *SRM September 2024*. Essay submitted to the University of Essex Online.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015) Security in cloud computing: Opportunities and challenges. *Information Sciences 305*: 357–383. DOI: https://doi.org/10.1016/j.ins.2015.01.025

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010) A view of cloud computing. *Communications of the ACM 53*(4): 50–58. DOI: https://doi.org/10.1145/1721654.1721672

Art. 32 GDPR – Security of processing - General Data Protection Regulation (GDPR) (2016). Available from: https://gdpr-info.eu/art-32-gdpr/#:~:text=The%20controller%20and%20processor%20shall,Union%20or%20Member%20State%20law [Accessed 7 October 2024].

Birkel, H. S., & Hartmann, E. (2019) Impact of IoT challenges and risks for SCM. *Supply Chain Management an International Journal 24*(1): 39–61. DOI: https://doi.org/10.1108/scm-03-2018-0142

Bohn, R., Liu, F., Tong, J., Mao, J., Messina, J., Badger, L., & Leaf, D. (2011) *NIST cloud computing reference architecture*. DOI: https://doi.org/10.6028/nist.sp.500-292

Buyya, R., Vecchiola, C., & Selvi, S. (2013) *Mastering cloud computing: Foundations and Applications Programming*. Newnes.

Chen, D., & Zhao, H. (2012) Data Security and Privacy Protection Issues in Cloud Computing. *Procedia Engineering*. DOI: https://doi.org/10.1109/iccsee.2012.193

Choubey, R., Dubey, R., & Bhattacharjee, J. (2011) A Survey on Cloud Computing Security, Challenges and Threats. *International Journal on Computer Science and Engineering 3*(3): 1227–1231. Available from: https://doaj.org/article/a7a09b6e529e45919f8e316c633beb50 [Accessed 7 October 2024].

Christopher, M. (2016) *Logistics and Supply Chain Management: Logistics & Supply Chain Management*. Pearson UK.

European Central Bank (2022) *Economic Bulletin issue 8, 2021*. Available from: https://www.ecb.europa.eu/press/economic-bulletin/html/eb202108.en.html. [Accessed 7 October 2024].

Gartner (2021) *Managing Risk Through Simulation and Analytics*. Available from: https://www.gartner.com/en/newsroom/press-releases/2021-03-23-gartner-identifies-top-security-and-risk-management-t [Accessed 10 October 2024].

González-Benito, J. (2007) A theory of purchasing's contribution to business performance. *Journal of Operations Management 25*(4): 901–917. DOI: https://doi.org/10.1016/j.jom.2007.02.001

Gupta, P., Seetharaman, A., & Raj, J. R. (2013) The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management 33*(5): 861–874. DOI: https://doi.org/10.1016/j.ijinfomgt.2013.07.001

Harland, C., Brenchley, R., & Walker, H. (2003) Risk in supply networks. *Journal of Purchasing and Supply Management 9*(2): 51–62. DOI: https://doi.org/10.1016/s1478-4092(03)00004-9

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013) An analysis of security issues for cloud computing. *Journal of Internet Services and Applications 4*(1): 5. DOI: https://doi.org/10.1186/1869-0238-4-5

Heizer, J., Render, B. und Munson, C. (2018) *Operations management sustainability and supply chain management*. Available from: http://dspace.urbe.university:8080/jspui/bitstream/123456789/204/4/Operations%20Management_%20Sustainability%20and%20Supply%20Chain%20Management_12th%20Edition_2016%20Pearson.pdf. [Accessed 7 October 2024].

Hertz, D.B. und Thomas, H. (1984) *Risk Analysis and Its Applications*.

Ivanov, D. (2021) Digital Supply Chain Management and Technology to Enhance Resilience by Building and Using End-to-End Visibility During the COVID-19 Pandemic. *IEEE Transactions on Engineering Management 71*: 10485–10495.DOI: https://doi.org/10.1109/tem.2021.3095193

Ivanov, D., & Dolgui, A. (2020) Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research 58*(10): 2904–2915. DOI: https://doi.org/10.1080/00207543.2020.1750727

Ivanov, D., Dolgui, A., Das, A., & Sokolov, B. (2019) Digital Supply Chain Twins: Managing the Ripple Effect, Resilience, and Disruption Risks by Data-Driven Optimization, Simulation, and Visibility. In *International series in management science/operations research/International series in operations research & management science*: 309-332. DOI: https://doi.org/10.1007/978-3-030-14302-2_15

