10/13/2025

Executive Summary

Resilient Digital Transformation in Luxury Goods

Musthaq Mohamed
UNIVERSITY OF ESSEX

Table of Contents

Individual Project: Executive Summary

1. Introduction

Cathy’s organisation is scaling up with digital transformation, integrating automated warehouses to enhance operations and meet growing customer demands. While these changes offer operational efficiencies and thriving business opportunities, they also expose the organisation to certain security risks. At the same time, businesses require that the online shop remain operational 24/7, with minimal disruption and recovery capabilities of less than one minute for both Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

This report assumes Cathy’s organisation operates in the high-value industries (specifically watches and designer bags). This assumption enables illustrative examples of luxury or high-value industries. This report discusses and evaluates the risks associated with the organisation’s digitalisation strategy by applying quantitative risk modelling techniques to assess their likelihood and impact and provides industry-standard recommendations. The report further designs a disaster recovery (DR) strategy that ensures resilience, high availability and compliance with legal frameworks such as GDPR and mitigates risks of vendor lock-in.

2. Risks to Product Quality and Supply Chain

2.1. Product Quality Risks

- **Automation Errors and Downtime:** Automated warehouses depend on robotics and AI-controlled processes. Failures in configuration or software bugs could create defects and compromise the quality. Radanliev et al. (2019) highlight that cyber-physical systems introduce new “edge” vulnerabilities, where a single failure can ripple through production lines.

- **Loss of Craftsmanship:** Relying heavily on automation can reduce craftsmanship, and skilled workers lose opportunities to apply their naturally gifted talent and knowledge that ensures product quality. This loss not only weakens the ability to detect defects that AI systems may overlook but also downplays customer trust in industries where the human touch remains central to brand value (European Commission, 2021; Ahangar et al., 2025).

- **Regulatory Compliance Risks**: In today’s markets, high regulatory standards demand protection of personal data. Inaccurate digital logs, audit trails, or data management failures can violate ISO 9001 requirements and GDPR accountability rules. This is especially critical for luxury brands and high-value products, where clients expect not only authenticity but also the utmost protection of personal information. Any data breach or noncompliance could trigger GDPR fines and cause irreparable brand damage (EU, 2016; Zaguir, Magalhães & Spinola, 2024).

- **Illustrative Example:** In luxury goods, counterfeit watches, jewellery, and designer bags pose a huge global risk. If these high-quality fakes get into Cathy's supply chain, they will compromise authenticity, reputation, and brand compliance. Quantitatively, counterfeit infiltration can be considered as a very high-impact risk on the Probability × Impact matrix. (OECD/EUIPO, 2021; Staake, Thiesse and Fleisch, 2009). In many regions counterfeit markets are highly visible, with cheaper replicas of luxury brands available discreetly. This highlights the vulnerability for luxury supply chains, where even a single counterfeit item could damage brand reputation and compromise customer trust.

- **Cybersecurity Impacting Quality Systems:** Cyberattacks on warehouse management can happen at any time; hence, quality assurance (QA) software can be corrupted or manipulated to disable alerts or erase digital records. Such attacks allow counterfeit products to bypass quality checks and enter the market, which can damage customer trust and brand compliance. Supply chains are interconnected in nature, so a single breach can cascade across systems (Herburger, 2024).

2.2 Supply Chain Security Risks

- **Cyberattacks on Logistics Partners:** Latif et al. (2021) conducted a review on cybersecurity within supply chain management, highlighting four dominant research domains. network security, information security, web application security. Their findings reveal that supply chains are highly vulnerable due to interconnectivity and dependence on digital technologies, with cyber threats emerging from both direct and third-party partners. Although the review provides a comprehensive pre-COVID era, subsequent studies indicate that threat complexity and attack surfaces have continued to expand (Herburger, 2024; Konecka and Bentyn, 2024).

- **Geopolitical Disruptions:** Global supply chains often depend on multiple international partners, and any disruption caused by sanctions or trade restrictions can have a major impact on luxury brands' operations. These events are low-probability but very high-impact, as they can interrupt sourcing, logistics, and access to key markets. The OECD (2025) explains that expanding global supply chains and e-commerce have increased exposure to geopolitical and regulatory risks. A clear example is the U.S. trade restriction on Huawei, which resulted in the company losing access to Google’s Android ecosystem (BBC, 2019). It shows how political decisions can disrupt technology supply chains and limit business continuity.
- **Vendor Lock-In:** Depending fully on a single technology or software provider creates serious risks for any organisation. Latif et al. (2021) highlight that vendor lock-in reduces flexibility, limits innovation, and can affect long-term business continuity. The Huawei case demonstrates this risk, as depending on one operating system exposed the company to geopolitical restrictions (BBC, 2019). In some healthcare sectors in the UAE, organisations using proprietary document management systems to store patient records often face strict data retention laws that prevent migration. Specifically, UAE Federal Law No. (2) of 2019 requires health care data to be retained for a minimum of twenty-five years

following a patient’s last procedure (Article 20), reinforcing long-term lock-in and restricting the ability to modernise systems. Herburger (2024) and the OECD (2025) contend that these risks can be mitigated through vendor diversification and the adoption of open-source standards.

