Pampered Pets, a company specializing in the sale of high-quality pet food, is embarking on an ambitious digital transformation that includes the establishment of an international supply chain and the automation of warehouses on a global scale. These changes, funded by Orla O'dour, have raised concerns from two major clients, HRH the King and Prince Albert II of Monaco, about product quality and supply chain security.

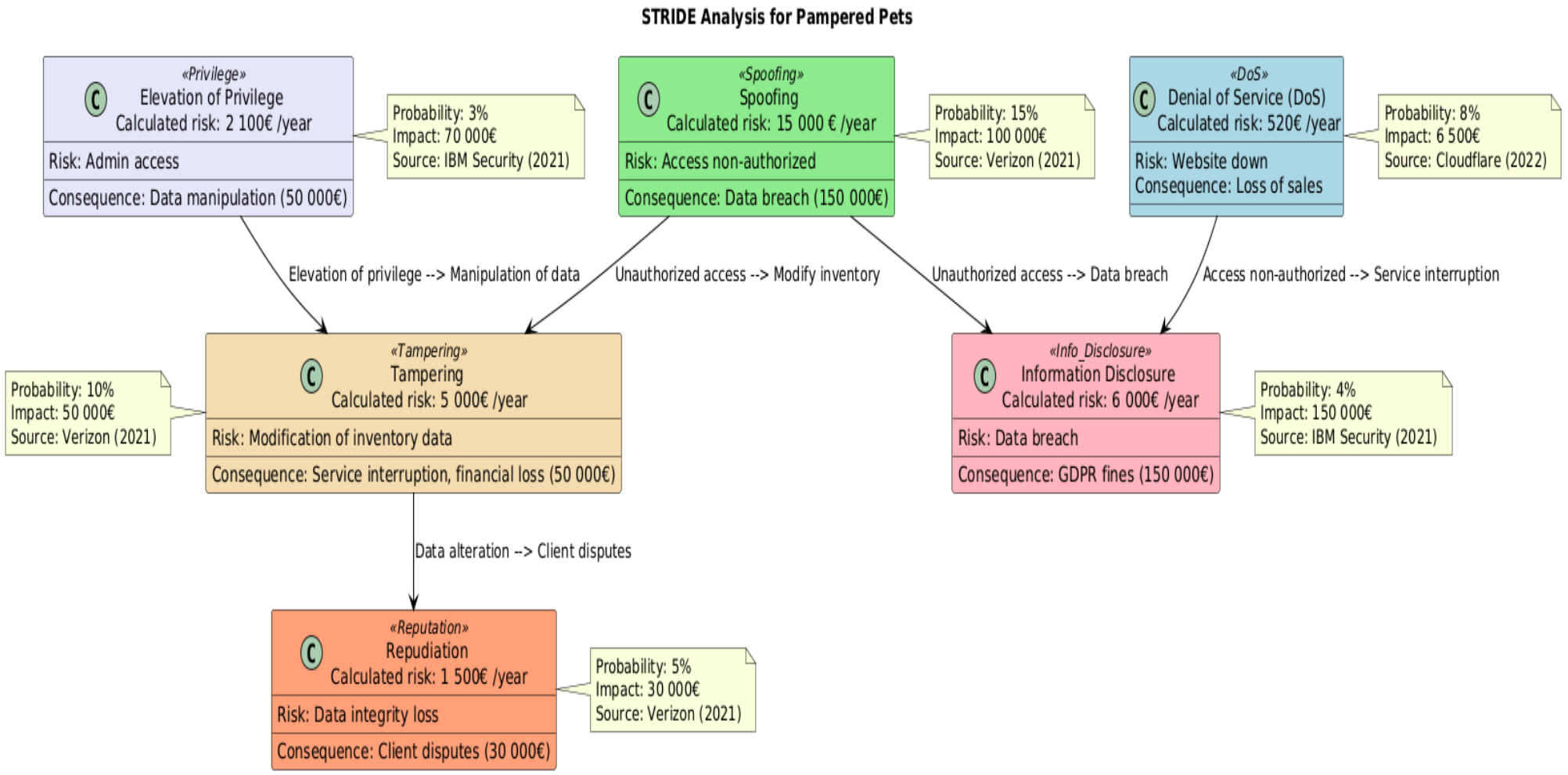
Pampered Pets chooses a cloud solution to meet the requirements set by O'dour. The cloud option is more scalable, resilient, and cost-efficient (Cloudflare, 2022). A multi-cloud environment, incorporating AWS, Azure, and GCP, ensures continuous data replication and rapid disaster recovery, thereby providing business continuity and robust data protection.

I. Identifying Potential Risks

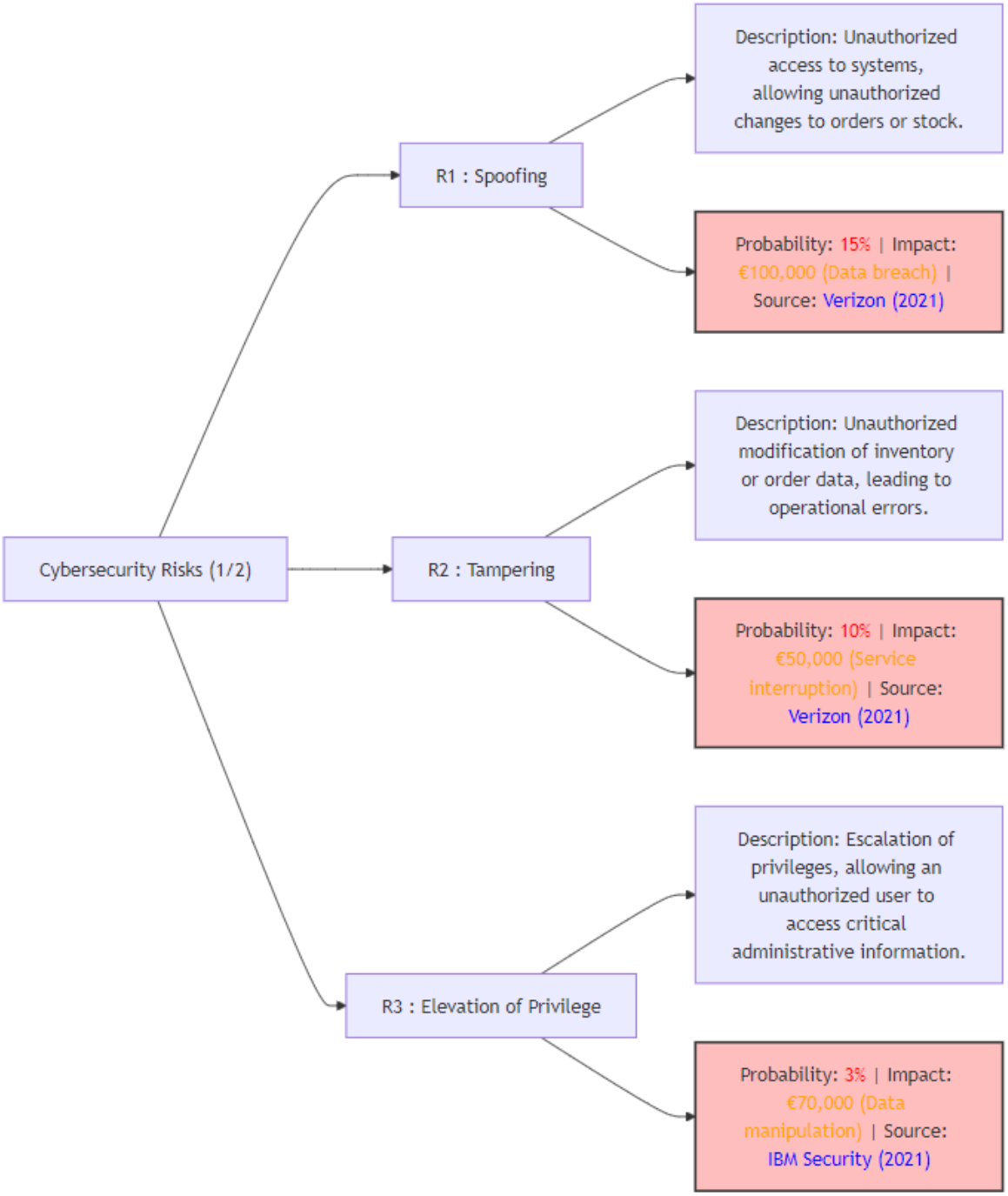
Several risks are identified, affecting both product quality and the security of the supply chain. These risks are modeled using quantitative approaches, allowing an estimation of their likelihood of occurrence and financial impact. The methods used include **STRIDE, Risk Breakdown Structure (RBS), Monte Carlo, FMEA, Bayesian Networks,** and **Quantitative Risk Assessment (QRA)**, each justified by its relevance to the critical aspects of the business.

