1. Introduction

Supply chain security and product quality assurance are essential concerns for business infrastructure in Industry 4.0. Supply chain security has been defined as “the application of policies, procedures, and technology to protect supply chain assets [...] from theft, damage, or terrorism” (Closs and McGarrell, 2004: 8), while product quality can be described as: “the assurance of quality of a product by means of a system which will manage quality and the product (Baines, et al., 2006: 91).

Simulated risk assessments are the standard method by which an organization can measure the likelihood of any category of risk (Olsen & Wu, 2017), as this method “allows users to apply whatever probability distributions exist in their particular applications” (Olsen & Wu, 2008: 653) to implement a fully-customized model for the projection of future risk (Chan & Chan, 2006).

It is thus the intent of this report to carry out a simulated risk assessment of supply chain security and product quality as applied to the organization Pampered Pets. Historical and objective data will first be reviewed and interpreted, followed by a simulated risk assessment. Results and conclusions from the simulation will be analysed and discussed, and applicable mitigation suggestions will be recommended. Finally, a disaster recovery plan will be outlined.

1 2. Quality and Safety Risks

Threats to maintaining product quality and supply chain safety can be separated into ‘Operational’ and ‘Hazardous’ taxonomies (*Table 1,* Bischof et al., 2009; Power, 2005; EEU, 2022; EM-DAT, 2021; Mitre, 2021). A historical disaster risk analysis and cyber vulnerability severity analysis of these risk categories are undertaken in sections 2.1 and

2.2 to provide context for the simulated risk assessment and mitigation selection in sections 3.1, 4.1, and 4.2.

Table 1: Operational & Hazardous Risks

Operational Risks		Hazardous Risks	
Technological	Cyber security	Climatological	Drought
Technological	Machinery		Wildfires
	Transport/distribution	Geophysical	Earthquakes
Product Quality	Regional standards	Hydrological	Floods
	Raw materials		Landslides
		Meteorological	Storms
			Extreme temperatures

1 2.1 Historical Disaster Risk

EM-DAT, an international disaster database (2021), provided historical data to calculate the proportion of disaster occurrence in key EU agricultural areas between 1980 and 2021 (*Table 2*). It should be noted data from the UK was not available. Proportion and probability statistics were used to calculate disaster occurrence (see Appendix I).

Table 2: Natural and Man-Made Disasters 1980-2021

Disaster Category	**Country**					
	France	Germany	Greece	Italy	Netherlands	Romania
Climatological	1.45%	0.09%	1.45%	1.03%	0.00%	0.17%
Geophysical	0.09%	0.17%	2.22%	2.22%	0.09%	0.26%
Hydrological	5.39%	1.88%	2.22%	4.62%	0.34%	4.36%
Meteorological	8.04%	5.90%	1.28%	2.99%	2.82%	2.48%
Technological[1]	5.22%	3.85%	4.02%	7.10%	1.37%	1.80%
Total % (Country)	**20.19%**	**11.89%**	**11.21%**	**17.96%**	**4.62%**	**9.07%**

[1]. 'Technological' refers to industrial machinery, modes of transportation, etc. See section 2.2 for cyber threat analysis.

Disaster Category	Country				
	Poland	Portugal	Spain	UK	**Total % (Category)**
Climatological	0.26%	1.54%	1.88%	N/A	**7.87%**
Geophysical	0.09%	0.00%	0.17%	N/A	**5.30%**
Hydrological	1.28%	0.94%	2.74%	N/A	**23.78%**
Meteorological	3.59%	1.37%	2.91%	N/A	**31.39%**
Technological	1.88%	1.28%	5.13%	N/A	**31.65%**
Total % (Country)	**7.10%**	**5.13%**	**12.83%**	**N/A**	**100.00%**
Probability of disaster occurrence/day:			8%		

The following results were significant:

- Highest disaster occurrence by country: France (20.19%)
- Highest disaster occurrence by category: technological (31.65%)
- Probability of disaster occurrence on an individual day: 8%

2 2.2 Cyber Security Vulnerabilities

Mitre's CAPEC Supply Chain taxonomy (2021) provided objective data to determine which cyber vulnerabilities specific to the supply chain have the highest severity and likelihood of occurrence (Table 3). TOPSIS was used to calculate the total severity, as this method computes the normalized ranking of objective data (*Çelikbilek & Tüysüz, 2020*, see Appendix II) .

