**SRM\_PCOM7E – Individual Project: Executive Summary**

**Title:** Executive Summary – Digitalisation, Global Supply Chain & Automated Warehouses: Quantitative Risk, Quality & DR Readiness  
**Module:** SRM\_PCOM7E (July 2025 A)  
**Institution:** University of Essex Online  
**Submission Date:** 13 October 2025  
  
  
**Declaration:** I confirm this submission is my own work and properly referenced in   
**Repository Note:** A copy of the final product will be saved to my individual GitHub repository.

Table of Contents, References and Appendices Not included in word count

**Table of Contents**

[**1. Executive Summary** 3](#_Toc211293150)

[**2. Context & Objectives** 4](#_Toc211293151)

[**3. Risk Identification – Quality & Availability** 4](#_Toc211293152)

[3.1 Supply-chain (globalisation & automation). 4](#_Toc211293153)

[3.2 Cyber/IoT (digital footprint). 4](#_Toc211293154)

[3.3 Product quality (process change & counterfeits). 5](#_Toc211293155)

[**4. Quantitative Modelling Approaches (with justification)** 5](#_Toc211293156)

[4.1 Event-tree roll-ups for availability. 5](#_Toc211293157)

[4.2 Fault-tree fragments for quality loss. 6](#_Toc211293158)

[4.3 Risk scoring and classification. 6](#_Toc211293159)

[4.4 Formal security modelling where critical. 6](#_Toc211293160)

[4.5 Dynamic risk assessment hooks. 7](#_Toc211293161)

[4.6 Practitioner fit and tool support. 7](#_Toc211293162)

[**5. Assumptions & Data (sources & parameters)** 7](#_Toc211293163)

[**6. Calculations & Results** 8](#_Toc211293164)

[6.1 Probability of *any* supply-chain issue (annual) 8](#_Toc211293165)

[6.4 Risk ranking snapshot (selected) 10](#_Toc211293166)

[6.5 One-way sensitivity (directional) 10](#_Toc211293167)

[6.6 Traceability and model extension 11](#_Toc211293168)

[**7. Recommendations (prioritised)** 11](#_Toc211293169)

[**8. Business Continuity & Disaster Recovery (DR)** 12](#_Toc211293170)

[**9. Compliance (GDPR/PDPL & security standards)** 13](#_Toc211293171)

[**10. Conclusion** 14](#_Toc211293172)

[**11. Appendix** 15](#_Toc211293173)

[**References** 18](#_Toc211293174)

# **1. Executive Summary**

Cathy's digitization—introducing an international supply chain and automated warehouses—increases both opportunity and risk. With event-tree roll-ups and fault-tree logic, I estimate an annual 35.8% chance of at least one material supply-chain disruption without extra controls; drivers include logistics delays and single-source risk (Aven & Thekdi, 2024). A top-event of high quality that merges automation-caused process drift with counterfeit ingress provides an opportunity for quantifiable quality loss of 14.5% per annum in the absence of novel controls (Son, Song & Lee, 2023). Cyber-caused failure modes (ransomware, IoT compromise, regional cloud outage) are salient in digitized operations and require formal quantification in order to guide mitigations (Zadeh, Lavine, Zolbanin & Hopkins, 2023).

For 24/7/365 availability with RTO ≤ 60s and RPO ≤ 60s, I suggest a cloud active-active, multi-region design with synchronous database replication, blue-green cutover, and automated health-probe failover, providing ≈99.999975% service availability (~7.9 seconds downtime/year) with conservative per-region assumptions (Kesa, 2023). Interdependency-aware DR patterns minimize cascading outages between cyber-physical components and logistics nodes (Chen & Wang, 2024).

Prioritised controls: zero-trust identity and EDR, segmented IoT/OT networks, immutable/journaled backups, anti-counterfeit serialization with supplier PPAP, dual-sourcing and multi-carrier routing, SPC-based quality gates, and quarterly chaos/table-top exercises (Morales, 2025). GDPR/PDPL compliance will be ensured by DPIAs, encryption, minimisation, geo-fencing, and breach-notification runbooks (Aven & Thekdi, 2024).