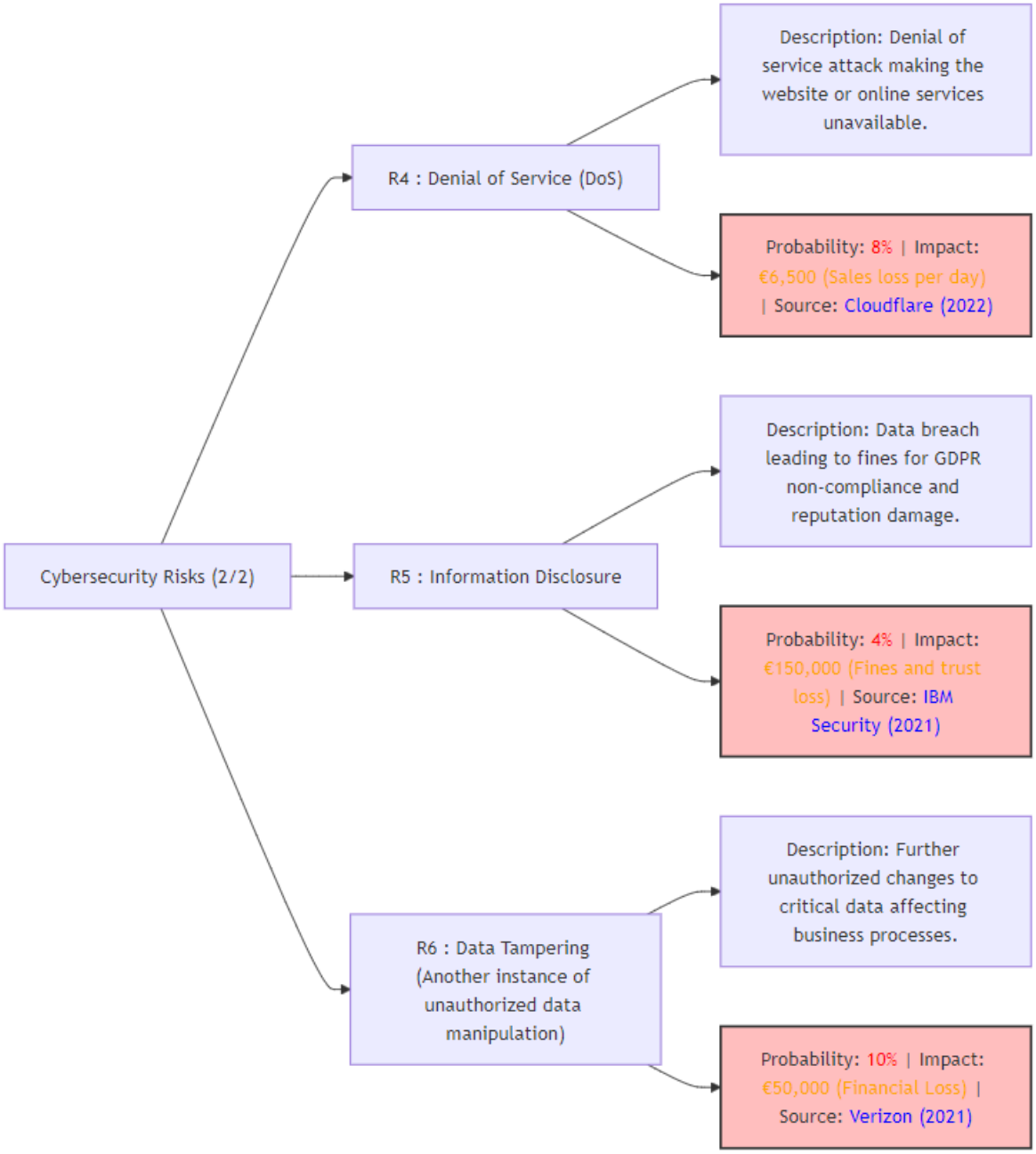
Quantitative Risk Modeling Approaches

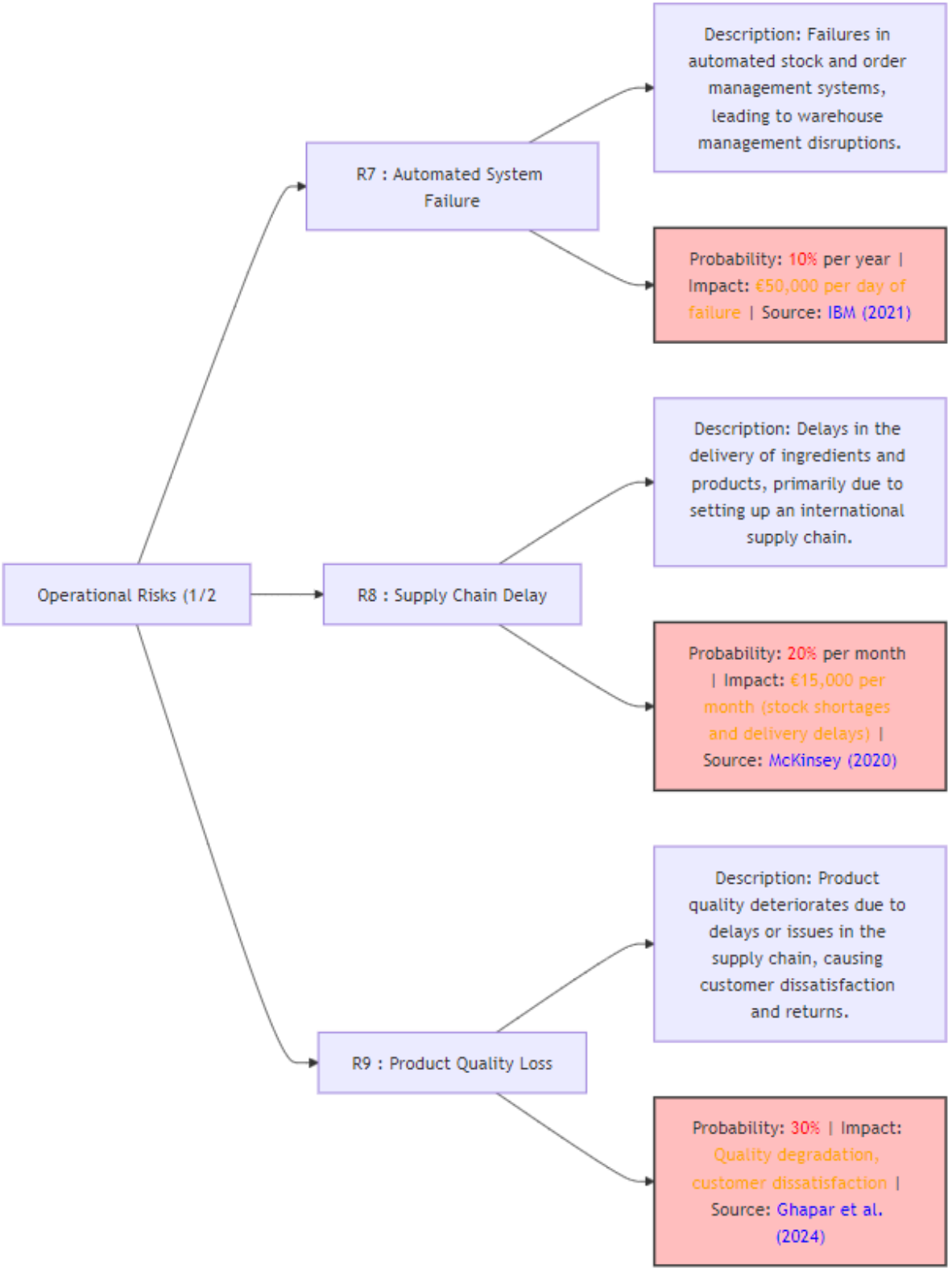
Initially, the **STRIDE** method is used to identify digital risks related to the security of Pampered Pets' systems and data as part of its digital transformation (Hubbard, 2019, p. 140). This approach, focused on digital threats, helped to identify the following risks:

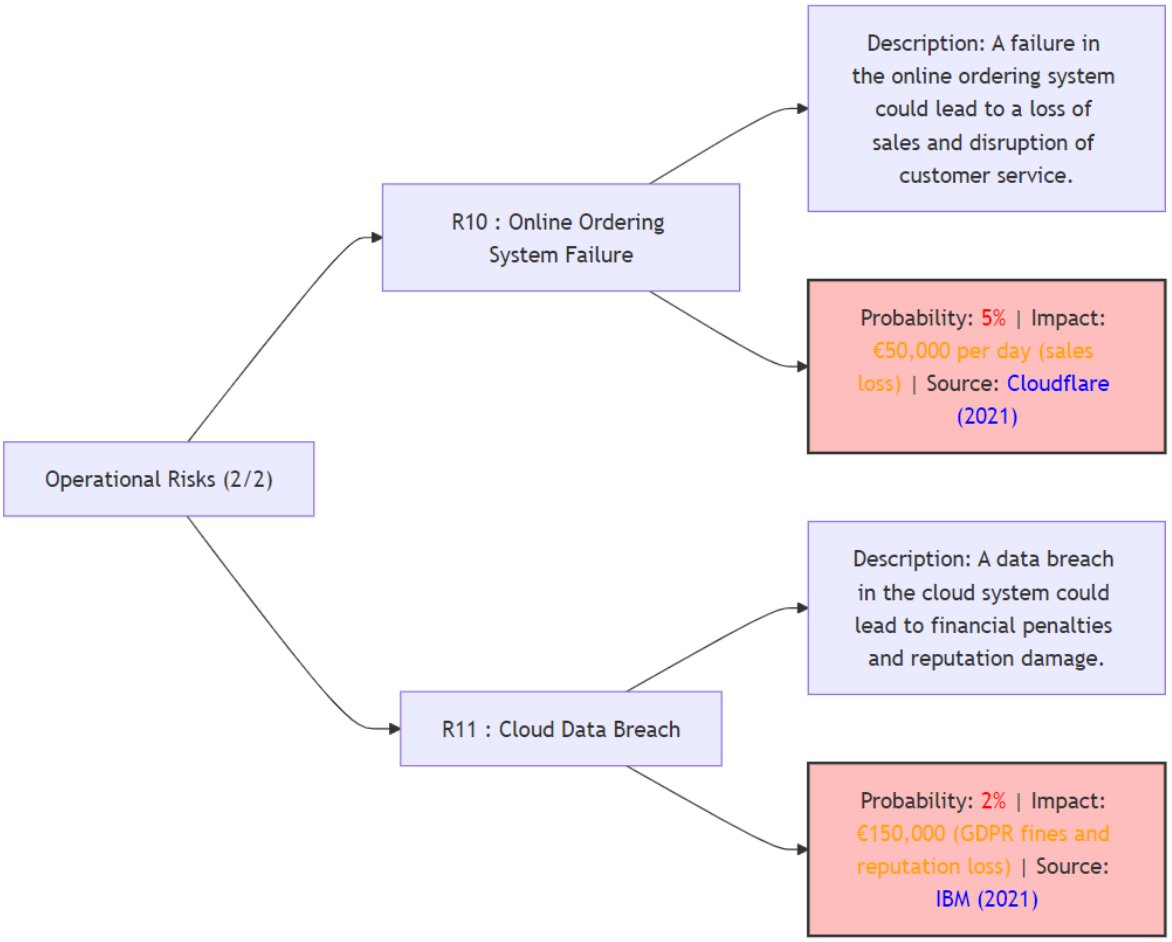

STRIDE Analysis for Pampered Pets
«Privilege»
Elevation of Privilege
Calculated risk: 2 100€ /year
Risk: Admin access
Consequence: Data manipulation (50 000€)
Probability: 3%
Impact: 70 000€
Source: IBM Security (2021)
«Spoofing»
Spoofing
Calculated risk: 15 000 € /year
Risk: Access non-authorized
Consequence: Data breach (150 000€)
Probability: 15%
Impact: 100 000€
Source: Verizon (2021)
«DoS»
Denial of Service (DoS)
Calculated risk: 520€ /year
Risk: Website down
Consequence: Loss of sales
Probability: 8%
Impact: 6 500€
Source: Cloudflare (2022)
Elevation of privilege --> Manipulation of data
Unauthorized access --> Modify inventory
Unauthorized access --> Data breach
Access non-authorized --> Service interruption
«Tampering»
Tampering
Calculated risk: 5 000€ /year
Risk: Modification of inventory data
Consequence: Service interruption, financial loss (50 000€)
Probability: 10%
Impact: 50 000€
Source: Verizon (2021)
«Info_Disclosure»
Information Disclosure
Calculated risk: 6 000€ /year
Risk: Data breach
Consequence: GDPR fines (150 000€)
Probability: 4%
Impact: 150 000€
Source: IBM Security (2021)
Data alteration --> Client disputes
«Reputation»
Repudiation
Calculated risk: 1 500€ /year
Risk: Data integrity loss
Consequence: Client disputes (30 000€)
Probability: 5%
Impact: 30 000€
Source: Verizon (2021)

After, it is essential to structure these risks and other threats through a **Risk Breakdown Structure (RBS)**. This approach provides a comprehensive overview of both digital and operational risks.




Cybersecurity Risks (2/2)
R4 : Denial of Service (DoS)
Description: Denial of service attack making the website or online services unavailable.
Probability: 8% | Impact: €6,500 (Sales loss per day) | Source: Cloudflare (2022)
R5 : Information Disclosure
Description: Data breach leading to fines for GDPR non-compliance and reputation damage.
Probability: 4% | Impact: €150,000 (Fines and trust loss) | Source: IBM Security (2021)
R6 : Data Tampering (Another instance of unauthorized data manipulation)
Description: Further unauthorized changes to critical data affecting business processes.
Probability: 10% | Impact: €50,000 (Financial Loss) | Source: Verizon (2021)


Operational Risks (1/2
R7 : Automated System Failure
Description: Failures in automated stock and order management systems, leading to warehouse management disruptions.
Probability: 10% per year | Impact: €50,000 per day of failure | Source: IBM (2021)
R8 : Supply Chain Delay
Description: Delays in the delivery of ingredients and products, primarily due to setting up an international supply chain.
Probability: 20% per month | Impact: €15,000 per month (stock shortages and delivery delays) | Source: McKinsey (2020)
R9 : Product Quality Loss
Description: Product quality deteriorates due to delays or issues in the supply chain, causing customer dissatisfaction and returns.
Probability: 30% | Impact: Quality degradation, customer dissatisfaction | Source: Ghapar et al. (2024)

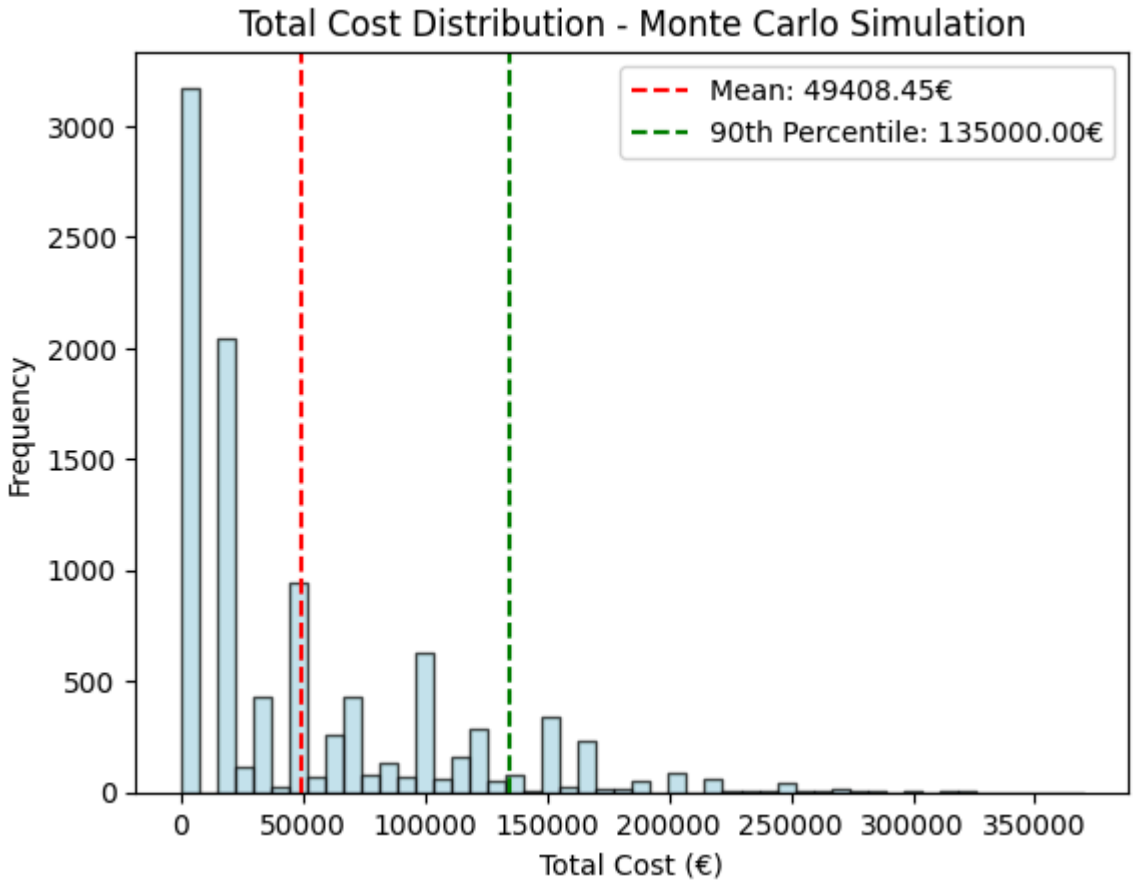


The RBS allows for the classification of risks. **Monte Carlo simulation** is used to better quantify the probabilities and financial impacts of these risks, considering multiple and complex scenarios.