The following results were significant:

- Most frequent attack types: information disclosure, data tampering
- Attacks with the highest severity (Pi score): leveraging/manipulating configuration search file paths, WSDL scanning
- Top ten total attack surface (supply chain): 12.66%

Table 3: TOPSIS Pi Top Ten

Vulnerability	STRIDE	Pi	Percentage
Leveraging/Manipulating Configuration File Search Paths	T	1	1.27%
WSDL Scanning (var. 1)	I	0.91	1.27%
WSDL Scanning (var. 2)	I	0.83	1.27%
Directory Indexing (var. 1)	I	0.82	1.27%
Bluetooth Impersonation AttackS (BIAS)	S, E	0.82	1.27%
Repo Jacking	T, I	0.82	1.27%
Collect Data from Registries	I	0.76	1.27%
Collect Data from Screen Capture	I	0.76	1.27%
Metadata Spoofing	S	0.76	1.27%
Altered Component Firmware (var. 3)	T, E	0.73	1.27%
Total Attack Surface:			**12.66%**

2 3. Pampered Pets' Simulated Risk Assessment

For Pampered Pets, the Monte Carlo Simulation (MCS) model was chosen to perform the risk assessment, as MCS provides "sets of assumptions concerning the relationship among model components" (Olsen & Wu, 2017: 70) which "allows making literally any assumption" (ibid: 73) necessary for organizational risk compliance.

The following parameters to the equation were assigned (see Appendix III):

- A Normal Probability Distribution
- 8 risk factors chosen from Operational and Hazardous taxonomies
- 90% confidence intervals for risk factors

The following assumptions were made:

- Subjective probability weightings
- Breadth of risk factor categories utilized

1 3.1 Assessment Results

The following results were significant:

- Highest potential disruption cost: Cloud server breach (£2,458,486.01)
- Highest subjective risk probability: warehouse distribution – orders (66%)
- Highest quantitative risk probability: supply chain disruption – ingredients (7%)
- A Cloud server breach would comprise 91.3% of the total potential disruption cost

Table 4: Monte Carlo Simulation – Product Quality & Supply Chain Risk

Risk Category	Target	Impact ($)	Timeframe	Subjective Probability	Quantitative Probability
Cloud server breach	Inventory	£2,458,486.01	>24 months	20%	5%
Supply chain disruption	Ingredients	£54,470.46	<12 months	10%	7%
Warehouse disruption	Orders	£93,423.34	<12 months	66%	5%
Warehouse disruption	Machine failure	£362,304.74	<18 months	10%	1%
Cloud server breach	Supplier info	£95,763.21	>24 months	5%	4%
Warehouse disruption	Power outage	£122,324.88	< 24 months	3%	5%
Supply chain disruption	Flooding	£341,853.60	>36 months	7%	5%
Supply chain disruption	Drought	£231,815.70	>48 months	2%	4%

Avg. Subjective Probability	Avg. Quantitative Probability	Potential Disruption Cost
15.3%	4.45%	£2,693,846.51

Accordingly, the following can be inferred as essential components of product quality/supply chain security:

- Cloud server security
- Data integrity
- Order distribution assurance
- Quality ingredient assurance

These components will thus inform the focus of the risk mitigation suggestions in the following section.