# **2. Context & Objectives**

Cathy's transition from a single-location craft store to a digitised, global, automated supply chain introduces new cyber-physical dependencies that can compromise availability and quality (Aven & Thekdi, 2024). This report measures those risks using simple, auditable models (event trees for disruption; fault trees for quality) and prescribes a DR design with RTO ≤ 60s and RPO ≤ 60s (ter Beek et al., 2021). Objectives: determine major risks, deliver reproducible yearly probabilities, suggest an active–active DR/BC architecture, prevent vendor lock-in using portable patterns, and map controls to GDPR-level expectations with DPIA, encryption, and exercised incident/DR runbooks (Zadeh et al., 2023).

# **3. Risk Identification – Quality & Availability**

## 3.1 Supply-chain (globalisation & automation).

Internationalisation creates single points in material, cross-border logistics, customs, and last-mile capacity which increase disruption risk and perceived quality variance (Andersson et al., 2025). Estimation should define explicit assumptions and traceable inputs to remain defendable under uncertainty (Aven & Thekdi, 2024). Rank exposures by expected loss to aim for diversification, SLAs, and dynamic re-routing (Zadeh et al., 2023).

## 3.2 Cyber/IoT (digital footprint).

Automated warehouses, APIs, and IoT/OT offer attack opportunities for ransomware, identity abuse, lateral movement, and device compromise, hitting availability and integrity (Czekster et al., 2025). Formal quantitative models validate states and controls beyond qualitative judgment for critical subsystems (ter Beek et al., 2021). Zero-trust, EDR/XDR, immutable backups, and drilled playbooks in operations possess blast radius and recovery speed (Morales, 2025).

## 3.3 Product quality (process change & counterfeits).

Automation alters tolerances and measurement; poor commissioning, calibration, or SPC renders latent defects unheard (Son et al., 2023). Record priors, evidence, and parameter uncertainty to stay defensible in the long term (Aven & Thekdi, 2024). Serialization/e-pedigree and PPAP audit on highest priority with quantitative probability severity ranking (Zadeh et al., 2023).

# **4. Quantitative Modelling Approaches (with justification)**

## 4.1 Event-tree roll-ups for availability.

For "any material disruption this year," I apply an open event-tree intersecting independent base events (e.g., supplier breakdown, logistics delay, local cloud outage, counterfeit ingress) with P(∪E\_i)=1-∏(1-P\_i). The approach is simple to audit, is sensitive to testing, and adheres to risk-science guidance to make models traceable for executive decision-making (Aven & Thekdi, 2024). Where sequential structure occurs (e.g., outage → backlog → stock-out), branches achieve sequential escalation with conditional probability, and these are traceable from assumptions through to top-line results (Aven & Thekdi, 2024).

## 4.2 Fault-tree fragments for quality loss.

Product-quality failure is shown as a top event given by OR/AND combinations of root causes: automation-generated process drift, counterfeit ingress, calibration lapse, and supplier non-conformance. Fault-tree logic makes a clear distinction between independent vs conjunctive contributors and is broadly applied in high-reliability fields; it also correlates well to where we put controls (e.g., SPC, serialization) (Son, Song & Lee, 2023).

## 4.3 Risk scoring and classification.

For rank-ordering, I compute simple risk scores and (where detectability varies) an FMEA-style RPN on a calibrated 1–10 scale, then compare to acceptance thresholds. Contemporary quantification/classification frameworks recommend such scoring to consistently prioritise cyber and operational mitigations and to link reductions to specific controls (Zadeh, Lavine, Zolbanin & Hopkins, 2023).

## 4.4 Formal security modelling where critical.

For control-critical subsystems (e.g., order-routing auth, warehouse robot safety interlocks), formal quantitative models such as RisQFLan can validate state space, transitions, and attack/defence scenarios, complementing lighter event/fault trees when assurance needs are higher (ter Beek, Legay, Lluch Lafuente & Vandin, 2021).

## 4.5 Dynamic risk assessment hooks.

Because digitised operations are non-stationary, I include parameters designed to be refreshed from telemetry (incident rates, mean-time-to-recover, control efficacy). Dynamic/streaming approaches from cyber-physical IoT contexts inform how to update priors and shorten detection/response loops (Czekster, Webber, Furstenau & Marcon, 2025).