During this simulation, the various identified risks are grouped into nine categories to simplify the analysis.

Risk	Probability	Impact (€)
Automated System Failures and Online Command Failures	15%	50 000 €
Supply Chain Delays	20%	15 000 €
Data Breach and Information Disclosure	6%	150 000 €
Product Quality Loss	30%	20 000 €
Spoofing and Unauthorized Access	15%	100 000 €
Tampering and Data Alteration	10%	50 000 €
Denial of Service (DoS)	8%	6 500 €
Elevation of Privilege	3%	70 000 €
Repudiation (Non-recognition of actions)	5%	30 000 €

Monte Carlo simulation, based on the individual probabilities of each risk, quantifies the financial impacts on Pampered Pets according to different possible scenarios (Hubbard, 2019, p. 120-125; Olson & Wu, 2019, p. 144-146). With 10,000 iterations, the average cost and the 90th percentile are estimated, offering a better understanding of the potential risks the company faces. This type of simulation is essential for anticipating costs related to high-risk events.



Results

On average, Pampered Pets could face costs of approximately €49,408.45 per year due to the identified risks, with a 90% chance that these costs will not exceed €135,000.00.

Once the risks are grouped, each risk and its impact is evaluated through a **Failure Modes and Effects Analysis (FMEA)**. This allows for prioritization of risks based on their severity, frequency, and detectability, and calculating a Risk Priority Number for each risk (Stamatis., 2003).

Identified risks	Potential Failure Mode	Potential Failure Effect	Severity (S)	Justification for Severity	Potential Causes	# Occurrence (O)	Detectability (D)	Justification for Detectability	RPN (S * O * D)
Product Quality Loss	Reduced customer satisfaction, increased returns	Product quality degradation	7	The impact is high because product quality is a crucial element of customer satisfaction and could lead to repeated losses if left unchecked.	Delivery delays, inadequate storage conditions	6	6	Quality control helps detect some losses, but delays add uncertainty to detection.	252
Automated System Failures and Online Command Failures	Delays in order processing	Customer dissatisfaction, revenue loss	8	The impact is high, but not catastrophic, as a backup solution could be put in place in the short term. However, the costs and disruptions are significant.	Technical failure, cyber attacks, outdated infrastructure	4	5	These failures can be difficult to anticipate without real-time monitoring but can be detected quickly through system alerts.	160
Elevation of Privilege	Unauthorized modifications to critical systems, data loss	Sabotage or unauthorized system modifications	6	The impact is moderate, as while system manipulation is serious, it can be contained with disaster recovery solutions.	Weak access controls, insufficient user monitoring	5	5	Privilege elevation can be detected with audit and monitoring systems, though they may not always alert immediately.	150
Denial of Service (DoS)	Website functionality loss, revenue loss	Website inaccessible, disruption of sales	4	The impact is low to moderate, as while it may result in lost revenue, DoS attacks can be mitigated or blocked quickly.	External attacks, system vulnerabilities	6	6	DoS attacks are easy to detect once they start but difficult to anticipate.	144
Repudiation (Non-recognition of actions)	Disputes, financial penalties, operational inefficiency	Conflicts over responsibility for actions	5	The score is moderate, as logging systems help limit disputes, but it may take time to resolve these issues.	Poor action logging, lack of traceability	4	7	Action traceability may fail, justifying a high detectability score.	140

Identified risks	Potential Failure Mode	Potential Failure Effect	Severity (S)	Justification for Severity	Potential Causes	#	Occurrence (O)	Detectability (D)	Justification for Detectability	RPN (S * O * D)
Tampering and Data Alteration	Financial loss, operational disruption	Incorrect modification of stock or data	5	The score is moderate, as these errors can be corrected with additional controls, but they would affect operational management and finances.	Insider threat, weak data integrity controls		5	5	It's possible to detect these alterations, but it's not guaranteed, hence a medium score.	125
Supply Chain Delays	Delivery delays, product shortages	Customer dissatisfaction, financial loss	7	The impact is significant, especially if customers are affected on a large scale.	Customs delays, supplier issues, poor inventory management		4	4	Many delays are predictable, but sudden disruptions, such as customs delays, are harder to forecast.	112
Spoofing and Unauthorized Access	Unauthorized access to customer data, manipulation of orders or stock	Alteration of customer data	6	The impact is moderate, as unauthorized access to data could be discovered quickly, but initial damages could be significant.	Weak authentication methods, phishing attacks		4	4	Access surveillance helps, but it's insufficient for detecting all attempts.	96
Data Breach and Information Disclosure	Legal penalties (GDPR), reputation damage, customer trust loss	Loss of customer information	9	The score is high due to legal consequences and reputational impacts, which are critical aspects for any company handling sensitive customer data.	Weak data encryption, phishing attacks		3	3	Detecting a data breach is often reactive, which justifies a low detectability score.	81

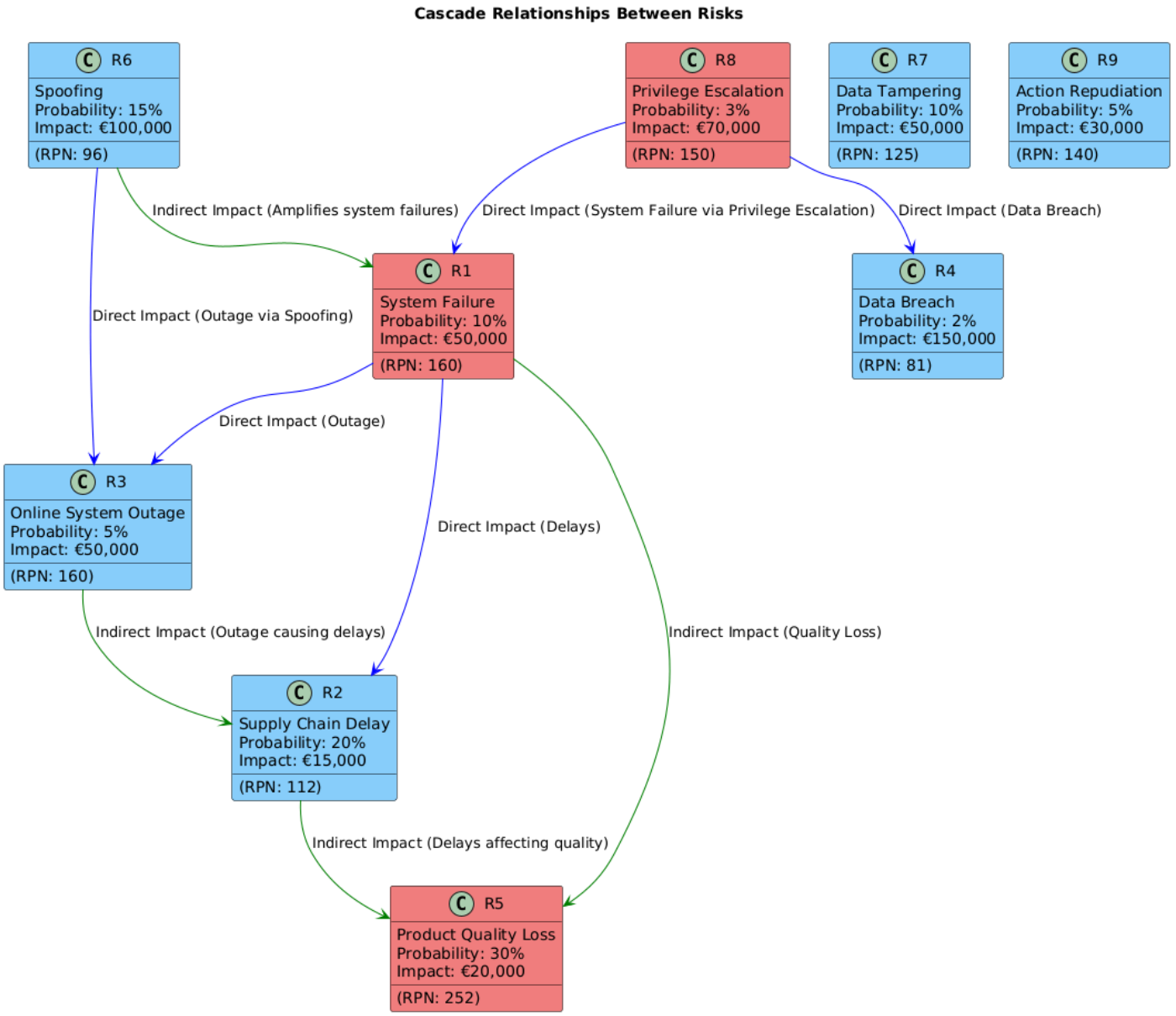
The FMEA analysis prioritizes the risks according to their RPN, enabling the identification of the most critical risks to address first. These include product quality loss, automated system failures, and online ordering system outages, which have the highest RPN values.*Recommendations will be provided in subsequent sections*.

