**Executive Summary**

**Introduction**

Cathy has embarked on an ambitious digitalisation process for her pet business, which includes the implementation of an international supply chain and automated warehouses worldwide. These changes have attracted customers and investors, such as HRH the King and Prince Albert II of Monaco. However, they have raised concerns about the potential impacts on product quality and supply chain security. To address these concerns, a Quantitative Risk Modelling approach (Monte Carlo Simulation) to estimate the probabilities that these operational changes could endanger both the quality and availability of the company's products is simulated.

**Potential Risks to Quality and Supply Chain**

* **Inventory Risk:** Risk of running out of stock – thereby declining in sales, and additional risk of insolvency due to excess cash flow tied up in inventory (Olsen & Wu, 2020).
* **Technical Risk:** Including system integration failure, poorly written contracts, software vulnerabilities, incomplete design, and inadequate technical expertise.
* **Supply Chain Risk:** Risk of damage or theft, subcontractor default, labour scarcity, equipment damage, and international supply chain risk (due to increased risk of disruptions from geopolitical factors, customs delay, and transportation issues).
* **Quality Control Risk:** Risk of automated warehousing – where potential inconsistencies in automated processes occur, leading to variations in product quality. Additionally, an increase in touchpoints and handoffs may introduce quality control issues.
* **Cybersecurity Risk:** Digitalisation could expose the company and its supply chain to cyber-attacks, potentially compromising sensitive data and operational integrity.
* **Environmental Risk:** Risk of flooding, extreme weather, natural disasters, and global pandemic.
* **Financial Risk:** Risk from sudden cost hikes, currency fluctuation due to international exchange rates, and penalties for non-compliance.
* **Socio-Political Risk**: Community issues, and change in regulation.

**Monte Carlo Simulation**

**Justification for Method Selection**: This simulation approach allows for the assessment of uncertainty/probability in complex systems – sampling from an infinite population of possible results for a given model (Olsen & Wu, 2020).It can model a wide range of potential outcomes based on various input variables, providing a comprehensive risk assessment.

* **Assumptions**:
  1. Data used for the simulation are historical. These include data on supply chain disruptions, pricing, governance and quality control issues.
  2. The probability estimates are largely from industry benchmarks, literature reviews, and opinion from Subject Matter Experts (SME’s).
* **Data Sources**:
  1. Company records for previous supply chain performance, inventory management, and quality control measures.
  2. Industry reports, literature review, and publications on supply chain risks and best practices.
  3. Subject Matter Expert interviews, and consultations.

**Simulation Process and Calculations**

* Identification of the risk items which were further categorised (for example, risk of theft, phishing, software vulnerabilities among others).
* A frequency distribution (Bernoulli, Poisson, and Binomial) selected for each risk item. These distributions were further given parameters to emphasise the frequency of events.
* A severity distribution to identify the impact of the risk items captured. These distributions further assigned parameters (minimum, most likely, maximum) depending on the severity distribution selected. This is in similitude to the three-point estimates of optimistic, most likely, and pessimistic (Steyn, 2018).
* A risk total was determined, which is a convolution of the risk frequency and severity.
* Potential outcomes are determined after running a simulation using multiple iterations. I did a simulation of up to 100 iterations/runs.
* An analysis to determine if the outcome has an effect on the quality and supply chain security of the business. Graphs and diagrams have been generated to determine a correlation or otherwise.