## 4.6 Practitioner fit and tool support.

The approach balances rigour and practicality, addressing known practitioner needs for prioritisation, collaboration, and evidence-based decisions across multi-actor environments; it is compatible with existing GRC/IR tools and playbooks (Andersson, Bergström, Lundgren, Bernsmed & Bour, 2025; Morales, 2025).

# **5. Assumptions & Data (sources & parameters)**

**Time horizon.** One-year exposure window to align with budget and review cycles (Aven & Thekdi, 2024).

**Event set (baseline annual probabilities, pre-controls).** Supplier disruption 0.15; logistics delay 0.18; regional cloud outage 0.02; counterfeit ingress 0.06; automation quality drift 0.09; ransomware 0.10; IoT compromise 0.12; data breach 0.08. Cyber/IoT base rates reflect digitised operations with mixed IT/OT assets (Zadeh et al., 2023). IoT dynamism justifies non-negligible priors (Czekster et al., 2025). Practitioner insight supports feasibility of control-driven reductions (Morales, 2025).

**Independence.** Base aggregation assumes pairwise independence for first-order estimates; correlated shocks (e.g., regional weather) are treated qualitatively and in sensitivity notes per risk-science guidance on model transparency (Aven & Thekdi, 2024).

**Quality top event.** “Material quality degradation” is defined as defect or spec non-conformance exceeding SPC limits or verified counterfeit at receipt. Fault-tree basic events: process drift (0.09), counterfeit ingress (0.06) (Son et al., 2023).

**Availability architecture.** Two active regions; conservative per-region availability **A = 99.95%** (managed PaaS baseline). Parallel availability computed assuming fail-independence with health-probe failover and pre-warmed capacity (Kesa, 2023). Interdependence risk is addressed by cross-region diversity and DR drills (Chen & Wang, 2024).

**Impact scale for ranking.** 1–10 ordinal impact for business objectives (revenue, brand, regulatory). Detectability scale 1–10 where used (Zadeh et al., 2023).

**Data pedigree.** Parameters are expert-elicited priors grounded in literature patterns; all inputs and formulas are listed in Appendix A for auditability (Aven & Thekdi, 2024). Tooling gaps from complex domains inform telemetry requirements (Andersson et al., 2025).

# **6. Calculations & Results**

## 6.1 Probability of *any* supply-chain issue (annual)

Events: supplier , logistics , regional cloud outage , counterfeit . Using an event-tree roll-up:

Event-tree transparency supports executive review of assumptions (Aven & Thekdi, 2024).

6.2 Probability of quality degradation (annual)

Top event via an OR gate of process drift and counterfeit ingress :

Fault-tree structuring reflects accepted practice in high-reliability domains (Son et al., 2023).

6.3 Availability target vs architecture availability

Two active regions with per-region .

Sync database replication + automated health-probe failover supports RTO ≤ 60 s and RPO ≤ 60 s when cutover is scripted and capacity pre-warmed (Kesa, 2023). Interdependency-aware DR patterns reduce cascade risk across cyber-physical layers (Chen & Wang, 2024).

## 6.4 Risk ranking snapshot (selected)

Simple risk score on a 1–10 impact scale:

* Logistics delay: → top operational driver.
* Supplier disruption: → diversify sources.
* Ransomware: → EDR, immutable backups, playbooks.
* IoT compromise: → network segmentation, signed firmware.
* Quality drift: → SPC + golden samples.  
  Quantification/classification supports prioritised mitigation portfolios (Zadeh et al., 2023). Practitioner guidance validates these control families in real programmes (Morales, 2025).

## 6.5 One-way sensitivity (directional)

* Logistics probability −50% (0.18→0.09): .
* Supplier disruption −50% (0.15→0.075): .
* Add third region at : (≈99.9999875%), ≈3.9 s/year.  
  Risk-science practice recommends showing such “tornado-style” effects to justify where each control buys the most risk reduction per cost (Aven & Thekdi, 2024).