FMEA reveals critical risks, but to better understand the interdependencies between these risks, a **Bayesian Network** model is used to analyze potential cascading effects (Griffiths, p. 35).

It is crucial to understand that risks should not be considered in isolation but within the context of their interdependencies. However, analyzing more than three or four factors simultaneously can lead to cognitive overload, making it difficult to make informed decisions. According to Simon (1997), decision-makers are limited in their ability to process multiple variables at once, and overly complex analysis can impair decision quality.

Bayesian Networks are chosen to model the complex relationships between interdependent risks, while taking this cognitive limitation into account.

This method provides a systemic view of the interdependencies within the organization *without carrying out detailed conditional and joint probability calculations*, not conducted due to a lack of sufficient statistical data. The individual probabilities identified are based on sectoral data, and the modeled causal relationships and key variables include:



The **Quantitative Risk Assessment (QRA)** method quantifies the financial impact of combined risks, providing a more accurate estimate of their potential effect on business. It provides a structured approach to estimating the economic impact of multiple combined risks. Hubbard (2019) stresses the importance of using QRA for evaluating complex risk interactions, especially in highly interconnected systems.

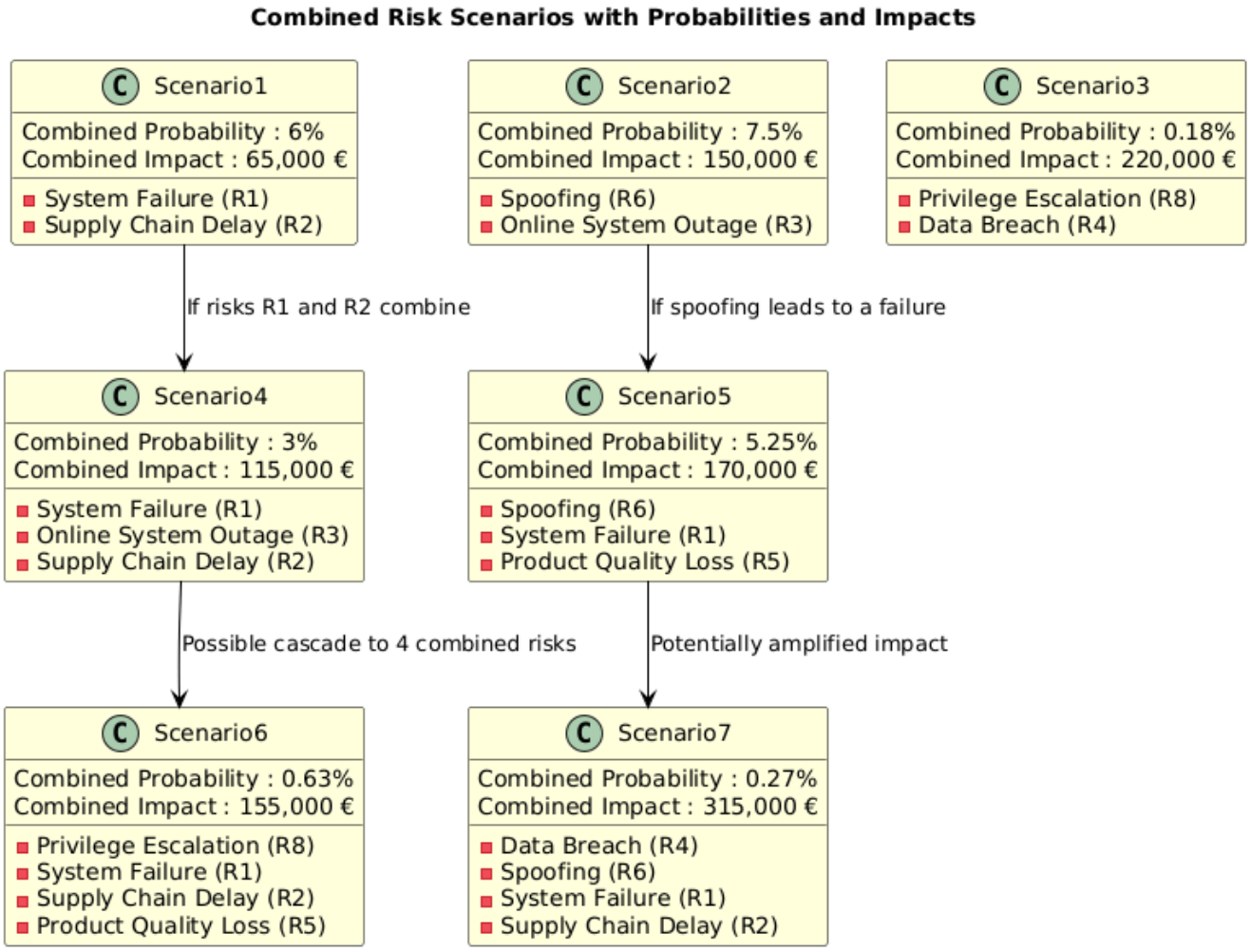
Several scenarios are created by combining the probabilities and impacts of individual events to estimate the total effect of interdependent risks. Conditional probabilities for each combination are calculated to understand the magnitude of the most risky scenarios.

For each scenario, the combined probability:

$P(Scenario) = P(R1) \times P(R2) \times ... \times P(Rn)$

The financial impacts:

$Impact\ total = Impact(R1) + Impact(R2) + ... + Impact(Rn)$



The extended QRA analysis reveals that certain combinations of risks, although unlikely, lead to significant financial impacts. The most concerning scenarios involve system failures combined with supply chain delays and product quality loss.

This exhaustive analysis shows that proactive management of critical risks is crucial to minimizing the negative impacts of Pampered Pets' digital transformation. By combining the approaches of STRIDE, RBS, Monte Carlo simulation, FMEA, Bayesian Networks, and QRA, risks are not only identified and quantified but their interactions and cascading effects are also modeled. This provides a clear estimate of probabilities and financial impacts. By

prioritizing the most critical risks, Pampered Pets will not only succeed in its digital transition but also protect its operations from major disruptions.

Results Summary

The quantitative risk analysis highlights the following critical risks:

- **Product quality loss** – primarily due to supply chain delays affecting the quality of raw materials and finished products. **Impact: €20,000** | 30%,
- **Automated system and online order failures** – causing disruptions in warehouse management and order processing. **Impact: €50,000 per day of downtime** | 15%,
- **Supply chain delays** – leading to stock shortages and a decline in product quality. **Impact: €15,000 per month** | 20%,

Risk aggravation scenarios have also been identified:

- Automated system failure + supply chain delays – **Impact: €65,000** | **3%**,
- Supply chain delays + product quality loss – **Impact: €35,000** | **6%**,
- Privilege escalation + system failure –, **Impact: €120,000** | **0.45%**

These results emphasize the need for proactive risk management to mitigate negative impacts.

II. Recommendations

Outsourcing of cybersecurity and critical infrastructure management

With digital transformation, including an international supply chain and automated warehouses, outsourcing cybersecurity allows the company to benefit from specialized expertise and flexible cost management (Willcocks, L., and Lacity, M. 2012). This approach would also ensure regulatory compliance (see **APPENDIX 1**). Additionally, outsourcing the management of critical infrastructure guarantees business continuity in case of system failure (through monitoring and intervention) and helps distribute operational risks more effectively.

Key Standards and Measures to Ensure Compliance

Pampered Pets must ensure that its operations comply with the main security and risk management standards.

- **GDPR**: Protection of personal data through regular audits, clear privacy policies, and encryption of sensitive data.
- **ISO/IEC 27001**: Implementation of an Information Security Management System (ISMS), strict management of access to critical information, and regular testing to identify vulnerabilities.
- **ISO 22301**: Establishment of a Business Continuity Plan (BCP) with a disaster recovery strategy for critical systems, ensuring that Pampered Pets can continue operations in the event of a major disruption.

- **PCI DSS**: Securing online credit card transactions with encryption systems and regular monitoring of transactions to ensure their integrity.
- **ISO 9001**: Implementation of a Quality Management System (QMS), conducting regular quality audits, and ensuring continuous improvement of production processes.
- **ISO 28000**: Management of logistical risks through the integration of buffer stocks, monitoring supplier performance, and implementing a risk management plan.
- **NIS2**: Strengthening cybersecurity for critical infrastructures with incident management protocols and regular communication with competent authorities in the event of a cyberattack.

