Louis Dodge

individual Project (Executive Summary)

**Index**

1. **Introduction**
2. **Key Risks and Frameworks for Identification** 
   * **2.1 Why Monte Carlo and FAIR?**
   * **2.2 Operational & Quality Risks (Monte Carlo)**
   * **2.3 Cyber & GDPR Risks (FAIR)**
3. **Assumptions and Calculations** 
   * **3.1 Operational Assumptions**
   * **3.2 Cost Assumptions**
   * **3.3 Operational Modelling Results**
4. **Operational Modelling Results**
   * **4.1 Total Cost Of Operating Supply Chain Risks**
   * **4.2 Breakdown By Risk Category**
5. **Cyber Security Risk**
   * **5.1 Unmitigated Risk Exposure**
   * **5.2 Risk Mitigation & Control Effectiveness**
6. **Technical Architecture & Data Protection Strategy** 
   * **6.1 High Level Architecture Overview**
   * **6.2 Key Architectural Decisions and Rationale**
   * **6.3 GDPR Compliance &Data Protection**
   * **6.4 Resilience and Recovery**
7. **Conclusion**
   * **7.1 Priority Recommendations**
   * **7.2 Summary**

# **Risk Assessment Report for Pampered Pets**

# 1. Introduction

Pampered Pets, originally a local store in Hashington-on-the-Water, is expanding internationally and has attracted the attention of two high profile customers - HRH the King and Prince Albert II of Monaco. The upcoming expansion involves the introduction of an international supply chain, automated warehouses and the launch of an e-commerce platform. While these initiatives support revenue growth, they also introduce new risks to product quality, logistics, cyber security and regulatory compliance. The following executive summary:

1. Uses Monte Carlo and Factor Analysis of Information Risk (FAIR) to estimate risk probabilities and potential financial, reputational and regulatory repercussions.

2. Maps each risk to impactful mitigations that minimize lost revenue, reputational harm, and regulatory noncompliance (particularly regarding GDPR).

3. Presents priority recommendations aligned with Ms. O’dour’s focus on operational resilience, brand reputation, and data protection.

# 2. Key Risks and Frameworks for Identification

# 2.1 Why Monte Carlo & FAIR?

Our analysis employs two complementary approaches to assess operational and cyber risks:

**Monte Carlo:**

Monte Carlo simulation was selected for operational risk modelling due to its ability to handle the complex variability inherent in global supply chains. The model allows us to effectively capture multiple interdependent factors (Mooney, 1997) including international shipping delays, manufacturing quality variations, and warehouse automation reliability. This approach is particularly valuable for identifying potential worst-case scenarios, such as compound events that could lead to significant service disruptions.

**FAIR:**

FAIR provides structured quantification of cyber security risks. The model estimates potential loss exposure by analysing specific risk scenarios, enabling us to understand where we are most vulnerable to cyberattacks (Phonpaseuth, n.d.) . This supports quantitative evaluation of security investments, allowing us to prioritise high impact mitigations.

Together, these models provide coverage of both physical operations and digital risks. This ensures we can effectively evaluate both the operational challenges of international growth and the cyber security implications of our digital transformation.

# 2.2 Operational & Quality Risks (Monte Carlo)

The tables below outline the top operational and cyber threats identified. For each risk, we highlight the underlying drivers, and both the immediate and secondary impacts should the risk materialize.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Category | Risk Drivers | Primary Impacts | Secondary Impacts |
| Shipping Delays | • Multiple handoff points  • International customs  • Introduction of complex supply chain  • Global transportation networks | • Missed VIP delivery commitments  • Perishable inventory loss  • Emergency shipping costs | • Brand reputation damage  • Loss of VIP clients  • Increased buffer stock costs |
| Quality/Defect Issues | • Loss of direct oversight  • New international suppliers  • Extended transit times  • Temperature variations | • Product spoilage  • Failed quality checks  • Returns and replacements | • Royal patron dissatisfaction  • Brand value erosion  • Market reputation loss |
| Automation Failures | • Complex system integration  • Multiple automation points  • 24/7 operation requirement  • Legacy system interfaces | • Order processing delays  • Manual intervention needs  • System recovery costs | • Supply chain disruption  • Client satisfaction impact  • Operational efficiency loss |