- **Natural Disasters and Global Health Crises:** Natural calamities and global health emergencies can disrupt supply chains. Floods, earthquakes, or wildfires can stop production and restrict the transportation of goods, while the COVID-19 pandemic showed how global logistics can collapse. This shows the importance of transportation in supply chain systems. Latif et al. (2021) note that resilience is key for organisations to recover from such disruptions. Herburger (2024) adds that the shift to remote operations during COVID-19 increased digital dependency and cyber risks.

- **Data Breaches in Customer Systems:** Luxury and retail brands manage extensive customer and payment data, making them vulnerable to data breaches that can cause reputational damage and regulatory penalties. Latif et al. (2021) identify information security as a core supply chain risk, as a single weak vendor can expose the entire system. The Kering cyberattack, affecting Gucci, Balenciaga, and Alexander McQueen, exemplifies how hackers can access sensitive customer data across interconnected brand platforms (Reuters, 2025).

3. Quantitative Risk Modelling:

3.1 Probability × Impact (PI) Matrix

This method uses estimated likelihood and impact scores, based on current research on luxury goods supply chains. Main risks include cyberattacks, geopolitical disruption, vendor lock-in, counterfeits, and GDPR compliance. Data and categories are adapted from ENISA, IBM, and OECD/EUIPO (ENISA, 2022; IBM, 2023; OECD/EUIPO, 2021).

Risk Category	Likelihood (%)	Impact (1–5)	Priority
Cyberattack on warehouse/logistics	40	5 (Critical)	High
Geopolitical disruption	30	5 (Critical)	High
Vendor lock-in	25	4 (High)	Medium
Counterfeit goods infiltration	20	4 (High)	Medium
Natural disaster / pandemic	15	5 (Critical)	Medium
Loss of craftsmanship	18	3 (Moderate)	Medium-Low
GDPR non-compliance	12	5 (Critical)	Medium-High

Source: ENISA (2022); IBM (2023); OECD/EUIPO (2021).
The data were calculated using secondary sources and illustrative modelling rather than primary user participation or field data.

PI Matrix Critique: The PI matrix prioritises risks but should be treated as a general guide. Likelihood and impact ratings are based on available data, which may change as new threats emerges (ENISA, 2022). In luxury brands, reputational damage from breaches or disruptions can exceed direct financial loss (IBM, 2023).

3.2 Open FAIR (Quantified Financial Risk)

FAIR breaks down risk as frequency x magnitude (Böhme et al., 2020). In this model, cyber incidents cause the highest financial loss, which matches the earlier Probability × Impact matrix. Counterfeit infiltration and GDPR breaches can also cost a lot because they hurt reputation, compliance, and customer trust.

Risk Scenario	**Probability (Frequency)**	**Estimated Loss Components (€ millions)**	**Annualised Loss Expectancy (ALE)**
Cyberattack on QA/ERP systems	0.4	20 (Reputational) + 5 (Operational) + 2 (Regulatory)	€10.8 million
Counterfeit infiltration	0.2	15 (Reputational) + 3 (Operational)	€3.6 million
GDPR breach	0.12	20 (Regulatory fine) + 5 (Brand damage)	€3.0 million

Source: *Data were prepared by combining secondary research (IBM Security, ENISA, OECD/EUIPO, Böhme et al., 2020) and illustrative ALE calculations as described in the assignment methodology section.*

FAIR Critique: While FAIR is useful to show risks in numbers, it depends on good data and checking scenarios regularly. If incidents are unreported or rare events happen, it is easy to be too optimistic. That’s why these risk numbers need to be updated often to stay realistic (Böhme et al., 2020; C-Risk, 2024; Safe Security, 2024).