FMEA

Identified risks	Potential Failure Mode	Potential Failure Effect	RPN (S * O * D)	Points of Vigilance and Recommended Actions
Product Quality Loss	Reduced customer satisfaction, increased returns	Product quality degradation	252	Set up real-time quality monitoring systems, and maintain quality standards throughout the supply chain.
Automated System Failures and Online Command Failures	Delays in order processing	Customer dissatisfaction, revenue loss	160	Ensure system architecture redundancy, plan regular updates, and implement continuous monitoring.
Elevation of Privilege	Unauthorized modifications to critical systems, data loss	Sabotage or unauthorized system modifications	150	Strengthen access control policies, implement detailed privilege management, and frequently audit access logs.
Denial of Service (DoS)	Website functionality loss, revenue loss	Website inaccessible, disruption of sales	144	Introduce protection systems against DoS attacks (e.g., firewalls, DDoS mitigation), and regularly update security infrastructure.
Repudiation (Non-recognition of actions)	Disputes, financial penalties, operational inefficiency	Conflicts over responsibility for actions	140	Set up robust logging systems, improve action traceability, and establish protocols for dispute resolution.
Tampering and Data Alteration	Financial loss, operational disruption	Incorrect modification of stock or data	125	Implement data integrity controls, ensure proper access control to sensitive data, and monitor unusual changes.
Supply Chain Delays	Delivery delays, product shortages	Customer dissatisfaction, financial loss	112	Improve supplier management, optimize stock forecasting, and ensure proper anticipation and control of customs procedures.
Spoofing and Unauthorized Access	Unauthorized access to customer data, manipulation of orders or stock	Alteration of customer data	96	Deploy multi-factor authentication, monitor suspicious login activities, and raise staff awareness of phishing risks.
Data Breach and Information Disclosure	Legal penalties (GDPR), reputation damage, customer trust loss	Loss of customer information	81	Implement robust data encryption, enable multi-factor authentication (MFA), and train employees on phishing risks.

Other recommendations

Strengthening system resilience

- **Preventive maintenance** with regular checks and ensure redundancy for critical systems to prevent outages.
- **Real-time monitoring** tools to quickly respond to disruptions.

Improving supply chain management

- Reduce reliance on a single supplier by expanding the supplier base.
- Establish buffer stocks for key components to limit the impact of delays.

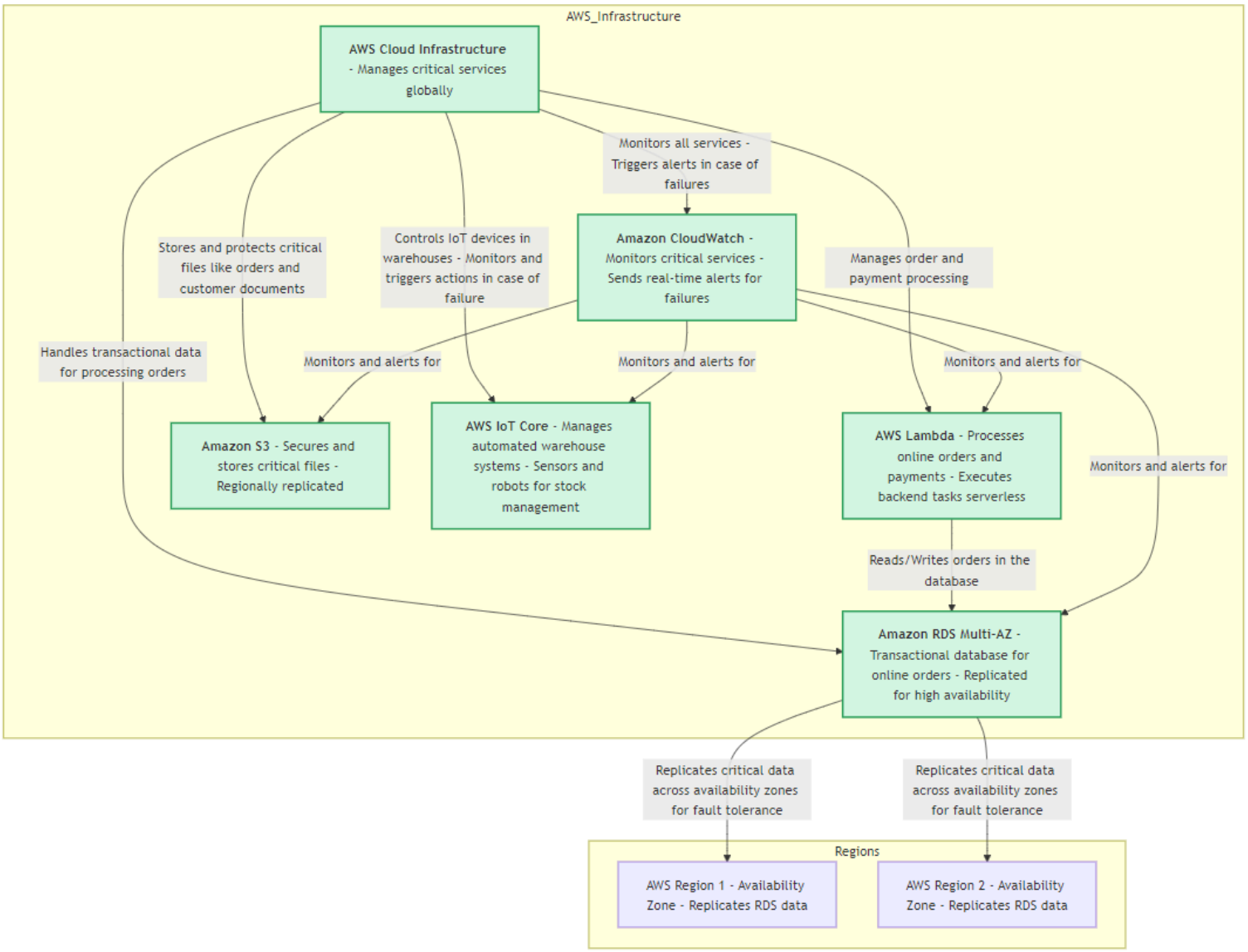
Proactive quality risk management

- Implement stricter quality control processes for both raw materials and finished product (Hoyle, D. 2009).
- Establish strict contracts to ensure timely deliveries and maintain the quality of raw materials.

III. Business Continuity and Disaster Recovery Strategy

Pampered Pets is adopting a multi-cloud architecture with Amazon Web Services, Microsoft Azure, and Google Cloud Platform to ensure resilience, scalability, and operational continuity.
This architecture is specifically designed to meet a Recovery Point Objective of one minute and a Recovery Time Objective of less than one minute while minimizing identified risks (Smith, Green & Clarke, 2024), such as failures in automated systems and online ordering, supply chain delays, and product quality loss.