# 2.3 Cyber & GDPR Risks (FAIR)

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Event | Risk Drivers | Primary Impacts | Secondary Impacts |
| Data Breach | • Complex logistics system integration  • Multiple access points to data across supply chain  • International data flows | • GDPR fines up to 4% of global turnover (if personal data is exposed) (Eur-Lex, 2016, Art. 83(5))  • Shipping data manipulation  • Order system disruption | • Supply chain disruption  • Delivery failures  •Reputational Damage  • Loss of supply chain visibility |
| Warehouse Automation System Compromise | • Internet-connected control systems  • Automated picking/packing systems  • Remote management capabilities | • Operational shutdown  • System damage  • Safety system compromise | • Product spoilage  • Manual operation costs  • Extended recovery time |
| Supplier Network Infiltration | • Multiple international suppliers  • Shared system access (Keskin et al., 2021)  • Varying security standards across suppliers and partners | • Fraudulent orders  • Inventory manipulation  • Financial fraud | • Stock level disruption  • Partner trust damage  • Increased security costs |

# 3. Assumptions and Calculations

# 3.1 Operational Assumptions

Our Monte Carlo simulation was modelled to represent a year of operations. We ran the simulation for 5,000 iterations to generate a robust distribution of potential outcomes. Key model assumptions are outlined and justified below, as they underpin our calculations and influence the reliability of our conclusions. Calculations are available in the appendix.

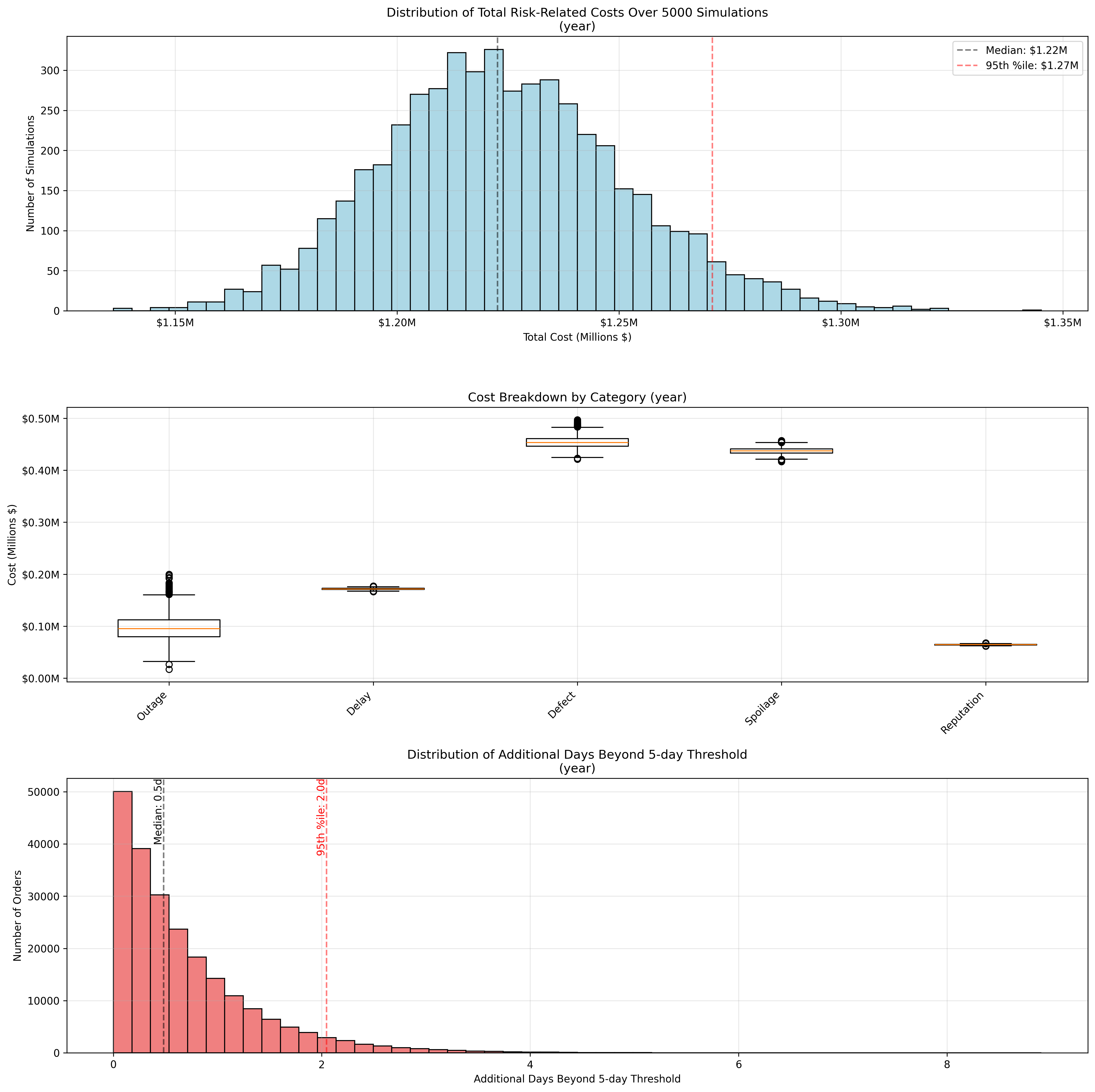
|  |  |  |  |
| --- | --- | --- | --- |
| Category | Distribution | Values | Justification |
| Shipping Times | Lognormal | μ=1.1, σ=0.5) | • Always positive  • Right-skewed delays (most deliveries near mean, long tail for delays)  • Results in ~3 day median delivery |
| Warehouse outages | Exponential (both length of outage, and mean time between failure) | MTBO = 60 days  MTTR = 4 hours | • Aligns with industry standard uptime AutoStore (n.d.)  • Standard model for random, independent failures (Gnedenko, B. and Ushakov, I.A., 1995) |
| Daily order volume | Normal | Mean = 1000/day  StD = 100 | • Central Limit Theorem suggests normal distribution  • 10% variation represents typical business fluctuation |
| Warehouse capacity | Equal distribution | 1/N per warehouse (e.g. downtime of one warehouse will reduce orders delivered during that period by 1/N) | • Simplified modelling approach. Represents a best guess given lack of data. |
| Spoilage Threshold | Temperature-dependent | Base = 6 days  Seasonal impact = 20% | • Large proportion of pet shop sales are perishable  • Products more likely to spoil in summer (Dagnas, S. and Membré, J.M., 2013) |
| Average Order Value | Fixed value | $50 | • Premium brand  • VIP Patronage increases average order value |