## 6.6 Traceability and model extension

Where higher assurance is required (e.g., robot safety interlocks; order-auth transitions), formal quantitative security models such as **RisQFLan** can be used to validate state spaces and attack/defence dynamics before cutover (ter Beek et al., 2021). Dynamic risk assessment hooks enable periodic recalibration of priors with live telemetry (Czekster et al., 2025).

# **7. Recommendations (prioritised)**

1. Active–active, multi-region platform with synchronous DB replication; automate health-probe failover and blue-green cutover to meet RTO ≤ 60s / RPO ≤ 60s. (Kesa, 2023)
2. Quarterly chaos drills and semi-annual table-tops covering region loss, DB failover, identity/DNS outages, and comms escalation. (Chen & Wang, 2024)
3. Zero-trust baseline: least-privilege IAM, MFA everywhere, short-lived tokens, EDR/XDR, and continuous configuration monitoring. (Morales, 2025)
4. IoT/OT segmentation: isolate robots/PLCs, allow-list protocols, require signed firmware and secure boot; add anomaly detection on OT telemetry. (Czekster et al., 2025)
5. Quality controls: SPC at critical points, golden-sample checks after automation changes, first-article approval before scale-up. (Aven & Thekdi, 2024)
6. Anti-counterfeit: serialization/e-pedigree scans at every handover; PPAP-style onboarding and periodic supplier audits. (Son et al., 2023)
7. Supply-chain resilience: dual-source critical inputs, multi-carrier contracts with dynamic re-routing SLAs, time-phased safety stock at automated sites. (Andersson et al., 2025)
8. Risk-based prioritisation: rank mitigations by quantified P × Impact (and Detectability where relevant) and recalibrate quarterly with telemetry. (Zadeh et al., 2023)
9. Compliance by design: DPIA for new processing, encryption in transit/at rest, data minimisation, breach-notification playbooks, and geo-fencing. (Aven & Thekdi, 2024)

# **8. Business Continuity & Disaster Recovery (DR)**

Architecture. Position the shop and APIs active–active in two regions behind a global load balancer, both regions multi-AZ. Leverage synchronous, commit-quorum DB replication, versioned object store, KMS/HSM-encrypted keys, and Infrastructure as Code for rebuilds reproducibility (Kesa, 2023). External interdependencies (DNS, IdP, carriers, power) map to and remove hidden single points to prevent cascades (Chen & Wang, 2024).

RTO/RPO ≤ 60s. Health probes drop a failed zone in <30s; traffic is rerouted automatically; maintain pre-warmed capacity and scripted blue-green cutovers (Kesa, 2023). Provide persistent journaling for databases (15–30s) and at-least-once queues with idempotent consumers for order reconciliation (Zadeh et al., 2023).

Security in DR. Have immutable, off-line accessible snapshots; use least-privilege DR roles with transient creds; pre-approve legal/comms templates to reduce response latency (Morales, 2025).

Preventing lock-in with vendors. Employ moveable abstractions (Terraform, Kubernetes, open DB engines), watched data-egress channels (snapshots/CDC), and a minimal "pilot-light" installation in a second cloud to maintain good exit alternatives with no obligation regarding resilience (Morales, 2025; Kesa, 2023).

# **9. Compliance (GDPR/PDPL & security standards)**

Take on privacy-by-design: map all personal-data flows (supplier contacts, telemetry, orders), use data minimisation, purpose and storage limitation, and record legitimate bases with retention schedules (Aven & Thekdi, 2024). For each new processing—IoT tracking or cross-border analytics—conduct DPIA and implement encryption in transit/at rest, fine-grained access controls, and pseudonymisation where possible (Aven & Thekdi, 2024). Limit international transfers to safe areas, allow data-subject rights via service flows, and make breach-notification runbooks certified alongside DR drills to fit GDPR-class timelines and PDPL compliance in regional areas (Kesa, 2023). Construct security-by-design: zero-trust IAM with MFA and least privilege; estate-wide EDR/XDR; immutable, offline-accessible backups; and segmented IoT/OT networks with allow-listed protocols and signed firmware (Morales, 2025). Apply quantitative risk classification to align controls with measurable probability/impact decrease and record residual-risk acceptance (Zadeh et al., 2023). For safety-critical subsystems, validate controls using formal models before go-live and fault/event-tree analysis; keep supplier DPAs, right-to-audit, serialization/e-pedigree, and PPAP for anti-counterfeit guardianship (ter Beek et al., 2021).