Jamsa, K. (2013) *Cloud computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More*. Jones & Bartlett Publishers.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014) Classification of Security Threats in Information Systems. *Procedia Computer Science 32*: 489-496. DOI: https://doi.org/10.1016/j.procs.2014.05.452

Kouhizadeh, M., Saberi, S., & Sarkis, J. (2020) Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics 231*: 107831. DOI: https://doi.org/10.1016/j.ijpe.2020.107831

Makridakis, S. G., Wheelwright, S. C., & McGee, V. E. (1993) Forecasting methods and applications. *Computers & Operations Research 20*(5): 559–560. DOI: https://doi.org/10.1016/0305-0548(93)90040-p

OCR of the Document (2018). Available from: https://nsarchive.gwu.edu/media/17671/ocr [Accessed 7 October 2024].

Olson, D. L., & Wu, D. (2020) *Enterprise Risk Management models*. Springer Nature.

Pahl, C., Brogi, A., Soldani, J., & Jamshidi, P. (2017) Cloud Container Technologies: A State-of-the-Art Review. *IEEE Transactions on Cloud Computing 7*(3): 677–692. DOI: https://doi.org/10.1109/tcc.2017.2702586

Palisade (2023) *Palisade | Software Tools for Risk Modeling & Decision Analysis*. Available from: https://palisade.lumivero.com/. [Accessed 5 October 2024].

Pet Food Institute (2021) *Supply Chains for the Production of Agricultural Commodities and Food Products*. Available from: https://www.petfoodinstitute.org/wp-content/uploads/2021.06.21-PFI-comment-on-supply-chain-challenges.pdf [Accessed 5 October 2024].

Redmond, E. C., & Griffith, C. J. (2004) Consumer perceptions of food safety risk, control and responsibility. *Appetite 43*(3): 309–313. DOI: https://doi.org/10.1016/j.appet.2004.05.003

Rittinghouse, J., & Ransome, J. (2010) Cloud computing: implementation, management, and security. *Choice Reviews Online 48*(02): 48–0915. https://doi.org/10.5860/choice.48-0915

Simon, H.A. (1996) *The sciences of the artificial (3rd ed.)*, *MIT Press eBooks*. Available from: https://dl.acm.org/citation.cfm?id=237774. [Accessed 6 October 2024].

Smith, D.J. (1993) *Reliability, Maintainability and Risk: Practical Methods for Engineers*. Available from: http://ci.nii.ac.jp/ncid/BA2438742X. [Accessed 6 October 2024].

Staff. (2005) *The information supply chain: data integrity rises in stature*. Supply Chain Resource Cooperative. Available from https://scm.ncsu.edu/scm-articles/article/the-information-supply-chain-data-integrity-rises-in-stature. [Accessed 10 October 2024].

Stevenson, M., & Spring, M. (2007) Flexibility from a supply chain perspective: definition and review. *International Journal of Operations & Production Management 27*(7): 685–713. DOI: https://doi.org/10.1108/01443570710756956

Tang, C. S. (2006) Robust strategies for mitigating supply chain disruptions. *International Journal of Logistics Research and Applications 9*(1): 33–45. DOI: https://doi.org/10.1080/13675560500405584

Toosi, A. N., Vanmechelen, K., Khodadadi, F., & Buyya, R. (2016) An Auction Mechanism for Cloud Spot Markets. *ACM Transactions on Autonomous and Adaptive Systems 11*(1): 1–33. DOI: https://doi.org/10.1145/2843945

Trent, R. J. (2004) The Use of Organizational Design Features in Purchasing and Supply Management. *Journal of Supply Chain Management 40*(2): 4–18. DOI: https://doi.org/10.1111/j.1745-493x.2004.tb00170.x

Turnbull, J. (2014). *The Docker Book*. Lulu.com. Available from: https://books.google.de/books?id=CtMEBwAAQBAJ&printsec=frontcover&hl=de&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [Accessed 9 October 2024].

Vose, D. (2008) *Risk Analysis: a Quantitative guide*. Available from: http://ci.nii.ac.jp/ncid/BA47154351. [Accessed 9 October 2024].

Wallace, M., & Webber, L. (2004) The disaster recovery handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. *Choice Reviews Online 42*(04): 42–2310. DOI: https://doi.org/10.5860/choice.42-2310

Zissis, D., & Lekkas, D. (2010) Addressing cloud computing security issues. *Future Generation Computer Systems 28*(3): 583–592. DOI: https://doi.org/10.1016/j.future.2010.12.006