# 3.1 Cost Assumptions

|  |  |  |
| --- | --- | --- |
| Cause of cost | Value | Justification |
| Defects/Spoilage | $60/item | • 1.2x average order value is reasonable given replacement and shipping, as per Gustafsson, Jonsson and Holmström, (2021) |
| Warehouse Outage | $2000/hour per affected warehouse | • Covers operations disruption  • Need for parts, additional labour and recovery operations |
| Delay compensation | 5-6 days: $10  7-9 days: $20  10+ days: $30 | • Maintains customer loyalty  • Mitigates reputational risks |
| Reputational impact | $1.0/delay $2.0/defect $3.0/spoilage | • Delays, defects and spoilage harm brand perception and customer confidence |

# 4. Operational modelling results:

# 4.1 Total Cost Of Operating Supply Chain Risks



The distribution of operational risk costs shows a median annual impact of $1.22M, with a 95th percentile exposure of $1.27M. This tight distribution suggests our operational risk estimates are stable and reasonably predictable, with only a ~4% increase from the median to the 95th percentile.

# 4.2 Breakdown By Risk Category:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Category | Annual Impact (50th percentile) | Probability | Recommended Mitigation |
| Product Defects | $454,501 (37.1%) | 2.1% of orders (7,573 units) | • Develop supplier audit and training program  • Integrate AI image recognition to identify defects during production |
| Product Spoilage | $437,432 (35.7%) | 2.0% of orders (7,290 units) | • Temperature control supply chain  • Implement FEFO inventory management |
| Shipping Delays | $171,640 (14.0%) | 4.5% of orders (16,279 units) | • Model expected delays for different routes  • Dynamically route products |
| Warehouse Outages | $96,322 (7.9%) | Every 60 days (mean 4 hours) | • Implement predictive maintenance by modelling expected component lifetimes |
| Reputational Damage | $64,401 (5.3%) | N/A | • Actively monitor and respond to customer feedback using surveys, reviews, and social media monitoring. |

A screenshot of a graph

AI-generated content may be incorrect.

Product quality issues, comprising defects and spoilage, represent nearly three-quarters of our total risk exposure. Defects account for $454,401 (37.1%) of annual risk costs, while spoilage contributes $437,432 (35.7%). The box plots show these categories have relatively consistent impact levels, with limited variability compared to other risk types.