# **10. Conclusion**

The quantitative estimates are that, without additional controls, the company has approximately a 35.8% annual chance of at least one material supply-chain disruption and 14.5% chance of quantifiable quality impairment, in line with risk-science best practice to make uncertainty explicit and traceable (Aven & Thekdi, 2024). Cyber-enabled disruption is still material in a digitised, IoT-intensive enterprise; formal quantification and grading are required to inform prioritisation of mitigations and to demonstrate residual-risk acceptance to executives and auditors (Zadeh, Lavine, Zolbanin & Hopkins, 2023).

Prescribed active–active, multi-region platform with synchronous replication, rehearsed failover, and immutable/journaled backups credibly meets RTO ≤ 60s and RPO ≤ 60s, and interdependency-aware DR patterns mitigate cascade risk over cyber-physical and logistics layers (Kesa, 2023). Priority actions include: zero-trust identity and EDR/XDR; IoT/OT segmentation with signed firmware; SPC and golden-sample checks; serialization/e-pedigree and supplier PPAP; dual-sourcing, multi-carrier routing, and time-phased safety stock. Baking DPIA, encryption, minimisation, and breach-notification runbooks into the compliance guarantees GDPR-level compliance and operational maturity. With quarterly sensitivity-based recalibration, based on live telemetry, management can iteratively reduce the leading causes of loss while preserving world-class availability and product quality (Aven & Thekdi, 2024).

# **11. Appendix**

**Appendix A – Parameters & Formulas**

Time window: 1 year.  
Baseline annual probabilities (pre-controls): Supplier disruption 0.15; Logistics delay 0.18; Regional cloud outage 0.02; Counterfeit ingress 0.06; Automation quality drift 0.09; Ransomware 0.10; IoT compromise 0.12; Data breach 0.08 (Aven & Thekdi, 2024; Zadeh et al., 2023; Czekster et al., 2025; Morales, 2025).  
Key formulas:

* Any-event roll-up: (Aven & Thekdi, 2024).
* Fault-tree OR (quality): (Son et al., 2023).
* Parallel availability: .
* Risk score: (1–10 scale).
* RPN (optional): (1–10 each).

**Appendix B – Risk Register (extract)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Risk (top-level)** | **P (yr⁻¹)** | **Impact (1–10)** | **Score** | **Controls (primary)** |
| SC-1 | Logistics delay | 0.18 | 7 | 1.26 | Multi-carrier, re-routing SLAs, safety stock |
| SC-2 | Supplier disruption | 0.15 | 8 | 1.20 | Dual-sourcing, audits, PPAP |
| CY-1 | Ransomware | 0.10 | 9 | 0.90 | EDR/XDR, immutable backups, playbooks |
| OT-1 | IoT/OT compromise | 0.12 | 7 | 0.84 | Segmentation, signed firmware, anomaly detection |
| QL-1 | Quality drift (automation) | 0.09 | 8 | 0.72 | SPC, calibration, golden sample |
| QL-2 | Counterfeit ingress | 0.06 | 8 | 0.48 | Serialization/e-pedigree, supplier vetting |
| INF-1 | Cloud regional outage | 0.02 | 9 | 0.18 | Active–active, multi-AZ, GLB |

**Appendix C – Step-by-step Calculations**

Any supply-chain issue:  
→ (≈35.8%).  
Quality degradation (OR): (≈14.5%).  
Two-region availability: (99.999975% ≈7.9 s/yr).  
Sensitivity example: Reduce logistics to 0.09 → (≈28.9%).  
(All per Aven & Thekdi, 2024; Chen & Wang, 2024; Kesa, 2023.)