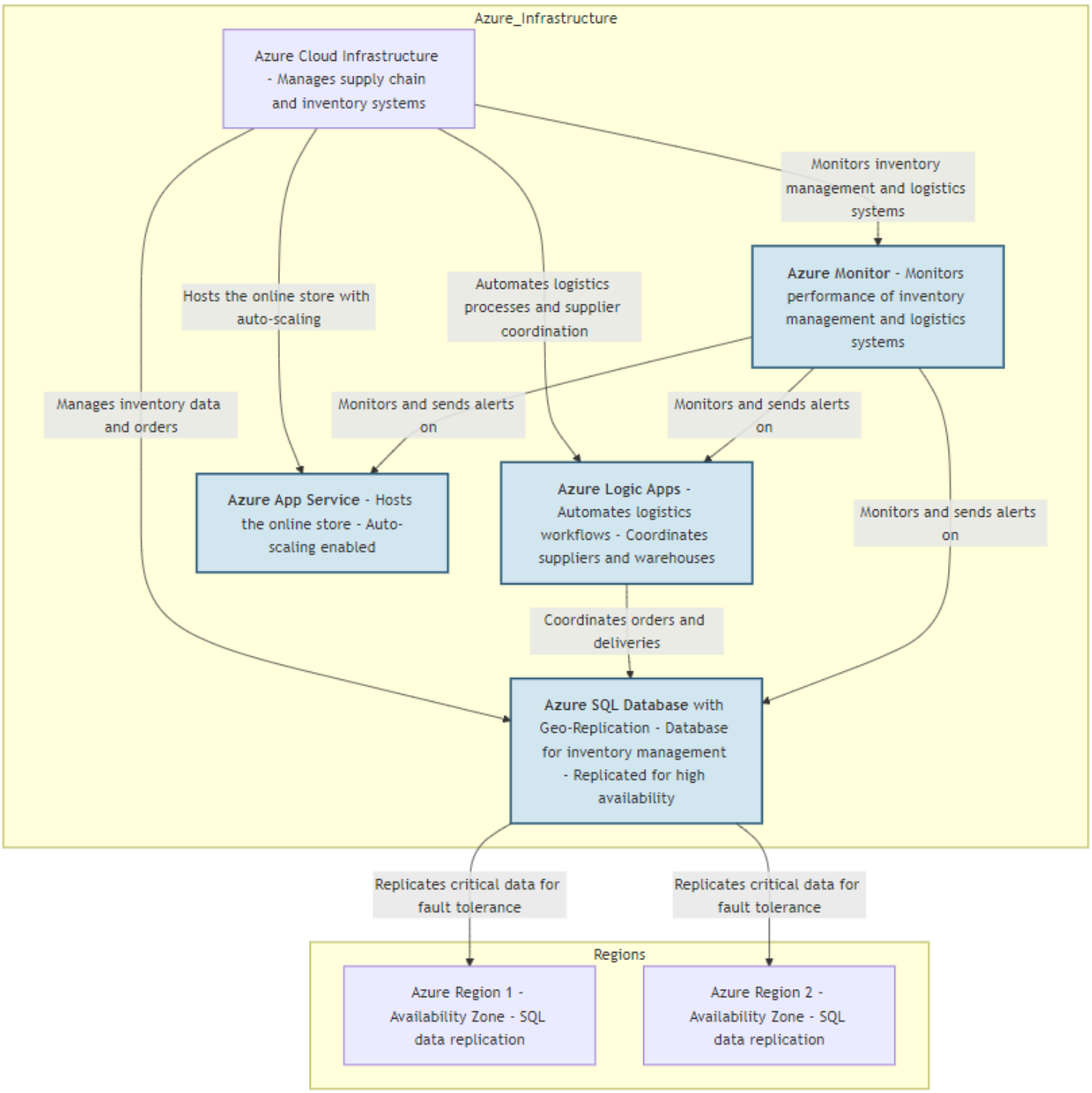
AWS Infrastructure – Management of Critical Systems



AWS architecture manages the critical services: Amazon CloudWatch monitors essential systems (databases and warehouse automation) in real-time and triggers alerts in the event of a failure. Online transactions are processed via Amazon RDS Multi-AZ, a database distributed across multiple availability zones to ensure fault tolerance and fast automatic failover (Doe, 2024). Critical files, such as orders, are securely stored in Amazon S3 with cross-region replication.

Backend processes related to orders and payments are executed by AWS Lambda, a serverless service that allows flexible and scalable management. Finally, AWS IoT Core manages the automated systems in warehouses, monitoring sensors and robots to trigger actions in case of a failure.

Azure Infrastructure – Stock and Supply Chain Management



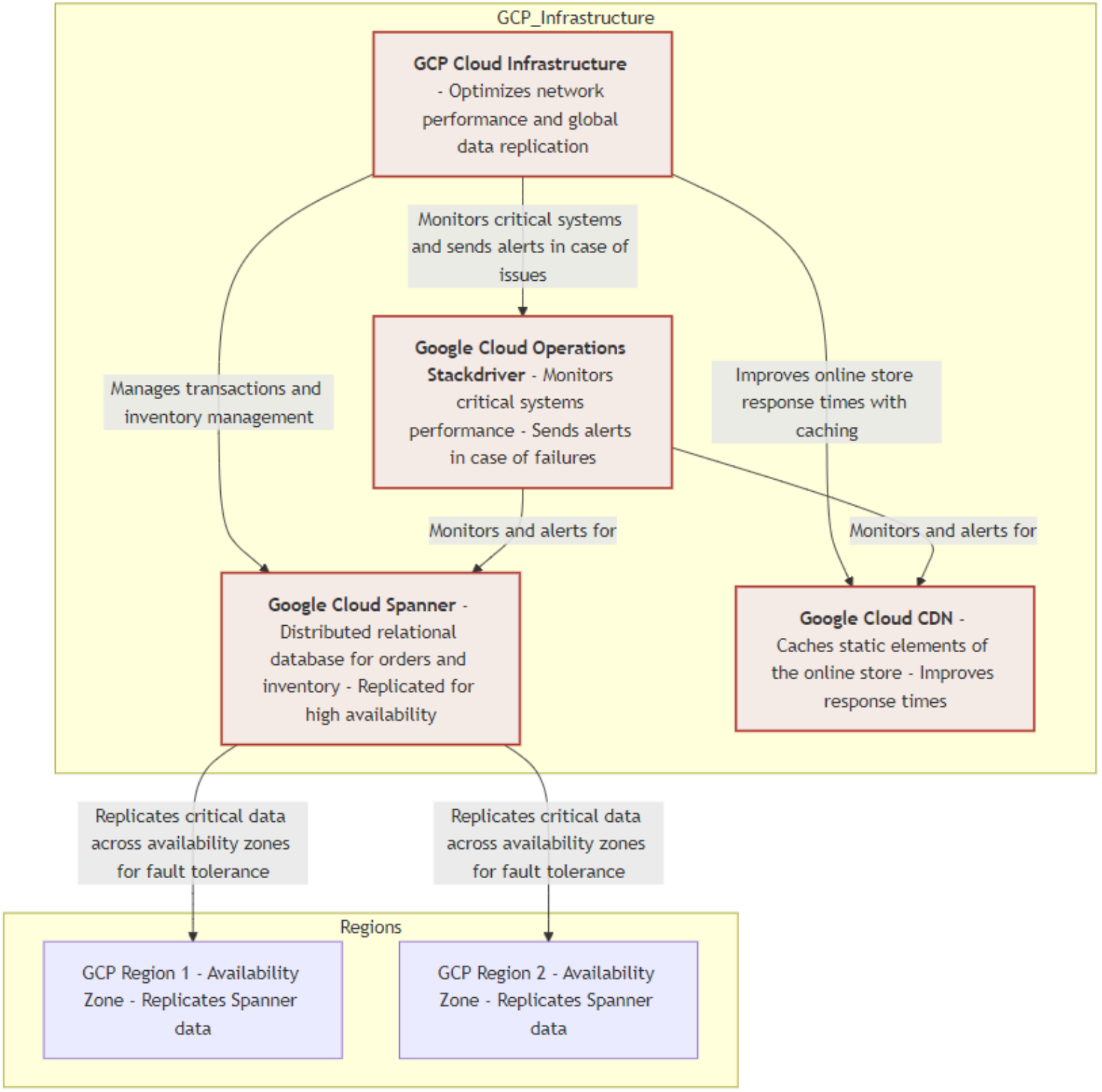
Azure manages Pampered Pets' supply chain and stock: Azure SQL Database ensures the replication of critical data (stocks and orders) between multiple regions, guaranteeing high availability and real-time synchronization of information.

Azure Logic Apps automates logistics processes, enabling smooth coordination between suppliers and automated warehouses, thus reducing potential delays (Johnson, Lee & Martinez, 2024). Azure App Service hosts the online store, offering automatic scalability based on user demand.

Finally, Azure Monitor monitors stock management systems and logistics performance in

real-time, sending alerts in case of failures, enabling proactive adjustments to prevent interruptions.