Operational disruptions, including shipping delays and warehouse outages, present a secondary but significant risk tier. Shipping delays generate $171,640 (14.0%) in annual costs, while warehouse outages contribute $96,322 (7.9%). Notably, warehouse outages drive shipping delays, which in turn exacerbate spoilage. Addressing these risks, despite their lower direct costs, could effectively reduce secondary impacts and overall risk exposure.

Reputational costs, while showing the lowest direct financial impact at $64,438 (5.3%), warrant attention given our VIP client base. The narrow distribution of these costs likely understates the potential long-term impact of reputation damage on our premium brand positioning.

# 5. Cyber Security Risk analysis

# 5.1 Unmitigated Risk Exposure:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Event | Loss frequency (Annual) | Loss Magnitude | Expected Annual Loss |
| Data Breach | 20% | $1.2 million (Department for Digital, Culture, Media & Sport [DCMS], 2023) | $240,000 |
| Warehouse Automation System Compromise | 12% | $330,000 | $39,600 |
| Compromise of Supplier/Partner Connectivity | 30% | $200,000 (ConnectWise, 2024) | $60,000 |

# 5.2 Risk Mitigation and Control Effectiveness :

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Event | Recommended Controls | Residual Risk  (Annual) | Risk Reduction % |
| Data Breach | 1.Zero Trust Architecture  2.Encryption in transit and at rest  3. Access logging and monitoring | 5% | 75% |
| Warehouse automation | 1.Network segmentation & industrial control system security  2.Regular vulnerability scans and patching | 4% | 66% |
| Supplier network infiltration | 1. Third-Party risk management (independent risk assessment of suppliers  2. MFA and strong authentication for partners  3.Segmented supplier portals | 10% | 66% |

Our analysis identifies three primary cyber security risks to Pampered Pets' international expansion, with data breaches representing our most critical concern. While industry suggests unmitigated annual losses of $339,600 is a reasonable estimate (DCMS, 2023), our confidence in this figure is lower than our operational risk forecasts due to the unique nature of our client base. The presence of royal patronage and high-profile clientele means the reputational impact of a data breach could significantly exceed the typical $1.2 million per-incident cost for retail business of our size and profile. Unlike operational risks, where we can model precise probabilities based on order volumes and failure rates, the long-term impact of losing VIP client trust is harder to predict.

The proposed control framework, centred on zero-trust architecture and network segmentation, could reduce most risk probabilities by 66-75%. However, the persistent 10% residual risk in supplier network security warrants attention. As we expand internationally and integrate additional suppliers into our digital systems, this residual risk could grow unless we implement additional compensating controls.

# 6.0 Technical Architecture & Data Protection Strategy

# 6.1 High Level Architecture Overview

A screenshot of a computer

AI-generated content may be incorrect.

Our architecture addresses three critical challenges: protecting client data under GDPR, ensuring near-instantaneous recovery (RTO/RPO <1 minute), and maintaining availability across an international supply chain. The design achieves this through active-active deployment across EU regions, with each component selected to minimize vendor lock-in while maximizing security and reliability.

# 6.2 Key Architectural Decisions and Rationale

**6.2.1 Infrastructure Platform Selection**

**Choice**: Azure with Multi-Region Deployment

**Rationale**:

* Azure's EU regions (Netherlands, Ireland) ensure data sovereignty and support GDPR compliance (Eur-Lex, 2016, Arts. 44–50)
* Azure's certifications (ISO 27001, SOC 2) support our security requirements
* Native support for our <1 minute RTO/RPO requirements through:
  + Azure Traffic Manager for instant failover (Microsoft,2024)
  + Built-in regional redundancy
  + Synchronous data replication capabilities

**6.2.2 Container Orchestration**

**Choice**: Kubernetes

**Rationale**:

* Open-source nature reduces vendor lock-in
* Platform-agnostic design allows potential future migration to other cloud providers

**6.2.3 Data Layer**

**Choice**: Combination of Azure Cosmos DB with MongoDB API and Azure SQL

**Rationale**:

* MongoDB API provides:
  + Open-source compatibility
  + Future migration possibilities
* Azure SQL offers:
  + Strong ACID compliance for critical transactions
  + Built-in security features

# 6.3 GDPR Compliance and Data Protection

**6.3.1 Data Sovereignty**

* Data centres exclusively within EU jurisdiction
* Regular data protection impact assessments (DPIAs)