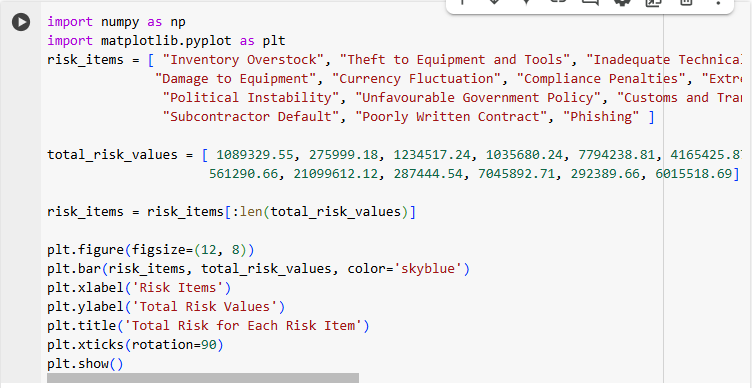
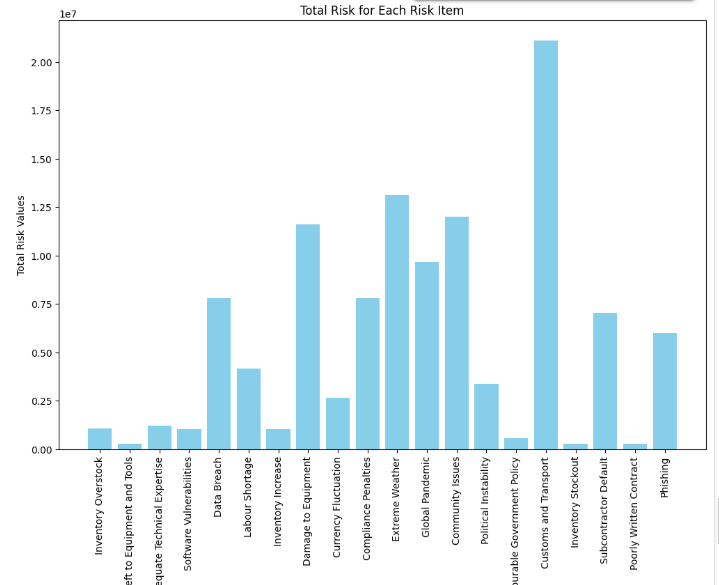
The Project Evaluation Technique (PERT) derived from below calculation (Matos-de-Lopes-Torres-Barboza & Celso-Longo 2018).

Pert Method = (Optimistic + 4\*Most Likely + Pessimistic) / 6

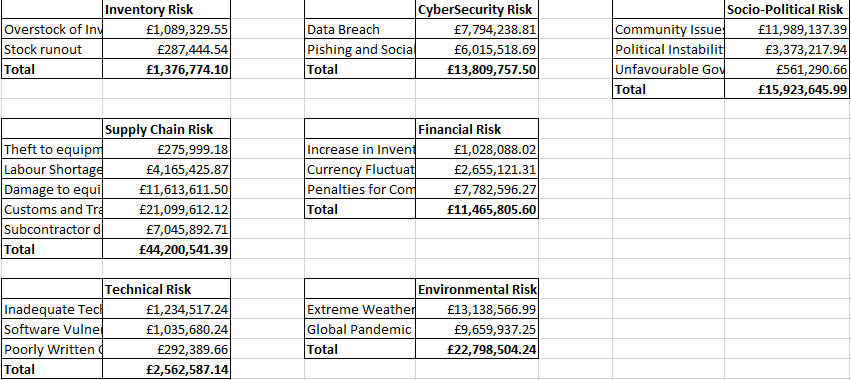
Pictorial representation of the total risk (histogram) derived using Python (Fig 1.0 and 3.0).

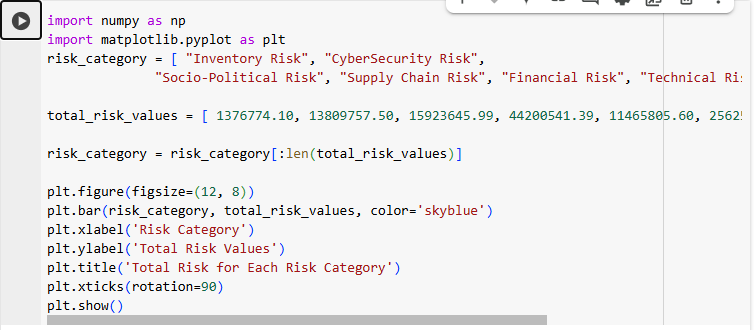
**Results**  
Table 1.0 – Risk analysis and distribution