GCP Infrastructure – Network Performance Optimization and Data Replication



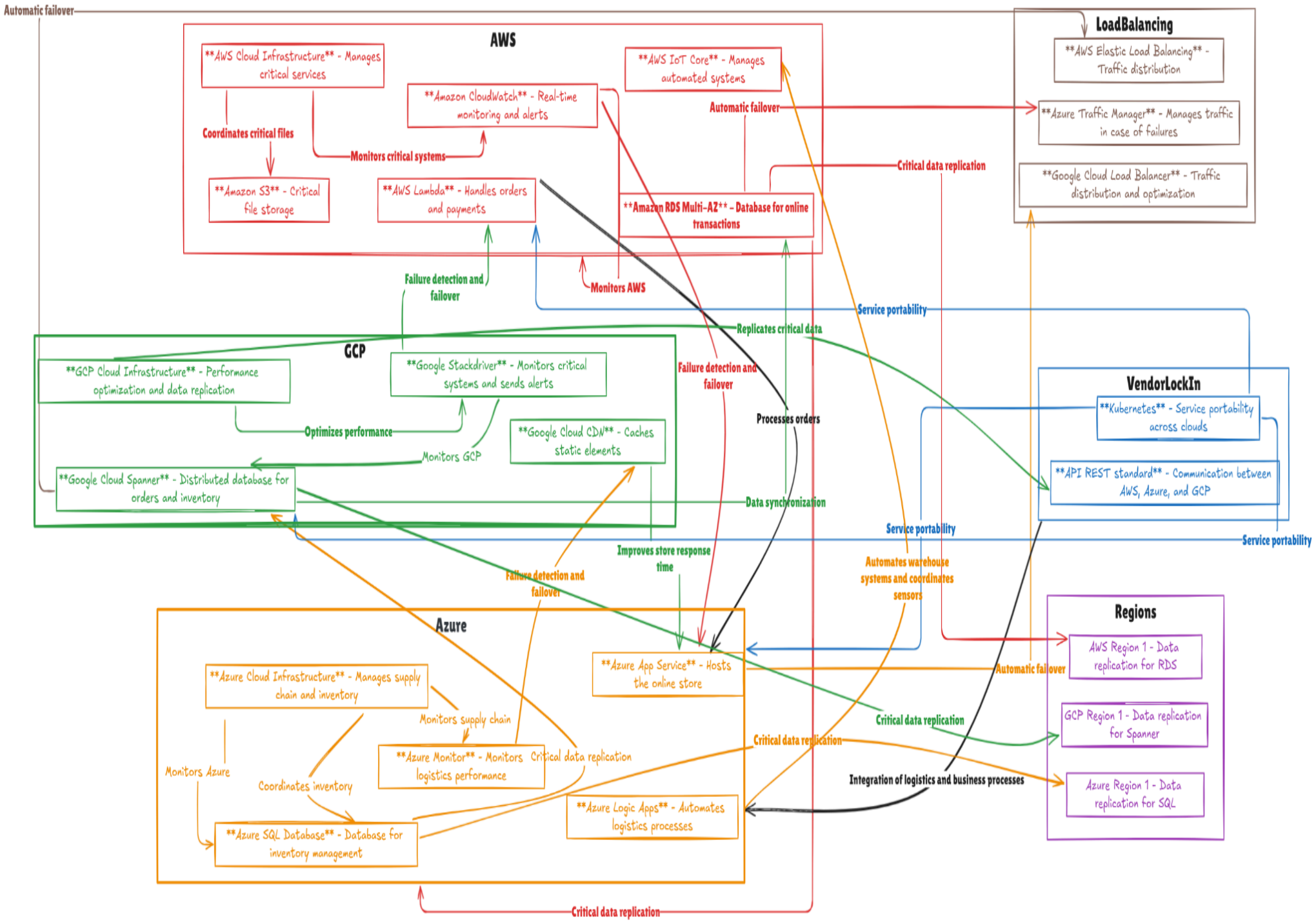
GCP optimizes network performance and ensures global replication of critical data: Google Cloud Spanner, a distributed relational database, manages global transactions and stock

information, with real-time replication to ensure high availability.
Google Cloud CDN is used to cache static elements of the online store, such as images and product descriptions, improving response times for users. Google Cloud Operations (Stackdriver) monitors the performance of critical systems hosted on GCP, sending alerts in case of problems to enable rapid intervention.
This system guarantees service continuity in case of a failure while optimizing network performance and user experience.

BC and DR

Multi-cloud strategy with AWS, Azure, and GCP ensure business continuity (BC) and disaster recovery (DR): high service availability, fast recovery in case of failure, and flexible management to avoid dependence on a single vendor (vendor lock-in) (Brown, 2024), as shown in the following diagram.

Multi-Platform Interaction for Pampered Pets' Resilience



The interactions between platforms ensure the resilience of infrastructure in the event of a failure or critical malfunction. This approach ensures business continuity (BC) and rapid disaster recovery (DR), meeting the needs for high availability, quick recovery, and flexibility to avoid vendor lock-in.

Failure Detection and Automatic Failover: Real-time monitoring systems such as AWS CloudWatch, Azure Monitor, and Google Cloud Operations continuously monitor the availability of services on each platform. In case of failure, these systems automatically trigger a failover to another available platform, such as AWS Elastic Load Balancer, Azure Traffic Manager, or Google Cloud Load Balancer. This mechanism ensures uninterrupted continuity of critical services (transactions, stock management, etc.).

Data Replication and Rapid Recovery: Critical data (orders, stock management) is replicated in real-time across multiple availability zones and platforms through services like Amazon RDS, Azure SQL Database, and Google Cloud Spanner. This continuous replication ensures minimal data loss (RPO of one minute) and quick service recovery (RTO of one minute), ensuring that operations continue without major disruptions even in case of a disaster.

Flexibility and Reduction of Vendor Lock-In:

- multi-cloud limit dependence on a single provider.
- Open technologies and standards (Kubernetes) allow container orchestration and the deployment of applications on any cloud provider, ensuring service portability between AWS, Azure, and GCP (Adams, 2024).
- Open APIs and microservices ensure maximum interoperability.
- Multi-cloud compatible services for the migration of services between platforms, offering greater flexibility in case of provider change (Terraform, Cloud Foundry).
- Flexible contractual clauses.

Regular Migration and Resilience Testing

Auto-Scalability and Cost Optimization

Failback (Return to Normal): Once the faulty platform is restored, systems gradually return to their initial state via a failback process, redirecting traffic and services to the original platform.

Conclusion

Pampered Pets identifies critical risks: product quality loss, automated system failures, and supply chain delays. Quantitative methods reveal the financial impacts. Recommendations include outsourcing cybersecurity, diversifying suppliers, and strengthening quality control. The multi-cloud strategy ensures resilience, scalability, and security. Through proactive monitoring and robust failover systems, Pampered Pets guarantees continuous operations 24/7, 365 days a year.

References

- Cloudflare (2022). Best practices for mitigating DDoS attacks. Cloudflare. Available at: https://cf-assets.www.cloudflare.com/slt3lc6tev37/58Znmio29pRXDLKoQgNIz4/5cf1a6d3b1b1f5f1ea995460e04eb512/BDES-2587-Design-Wrap-Refreshed-DDoS-White-Paper-Letter.pdf [Accessed 29 September 2024].
- Hubbard, D., 2019. *The Failure of Risk Management*. Chapter 7, p. 140. New York: Wiley.
- IBM (2021). *Cost of a Data Breach Report*. IBM Security. Available at: https://www.ibm.com/security/data-breach [Accessed 29 September 2024].
- Verizon (2021). *Data Breach Investigations Report*. Verizon. Available at: https://www.verizon.com/business/resources/T26a/reports/2021-data-breach-investigations-report.pdf [Accessed 30 September 2024].
- Ghapar, F., Othman, N., Chew, L. L., Othman, A. K., Sundram, V. P. K. (2024). *Supply Chain Disruptions in the Food Manufacturing Industry*. Available at: https://www.europeanproceedings.com/article/10.15405/epsbs.2024.05.71 [Accessed 27 September 2024].
- McKinsey & Company, 2020. *Risk, Resilience, and Rebalancing in Global Value Chains*. McKinsey Global Institute. Available at: https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2020/2020-08-06%20mgi%20global%20value%20chains/risk-resilience-and-rebalancing-in-global-value-chains-full-report-vf.pdf [Accessed 29 September 2024].
- Hubbard, D., 2019. *The Failure of Risk Management*. Chapter 6, pp. 120-125. New York: Wiley.
- Olson, D.L. & Wu, D., 2019. *Enterprise Risk Management Models*. Chapter 6, pp. 144-146. Springer.
- Stamatis, D.H., 2003. *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. Milwaukee: ASQ Quality Press.
- Griffiths, P., *Think Bayes*. Section 2.1, p. 35. O'Reilly Media.
- Simon, H.A., 1997. *Models of Bounded Rationality: Empirically Grounded Economic Reason*. Vol. 3. Cambridge, MA: MIT Press.
- Willcocks, L. and Lacity, M. (2012). *The Outsourcing Enterprise: From Cost Management to Collaborative Innovation*. Palgrave Macmillan.
- Hoyle, D. (2009). *ISO 9001 Quality Systems Handbook*. Butterworth-Heinemann.

- Chopra, S. & Sodhi, M.S., 2004. *Managing Risk to Avoid Supply-Chain Breakdown*. MIT Sloan Management Review, 46(1), pp.53-61.
- Smith, T., Green, D. and Clarke, A. (2024). *Availability Modeling and Analysis of a Disaster-Recovery-as-a-Service Solution*. 2nd edn. Boston: CloudTech Press.
- Doe, M. (2024). *Evaluating Disaster Recovery Plans Using the Cloud*. San Francisco: Cloud Strategies Publishing, p. 7.
- Johnson, R., Lee, S. and Martinez, P. (2024). *Enterprise Risk Management Models*. 3rd edn. Oxford: Oxford University Press.
- Brown, J. (2024). *Critical Review of Vendor Lock-In and Its Impact on the Adoption of Cloud Computing*. New York: TechPress, p. 5.
- Adams, L. (2024). *Cloud Security Best Practices Derived from Mission Thread Analysis*. London: Cloud Security Institute, p. 22.