**6.3.2 Technical Controls**

1. **Encryption**:
   * Data-at-rest encryption using Azure Storage Service Encryption
   * TLS 1.3 for all data-in-transit
2. **Access Control**:
   * Zero Trust Architecture implementation
   * Role-Based Access Control (RBAC) with principle of least privilege
   * Multi-Factor Authentication (MFA) for all administrative access
   * Regular access reviews and audit logging
3. **Data Management**:
   * Retention policies aligned with GDPR requirements
   * Right to be forgotten implementation through data tagging
   * Regular data protection impact assessments

# 6.4 Resilience and Recovery

**6.4.1 Active-Active Configuration**

* Both regions operate at production capacity
* Each region capable of handling full load
* Automatic failover through Azure Traffic Manager
* Regular failover testing without service interruption

**RTO/RPO Achievement through Active-Active Design:** Our active-active configuration directly supports Ms. O'dour's stringent RTO (<1 minute) and RPO (<1 minute) requirements (Microsoft, n.d.) through:

* Zero-downtime failover: Azure Traffic Manager automatically redirects traffic to the healthy region within seconds of detecting an issue
* Synchronous data replication: All transactions are synchronously committed to both regions, ensuring zero data loss (RPO=0) during failover
* No cold start: Since both regions are always running at production capacity, there's no startup time when failover occurs
* Independent regional operation: Each region can independently process transactions, eliminating the delay typically associated with primary-secondary failover

**6.4.2 Data Replication Strategy**

* Synchronous replication for critical data
* Point-in-time recovery capabilities
* Regular backup validation
* Documented recovery procedures

The architecture reflects critical trade-offs: enterprise reliability versus vendor independence; data protection versus operational accessibility; and immediate disaster recovery versus system complexity. Our selection of Azure as a compliant data processor provides key security certifications, while our use of open-source technologies (Kubernetes, MongoDB API) accepts increased operational complexity in exchange for reduced vendor lock-in. Our security approach balances data protection for VIP clients with performance considerations, ensuring GDPR compliance without compromising system responsiveness.

# 7. Conclusion

# 7.1 Priority Initiatives

Implementation priorities based on risk analysis:

|  |  |  |  |
| --- | --- | --- | --- |
| Priority | Initiative | Timeline | Implementation Considerations |
| 1. Data Protection | • Zero-trust architecture  • EU Azure infrastructure  • GDPR controls | 0-6 months | Critical foundation for international expansion, VIP client protection and GDPR compliance |
| 2. Quality Control | • Temperature monitoring  • Supplier management | 3-9 months | Can begin in parallel with data protection; essential for maintaining premium brand reputation |
| 3. Supply Chain | • Warehouse automation & network hardening  • Dynamic routing | 6-12 months | Benefits from secure infrastructure but can start independently |
| 4. Supplier Security | • Independent security audits  • Segmented access portals | 9-15 months | Most effective after core security infrastructure is in place |

# 7.2 Summary

Our analysis indicates that Pampered Pets' successful international expansion requires a carefully implementation of security and operational improvements. By prioritizing data protection, we establish the foundation necessary to safeguard our VIP client relationships and ensure regulatory compliance. This security framework, combined with quality control and supply chain improvements, will enable us to maintain our premium brand standards while growing. The implementation sequence balances urgent risk mitigation with practical operational considerations, providing a clear roadmap for secure, sustainable expansion.

# References:

AutoStore (n.d.) *AutoStore Official Website*. Available at: <https://www.autostoresystem.com/> (Accessed: 23 January 2025).

ConnectWise (2024) *SMB research 2024*. Available at: <https://www.connectwise.com/resources/smb-research-2024> (Accessed: 27 January 2025).

Dagnas, S. and Membré, J.M. (2013) 'Predicting and preventing mold spoilage of food products', *Journal of food protection*, 76(3), pp. 538-551.

Department for Digital, Culture, Media & Sport (DCMS) (2023) *Cyber security breaches survey 2023*. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023> (Accessed: 26 January 2025).

Eur-Lex (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1> (Accessed: 23 January 2025).

Gnedenko, B. and Ushakov, I.A. (1995) *Probabilistic reliability engineering*. John Wiley & Sons.

Gustafsson, E., Jonsson, P. and Holmström, J. (2021) 'Reducing retail supply chain costs of product returns using digital product fitting', *International Journal of Physical Distribution & Logistics Management*, 51(8), pp. 876-894. Available at: <https://www.emerald.com/insight/content/doi/10.1108/ijpdlm-10-2020-0334/full/html> (Accessed: 22 January 2025).

Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. and Tatar, U., 2021. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), p.1168.

Microsoft (2024) Traffic Manager overview - Azure Reliability. Available at: <https://learn.microsoft.com/en-us/azure/reliability/reliability-traffic-manager> (Accessed: 26 January 2025).

Microsoft (n.d.) Highly available multi-region application design - Azure Well-Architected Framework. Available at: Recommendations for highly available multi-region design - Microsoft Azure Well-Architected Framework | Microsoft Learn (Accessed: 26 January 2025).

Mooney, C.Z. (1997) *Monte carlo simulation* (No. 116). Sage.

Phonpaseuth, P. (n.d.) *FAIR Model for Risk Quantification: Pros and Cons*. Available at: <https://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons> (Accessed: 23 January 2025).

# Appendix A: Simulation Parameters and Calculations

# A.1 Simulation Parameters

**Base Business Parameters**

* Daily Order Volume: Normal distribution (μ = 1,000, σ = 100)
* Operating Days: 365
* Average Order Value: £50
* Number of Warehouses: 5
* Operating Hours per Day: 24

**Shipping Parameters**

* Base Delivery Time: Lognormal distribution (μ = 1.1, σ = 0.3)
* Delay Threshold: 5 days
* Compensation Schedule:
  + 5-7 days: £10
  + 7-10 days: £20
  + 10+ days: £30

**Quality Control Parameters**

* Base Defect Rate: 2%
* Defect Cluster Probability: 1%
* Defect Cluster Multiplier: 5x normal rate
* Cost per Defect: £60 (1.2x order value)

**Storage Parameters**

* Base Spoilage Threshold: 6 days
* Seasonal Impact Factor: ±20%
* Cost per Spoiled Item: £60 (1.2x order value)

**Warehouse Parameters**

* Mean Time Between Outages: 60 days
* Mean Outage Duration: 4 hours
* Outage Cost: £4,000 per hour

# A.2 Key Probability Distributions

**Daily Order Generation**

Orders = N(1000, 100), where N represents the normal distribution Daily orders are floored and capped at 0 to ensure non-negative values

**Shipping Time Calculation**

Shipping\_Time = exp(N(1.1, 0.3)), where exp() represents the exponential function This generates a right-skewed distribution with:

* Median ≈ 3 days
* Mean ≈ 3.3 days
* 95th percentile ≈ 5.8 days

**Warehouse Failures**

Time\_Between\_Failures = exp(1/60) days Outage\_Duration = exp(1/4) hours Where exp() represents the exponential distribution

# A.3 Cost Calculations

**Delay Cost Formula**

For a shipping time t:

if t ≤ 5 days: cost = 0

if 5 < t ≤ 7 days: cost = £10

if 7 < t ≤ 10 days: cost = £20

if t > 10 days: cost = £30

**Quality Cost Formula**

For n orders:

defect\_probability = 0.02 \* (5 if cluster else 1)

defect\_count = Binomial(n, defect\_probability)

defect\_cost = defect\_count \* £60

**Spoilage Cost Formula**

For shipping time t and day d:

seasonal\_factor = 1 + 0.2 \* cos(2π \* d/365)

threshold = 6 \* seasonal\_factor

spoilage\_cost = £60 \* count(where t > threshold)

**Outage Cost Formula**

For duration h and warehouse capacity share s:

outage\_cost = h \* £4,000 \* s

# A.4 Reputation Impact Calculations

Reputation costs are calculated using dampened scaling to prevent extreme outliers:

**Delay Impact**

delay\_impact = £1.0 \* number\_of\_delays \* (1 + min(average\_delay\_days, 10) \* 0.1)

**Defect Impact**

defect\_scale = sqrt(defect\_count/100) if defect\_count > 100 else 1

defect\_impact = £3.0 \* defect\_count \* min(1 + defect\_scale \* 0.3, 1.3)

**Spoilage Impact**

spoilage\_scale = sqrt(spoiled\_count/100) if spoiled\_count > 100 else 1

spoilage\_impact = £2.0 \* spoiled\_count \* min(1 + spoilage\_scale \* 0.2, 1.2)

# A.5 Monte Carlo Simulation

The simulation was run for 5,000 iterations, with each iteration representing one year of operations. Results were aggregated to generate distributions of outcomes and calculate confidence intervals for various metrics. The simulation implements compound effects where applicable, such as how warehouse outages can lead to increased spoilage through delayed shipments.