3.3 CVSS Scoring

Applying the Common Vulnerability Scoring System (FIRST, 2021) to main vulnerabilities in the warehouse and ERP systems gives:

Vulnerability	CVSS Base Score (v3.1)	Severity Level	Mitigation Priority
Unpatched ERP API	9.8	Critical	Immediate patching
Weak encryption on customer data	8.5	High	Enforce AES-256/SSL-TLS
Misconfigured warehouse IoT	7.6	High	Network segmentation

CVSS Critique: CVSS is well known for highlighting technical risks by number, but it needs to be used with real business knowledge, knowing which systems are most important, and with up-to-date threat info to make sure decisions are right for the business (FIRST, 2021).

4. Recommendations and Mitigation Strategies

The following recommendations are prioritised based on the risk assessment results and highlight actions for immediate and ongoing implementation across the organisation.

4.1 Cybersecurity Enhancements

- Implement Zero Trust Architecture to limit lateral movement (IBM, 2023).
- Adopt continuous vulnerability management guided by CVSS scores.
- Conduct quarterly red-team testing using MITRE ATT&CK scenarios (Bello, 2025).
- Use immutable backups (server and database) and microsegmentation of networks to defend against ransomware attacks and other web-based attacks.

4.2 Supply Chain Resilience

- Diversify critical suppliers and logistics partners across regions (Tang & Musa, 2011).
- Adopt blockchain to verify authenticity (Kamble et al., 2020).
- Mandate third-party security audits and incident-response capabilities (ENISA, 2022).

4.3 Quality Assurance & Operational Integrity

- Deploy digital twins to simulate production flows and detect deviations (Pantlin, 2023).
- Maintain human-in-the-loop inspection to preserve craftsmanship and brand value (European Commission, 2021).
- Use AI defect detection along with manual validation to avoid automation bias (Ahangar et al., 2025).

4.4 Compliance & Governance

- Integrate ISO 27001 and 22301 frameworks for security and continuity (Bello, 2025).
- Embed privacy-by-design into supplier contracts and systems (Zaguir et al., 2024).
- Conduct annual external audits and publish transparency reports to strengthen trust.

4.5 Continuous Learning Culture

- Quarterly update risk models to reflect new threats.
- Reward staff for reporting security concerns and incidents
- Encourage adversarial thinking (“How would an attacker exploit us?”) to counter complacency (Rinaldi et al., 2022).

5. Disaster Recovery (DR) and Business Continuity (BC) Strategy

In a complex digital and supply chain environment, disaster recovery and business continuity strategy are essential to protect operations, reputation, and compliance (ENISA, 2022; Gartner, 2023).

5.1 Requirements

The chosen solution must follow the below guidelines.

- Maintain 24/7/365 availability.

- Achieve RTO and RPO of less than one minute.
- Ensure full GDPR compliance for all customer and operational data.
- Minimise vendor lock-in, with workloads portable across cloud platforms

5.2 Recommended Architecture

A multi-cloud Active-Active configuration is recommended, using synchronous, real-time database replication across AWS and Azure (Mankotia, 2024; Nelson et al., 2025).

Key design components include:

- Containerisation (Kubernetes, Docker): Enables workload portability and rapid redeployment across alternate providers (Opara-Martins et al., 2016).
- Synchronous replication: Prevents data loss and supports sub-minute recovery targets (Alshammari & Alwan, 2017). This can be achieved through SQL Server Always On availability groups or Oracle Real Application Clusters (RAC) to provide continuous availability and automatic failover between nodes.
- Future Risk Monitoring: monitoring emerging risks and regulatory updates with annual reviews to adapt DR and supply chain continuity plans accordingly.

Option	RTO/RPO	Cost	Lock-in Risk	Suitability
Single-Cloud Active-Passive	5–15 min	Medium	High	Not suitable
On-Prem DR Site	10–30min	High	Low	Too slow
Multi-Cloud Active-Passive	1–3 min	High	Medium	Better

Option	RTO/RPO	Cost	Lock-in Risk	Suitability
Multi-Cloud Active-Active	<1 min	High	Low	Best fit

While multi-cloud Active-Active architectures deliver the highest resilience and minimise vendor lock-in, achieving true operational readiness remains challenging. Many organisations discover configuration mismatches or incomplete DR replication only during live DR drills. High costs, especially for hybrid setups requiring significant bandwidth from on-premises to cloud for data replication, further complicate adoption. Ultimately, effective multi-cloud or hybrid DR demands continuous monitoring and automation to ensure genuine readiness (Gartner, 2023; Wanclouds, 2025).