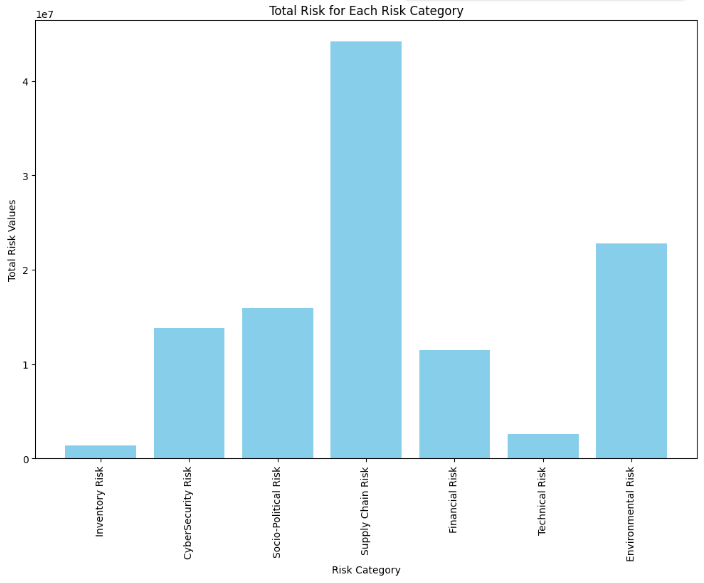
  
Table 2.0 – Total Risk Iterations

****Fig 1.0 – Code used to derive the histogram ****Fig 2.0 – Histogram of total risk for each risk item

**Highly Severe Risks**: From the total risk on table 1.0, risk items 4, 11, and 12 have very high severity values, which could significantly impact the business. These risks if not managed properly could lead to substantial financial losses – thereby negatively impacting the overall quality and security of the supply chain. These risks are the software vulnerabilities, extreme weather and global pandemic. However, when matching risk severity with frequency, risk items 5, 8, 10, 11, 13, and 16 pose greater threat to the business sustainability.

**Supply Chain Security**: The risk item with the most impact is the customs and transport. Risks such as cybersecurity, political instability, currency fluctuation, unfavourable government policy, and customs (due to the implementation of an international supply chain and automated warehouses) significantly impact the business.   
**Product Quality**: Risks with high severity can affect product quality, which can lead to dissatisfied customers, potential loss of business, fines, and reputational damage. Implementing quality control measures and regular audits can help mitigate these risks.  
  
**Risk Category Analysis  
  
**Table 3.0 – Total for each risk category

****Fig 3.0 – Code used to derive risk category histogram

  
Fig 4.0 – Histogram of total risk for each risk category

* **Quality Control Risk**: The simulation estimated a 3.5% probability that automated warehousing could result in significant variations in product quality. This is an aggregation of the inventory and technical risk as a percentage of the total.
* **Supply Chain Disruptions**: The simulation estimates supply chain risk as the highest to impact the operations of the business. This represents a 40% probability of major supply chain disruptions due to supplier defaults, labour shortage, equipment damage, customs and transportation delays.
* **Cybersecurity**: The risk of cyber-attacks compromising the supply chain is estimated at 24%, with the potential to cause significant operational disruptions due to compromise of sensitive data and integrity.
* The simulation predicts that inventory and technical risk categories rarely have a huge impact on the business operations (as they both represent a 3.5% probability). However, due diligence need to be established to avoid complacency.

### Recommendations

#### Mitigating Quality Control Risks

1. **Enhanced Quality Assurance**: Implementation of adequate quality control processes to monitor variations because of the automation process.
2. **Regular Audits**: Frequent audits and inspections of automated processes in addition to other processes initiated in the business, to ensure consistent product quality.
3. **Corporate Governance**: The business to ensure corporate governance to prevent fiscal indiscipline within the business operations.

#### Mitigating Supply Chain Risks

1. **Contingency Planning**: A robust contingency plan to envisage and mitigate issues relating to geopolitical & operational disruptions. This should include alternative supply routes and suppliers. These plans should adequately provide remedial actions in the event of supplier defaults, or instances of extreme weather conditions.
2. **Cybersecurity Enhancements**: Strengthen cybersecurity protocols to protect against cyber-attacks, including regular scanning and vulnerability assessments, employee training, encryption, identity access management, security detection and incidence response management.
3. **Regulatory Compliance**: Cathy’s business should adhere to the provisions of the General Data Protection Regulation (GDPR) 2018, which relates to the handling and processing of data. Other legal requirements and standards to follow are the Consumer Rights Act 2015, International Organisation for Standardisation (ISO), Payment Card Industry Data Security Standard (PCI- DSS), Privacy and Electronic Regulations (PECR), and provisions from the National Institute of Standards and Technology (NIST, 2023).
4. **Supplier Diversification**: Reduce the reliance on single suppliers or regions by diversifying the supply base to mitigate the impact of regional disruptions (Olson & Wu, 2020).
5. **Collaboration: Collaborate and share information to identify vulnerabilities in the supply chain.**

By implementing these recommendations, Cathy can minimize the potential risks associated with digitalisation, ensuring the continued high quality and availability of products for all her customers (especially HRH the King and Prince Albert II of Monaco).