**Appendix D – Mini Diagrams (ASCII)**

**D1 – Fault-tree (quality top event)**

QUALITY DEGRADATION (Top)

|

OR

+---------+---------+

| |

Process drift Counterfeit ingress

| |

Calibration lapse Supplier lapse / Tamper

(Son et al., 2023)

**D2 – Event roll-up (supply chain “any disruption”)**

Start → Supplier fail? → yes → Disruption

no → Logistics delay? → yes → Disruption

no → Cloud region out? → yes → Disruption

no → Counterfeit ingress? → yes → Disruption

no → No disruption

**D3 – DR reference (active–active)**

Users → Global LB → Region A (multi-AZ) ⇄ Region B (multi-AZ)

| | | |

Web/API Sync DB ⇄ Web/API Sync DB

↘ Journals ↙

Object Storage (versioning)

(Kesa, 2023; Chen & Wang, 2024)

**Appendix E – Glossary (Terms)**

RTO: Recovery Time Objective. RPO: Recovery Point Objective. SPC: Statistical Process Control. EDR/XDR: Endpoint/Extended Detection & Response. IaC: Infrastructure as Code. PPAP: Production Part Approval Process. GLB: Global Load Balancer. DPIA: Data Protection Impact Assessment. (Aven & Thekdi, 2024)

# **References**

Andersson, S., Bergström, E., Lundgren, M., Bernsmed, K. & Bour, G. (2025) ‘Information security risk management tools in the air traffic management domain: what are practitioners’ needs?’, *Journal of Cyber Security Technology*. Available at: <https://www.tandfonline.com/doi/full/10.1080/19393555.2025.2498472> (Accessed: 10 October 2025).

Aven, T. & Thekdi, S. (2024) *Risk Science: An Introduction*. 2nd edn. Oxon: Routledge. (Accessed: 10 October 2025).

Beek, M.H. ter, Legay, A., Lluch Lafuente, A. & Vandin, A. (2021) ‘Quantitative security risk modeling and analysis with RisQFLan’, *Computers & Security*, 109, 102381. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0167404821002054> (Accessed: 10 October 2025).

Chen, L. & Wang, B. (2024) ‘Disaster recovery strategies for cyber-physical systems considering the interdependence’, *Electric Power Systems Research*, 232, 110397. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0378779624002852> (Accessed: 10 October 2025).

Czekster, R.M., Webber, T., Furstenau, L.B. & Marcon, C. (2025) ‘Dynamic risk assessment approach for analysing cyber security events in medical IoT networks’, *Internet of Things*, 29, 101437. Available at: <https://www.sciencedirect.com/science/article/pii/S2542660524003780> (Accessed: 10 October 2025).

Hoffmann, R., Napiórkowski, J., Protasowicki, T. & Stanik, J. (2020) ‘Risk based approach in scope of cybersecurity threats and requirements’, *Procedia Manufacturing*, 44, pp. 655–662. Available at: <https://www.researchgate.net/publication/341136800_Risk_based_approach_in_scope_of_cybersecurity_threats_and_requirements> (Accessed: 10 October 2025).

Kesa, D.M. (2023) ‘Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations’, *World Journal of Advanced Research and Reviews*, 18(03), pp. 970–992. Available at: <https://wjarr.com/content/ensuring-resilience-integrating-it-disaster-recovery-planning-and-business-continuity> (Accessed: 10 October 2025).

Morales, C. (2025) ‘Cyber Risk Management in Practice: A Guide to Real-World Solutions’, pp. 80–108. Available at: <https://www.tandfonline.com/doi/full/10.1080/07366981.2025.2489225> (Accessed: 10 October 2025).

Son, K.-S., Song, J.-G. & Lee, J.-W. (2023) ‘Development of the framework for quantitative cyber risk assessment in nuclear facilities’, *Nuclear Engineering and Technology*, 55(6), pp. 2034–2046. Available at: <https://www.sciencedirect.com/science/article/pii/S1738573323001328> (Accessed: 10 October 2025).

Zadeh, A., Lavine, B., Zolbanin, H. & Hopkins, D. (2023) ‘A cybersecurity risk quantification and classification framework for informed risk mitigation decisions’, *Decision Analytics Journal*, 9, 100328. Available at: <https://www.sciencedirect.com/science/article/pii/S2772662223001686> (Accessed: 10 October 2025).