6 Ethical, Legal and Professional Issues

Luxury brands must address broader ethical and societal implications of digitalisation:

- ESG and Human Rights: Sourcing precious metals and gems must align with ethical labour and environmental standards (OECD, 2021).
- Data Privacy and Customer Trust: Clients expect strong confidentiality for purchase and personal data (GDPR Art. 32).
- Professional Responsibility: Cybersecurity practitioners must uphold integrity, transparency and continuous professional development to meet industry standards (ISC², 2023).

7 Conclusion

Digitalisation brings Cathy's organisation to the potential growth path with high operational efficiency but introduces new risks to product quality and supply chain integrity. Quantitative analysis identified cyberattacks and counterfeit infiltration as the most critical threats. Adopting Zero Trust security, vendor diversification, blockchain traceability, and a multi-cloud DR solution provides balanced resilience and high availability by ensuring human oversight for craftsmanship, ethical sourcing, and continuous learning. It will ensure that digital transformation enhancements align with the brand's legacy and customer trust.

8 Reference

Ahangar, M.N., Farhat, Z.A. *et al.* (2025) 'AI trustworthiness in manufacturing: challenges, toolkits and the path to Industry 5.0', *Sensors (Basel)*, 25(14), p. 4357. doi:10.3390/s25144357 *(Available at: https://www.mdpi.com/1424-8220/25/14/4357)*

Alshammari, R. and Alwan, Z. (2017) 'Disaster Recovery in Single-Cloud and Multi-Cloud Environments', *International Journal of Computer Applications*, 168(3), pp. 21–28.

Al Tamimi & Company (2020) 'The Federal Law regulating the Use of Information and Communication Technology in the UAE Healthcare Sector'. Available at: https://www.tamimi.com/law-update-articles/the-federal-law-regulating-the-use-of-information-and-communication-technology-in-the-uae-healthcare-sector/ (Accessed: 12 October 2025).

BBC (2019) *Huawei's use of Android restricted by Google.* Available at: https://www.bbc.com/news/business-48330310 (Accessed: 13 October 2025).

Black Kite (2025) 'Cyber Risk Quantification & Open FAIR™ Risk Methodology'. Available at: https://blackkite.com/financial-impact/ (Accessed: 11 October 2025).

Böhme, R., Laube, S. and Riek, M. (2020) 'A fundamental approach to cybersecurity risk management based on FAIR', *Journal of Cybersecurity*, 6(1), pp. 1–16. Available at: https://www.casact.org/sites/default/files/2021-07/Approach-Cyber-Risk-Bohme-Laube-Riek.pdf (Accessed: 13 October 2025).

C-Risk (2024) 'The FAIR™ Methodology for Cyber Risks'. Available at: https://www.c-risk.com/blog/fair-analysis (Accessed: 13 October 2025).

European Commission (2021) 'Industry 5.0: Towards a sustainable, human-centric and resilient European industry'. Brussels: European Commission. Available at: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en (Accessed: 9 October 2025).

European Parliament and Council (2016) *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)*, OJ L 119, pp. 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (Accessed: 12 October 2025).

ENISA (2022) ‘ENISA Threat Landscape 2022’. *European Union Agency for Cybersecurity*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed: 13 October 2025).

FIRST (2021) ‘Common Vulnerability Scoring System v3.1: Specification Document’. *Forum of Incident Response and Security Teams (FIRST)*. Available at: https://www.first.org/cvss/v3-1/ (Accessed: 10 October 2025).

Gartner (2023) ‘Market Guide for Disaster Recovery as a Service (DRaaS)’. Available at: https://recoverypoint.com/press-release/recovery-point-systems-recognized-in-gartners-2023-draas-market-guide/ (Accessed: 13 October 2025).

Herburger, M., Wieland, A. & Hochstrasser, C. (2024) ‘Building supply chain resilience to cyber risks: a dynamic capabilities perspective’, *Supply Chain Management: An International Journal*, 29(7), pp. 28–50. doi: 10.1108/SCM-01-2023-0016. Available at: https://www.emerald.com/insight/content/doi/10.1108/SCM-01-2023-0016/full/html (Accessed: 13 October 2025).

IBM (2023) ‘Cost of a Data Breach Report 2023’. *IBM Security*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 13 October 2025).

Kamble, S., Gunasekaran, A. & Sharma, R. (2020) ‘Modeling the blockchain-enabled traceability in supply chain’, *International Journal of Information Management*, 52, 101967.

Konecka, S. & Bentyn, Z. (2024) 'Cyberattacks as threats in supply chains', *LogForum*, 20(2), pp. 123–135. Available at: https://www.logforum.net/ (Accessed: 11 October 2025).