### Disaster Recovery

This disaster recovery (DR) solution will focus on **high availability, minimal data loss, and rapid recovery**. Adopting this recovery solution would require a plan that includes the following:

1. **Primary and Secondary Locations**: Initiate a primary data centre, which handles requests in normal conditions in addition to a secondary data centre (which is the disaster recovery cloud). Andrade et al, (2017) enunciates that the secondary location should be a replica of the web application and database servers of the primary data centre. Furthermore, it should be active and kept synchronised.
2. **Backup and Replication**: Aggressive backups and replication of data should be in place. There should be appropriate backup storage/server to address security issues such as denial of service (DoS), and data compromise (Alhazmi & Malaiya, 2013). This will ensure that data is always up to date, and quickly restored in the event of a disaster. Additionally, data backups and replicas should be stored in multiple geographic locations as a guard against regional disasters (Andrade et al, 2017).
3. **Disaster Monitor**: Set up a disaster monitor located outside the primary and secondary sites. This monitor will detect when the primary site has failed due to a disaster. Proper monitoring and alerting systems will aid the detection of issues, and trigger the disaster recovery plan.
4. **Failover**: Configure an automatic failover to the secondary site in the event the primary site fails. Additionally, a failback should be set up to restore the operations to the primary site once back online (Andrade et al, 2017).
5. **Testing and Simulation**: Thorough testing of the disaster recovery plan should be adopted using simulations that determine its effectiveness.

### Platform Recommendation

There are a number of Disaster-Recovery-as-a-Service (DRaaS) platforms offering similar solutions. However, we will recommend you implement the solution from **Google Cloud Platform (GCP).** GCP allows backup and replication using VMware tools and automation capabilities. It enables automated failover and failback, ensuring continuity of critical applications (Bonga & Varshney 2024).

GCP offers cloud back up and disaster recovery, seamless failover and failback processes, geo-redundancy, application diagnostics, versioning and security.

### Vendor Lock-In To avoid issues relating to vendor lock-in, you can consider the following:

1. **Open Standards and Solutions**: You should patronise open standards and protocols for data storage and replication to ensure compatibility with other platforms (Opara-Martins et al., 2014).
2. **Tendency for Future Integration**: Select a solution that is scalable and accommodates future integration. This will ensure integration implementation in the future.
3. **Multi-Cloud Strategy**: Implement a multi-cloud strategy to ensure data is accessible across multiple cloud providers.
4. **Negotiation and Service Agreements**: Adopt a solution that allows for proper negotiation. Additionally, service agreements need implemented with contracts that are enforceable by law.
5. **Portability**: Select recovery solutions that accommodate portability, and allows ease of data flow across different platforms.
6. **Regular Reviews**: Reviews your disaster recovery solution and vendor contracts to ensure they are flexible to avoid dependence on a single provider.

**Conclusion**

The Monte Carlo simulation indicates a high probability of supply chain disruptions. This would therefore mean that the business adopts adequate mitigation methods if intending to proceed with the implementation of international supply chain, and automated warehouses worldwide. In an attempt to preserve the quality of products, sustaining customer satisfaction, Cathy needs to implement robust quality control measures, enhance cybersecurity protocols, and develop contingency plans for supply chain disruptions.

**Reference**

Alhazmi, O.H. and Malaiya, Y.K., 2013, January. Evaluating disaster recovery plans using the cloud. In 2013 proceedings annual reliability and maintainability symposium (rams) (pp. 1-6). IEEE.

Andrade, E., Nogueira, B., Matos, R., Callou, G. and Maciel, P., 2017. Availability modeling and analysis of a disaster-recovery-as-a-service solution. Computing, 99, pp.929-954.

Bonga, F.K. and Varshney, P., 2024. An Overview of Cloud Disaster Recovery Automated Systems.

European Parliament (2021) Regulation (EU) 2016/679: General Data Protection Regulation (GDPR). Available from: <https://eur-lex.europa.eu/> [Accessed 18 January 2025].

Matos-de-Lopes-Torres-Barboza, R. and Celso-Longo, O., 2018. Risk Analysis In Schedules–Evaluation Of Pert-Risk Method Through The Monte Carlo Method In A Construction Project. Dyna Management journal 2013, 6(1), pp.1-14.

National Institute of Standards and Technology (NIST), 2023 Cybersecurity Log Management Planning Guide. Available from: <https://csrc.nist.gov/pubs/sp/800/92/r1/ipd>. [Accessed 18 January 2025].

Olson, D.L. and Wu, D.D., 2020. Enterprise risk management models (pp. 3-5). Springer Berlin Heidelberg.

Opara-Martins, J., Sahandi, R. and Tian, F., 2014. Critical review of vendor lock-in and its impact on adoption of cloud computing. International Conference on Information Society (i-Society 2014), London, UK, pp.92-97. doi: 10.1109/i-Society.2014.7009018.

Steyn, J., 2018. Quantitative risk analysis for projects [online]