Latif, M.N.A., Aziz, N.A.A., Hussin, N.S.N. & Aziz, Z.A. (2021) 'Cyber security in supply chain management: a systematic review', *LogForum*, 17(1), pp. 49–57. doi:10.17270/J.LOG.2021.555. Available at: https://www.yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-03b6ae64-b86c-40e2-8f68-970d90ce863e/c/Latif_1_2021.pdf (Accessed: 12 October 2025).

Mankotia, R. (2024) 'Comparing High Availability and Disaster Recovery in Multi-Cloud Environments', *International Journal of Computer Trends and Technology*, 72(1), pp. 34–41.

Nelson, J., Wallis, R. and Oye, K. (2025) 'Comparative Analysis of Disaster Recovery Tools in Multi-Cloud Deployments', *IEEE Access*, 13, pp. 214–229.

OECD (2025) 'Mapping global trade in fakes 2025: Global trends and enforcement challenges'. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html (Accessed: 11 October 2025).

OECD/EUIPO (2021) 'Global trade in fakes: A worrying threat'. Paris: OECD Publishing. Available at: https://www.oecd-ilibrary.org/trade/global-trade-in-fakes_74c81154-en (Accessed: 10 October 2025).

Opara-Martins, J., Sahandi, R. and Tian, F. (2016) ‘Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective’, *Journal of Cloud Computing*, 5(1), pp. 1–18.

Pantlin, R. (2023) ‘Digital twins and predictive analytics for quality management’, *Journal of Manufacturing Systems*, 66, pp. 120–133.

Radanliev, P., De Roure, D., Page, K., Nurse, J.R.C., Mantilla Montalvo, R., Santos, O., Maddox, L. & Burnap, P. (2020) ‘Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains’, *Cybersecurity*, 3:13. doi:10.1186/s42400-020-00052-8. Available at: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00052-8 (Accessed: 13 October 2025). cybersecurity.springeropen.com

Reuters (2025) ‘Hackers steal client data from Kering’s Gucci, Balenciaga, and McQueen, BBC says’, *Reuters*, 15 September. Available at: https://www.reuters.com/sustainability/boards-policy-regulation/hackers-steal-client-data-kerings-gucci-balenciaga-mcqueen-bbc-says-2025-09-15/ (Accessed: 11 October 2025).

Rinaldi, M., Bottani, E. & Regattieri, A. (2022) ‘A literature review on quantitative models for supply chain risk’, *Computers & Industrial Engineering*, 170, 108329.

Safe Security (2024) ‘FAIR Cyber Risk Model Pros and Cons’. Available at: https://safe.security/resources/blog/pros-cons-fair-model/ (Accessed: 13 October 2025).

Staake, T., Thiesse, F. & Fleisch, E. (2009) ‘The emergence of counterfeit trade: a literature review’, *European Journal of Marketing*, 43(3/4), pp. 320–349. doi: 10.1108/03090560910935451. Available at: https://www.emerald.com/insight/content/doi/10.1108/03090560910935451/full/html (Accessed: 13 October 2025).

SupplyChainDive (2024) ‘Global supply chain compliance with data privacy regulations’. Available at: https://www.supplychaindive.com/spons/global-supply-chain-compliance-with-data-privacy-regulations/727194/ (Accessed: 10 October 2025).

Tang, C.S. & Musa, S.N. (2011) ‘Identifying risk issues and research advancements in supply chain risk management’, *International Journal of Production Economics*, 133(1), pp. 25–34.

UAE Federal Law No. (2) of 2019 ‘Concerning the Use of Information and Communications Technology in Health’. Available at: https://uaelegislation.gov.ae/en/legislations/1209/download (Accessed: 12 October 2025).

Wanclouds (2025) ‘Best Practices for Building a Cloud-Native Disaster Recovery Strategy’. Available at: https://www.wanclouds.net/blog/kubernetes/best-practices-for-your-cloud-native-disaster-recovery-strategy (Accessed: 13 October 2025).

Wanclouds (2025) 'How a Multi-Cloud Strategy Can Help You Avoid Vendor Lock-In'. Available at: https://www.wanclouds.net/blog/product/how-a-multi-cloud-strategy-can-help-you-avoid-vendor-lock-in (Accessed: 12 October 2025).

WTW (2023) 'How luxury brands can mitigate the impact of cyber risks'. Available at: https://www.wtwco.com/en-vn/insights/2023/03/how-luxury-brands-can-mitigate-the-impact-of-cyber-risks (Accessed: 10 October 2025).

Zaguir, N., Magalhães, G.H. de and Spinola, M. de M. (2024) 'Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions', *IEEE Access*. doi:10.1109/ACCESS.2024.3406724.