3 4. Risk Mitigation

1 4.1 Natural and Man-Made Disaster Mitigation

MCS was performed to determine the optimal ratio for uninterrupted supply chain performance in the event of a natural or man-made disaster (see Appendix IV). The following assumptions have been applied:

- Main inventory/vendor locations are within the UK/EU
- The supply chain should have very little performance variance
- Alternate warehouse locations should ensure equivalent product quality

Table 5: Pampered Pets Inventory Simulation - Policies

Policy	Reorder Point	Order Quantity	Parameters for MCS Simulation	
1	5000	8000	Mean Unit Demand	4500
2	4000	8000	Fixed Order Cost	£50
3	5500	100	Unit Cost	£1
4	6000	9100	Sales Price	£5
5	800	300	Holding Cost	£1
6	6000	400	Salvage Value	£3
7	500	500		

Table 6: Monte Carlo Simulation – Inventory

Policy	Mean Profit	Sales Revenue	Order Cost	Holding Cost	Out-of-Stock
1	£230,075.88	£432,268	£104, 650	£108,015	0%
2	£230,599.23	£536,030	£104,650	£84,496	8%
3	£230,960.33	£57,000	£3,600	£4,957	92%
4	£**231,867.46**	£**540,335**	£**109,800**	£**178,415**	**0%**
5	£230,749.71	£78,500	£8,050	£4,857	92%
6	£230,837.02	£73,200	£10,800	£5,257	92%
7	£230,506.15	£100,500	£12,650	£4857	92%

Policy	Risk of Loss	Overall Rating
4	0%	Best
2	33%	Middle
3	200%	Worst

Policy 4, with a reorder point of 6000 and a order quantity of 9100, had the following optimal characteristics:

- Highest mean profit: £231,867.46
- Lowest Out-Of-Stock rating: 0%
- Lowest Risk of Loss rating: 0%

Thus this policy would perform most adequately in the event a warehouse source is lost and production were required to increase at a second location.

Table 7: SMART Calculation – Supplier by Country

Supplier Country	Crop Output (€M)	Crop Price	Animal Output (€M)	Animal Price
France	**€47,973.66**	**€128.30**	**€26,847.40**	**€112.80**
Germany	€29,698.62	€129.30	€25,917.59	€116.50
Greece	€8,725.22	€156.10	€2,455.55	€125.80
Italy	**€34,283.10**	**€124.30**	**€16,353.91**	**€113.70**
Netherlands	€15,671.56	€118.70	€10,954.00	€113.50
Poland	€13,620.87	€131.10	€13,584.02	€117.20
Portugal	€6,072.62	€126.60	€3,053.82	€115.20
Romania	€15,028.32	€334.50	€4,245.42	€287.30
Spain	**€34,999.84**	**€121.40**	**€20,478.57**	**€116.10**
UK	€9,803.06	€164.40	€16,574.00	€150.10

Supplier Country	Organic Crops (tonne)	Organic Livestock (head)	Disaster Rate	SMART Score
France	**692,243.00**	**860,308.00**	**20.19%**	**75.49**
Germany	0.00	861,272.00	11.89%	63.25
Greece	152,118.00	163,066.00	11.21%	35.00
Italy	**968,425.00**	**397,187.00**	**17.96%**	**71.18**
Netherlands	19,591.00	76,069.00	4.62%	55.24
Poland	315,269.00	31,102.00	7.10%	46.70
Portugal	0.00	92,673.00	5.13%	41.83

Romania	229,794.00	19,870.00	9.07%	23.16
Spain	**382,153.00**	**219,769.00**	**12.83%**	**62.31**
UK	129,297.00	300,788.00	N/A	28.50

Rank	Country	SMART Rating
1	France	75.49
2	Italy	71.18
3	Spain	62.31

A SMART analysis (see Appendix IV) was conducted on the agriculture industry of ten key EU states with a data combination of Eurostat's (2022) and the historical disaster rate calculated in section 2.1 to determine an optimal second location (Table 7). Significant desirability factors include:

- High count of organic crops (Italy: 968,425) and livestock (France: 860,308)
- High crop and animal output (France: €47,973.66, €26,847.40)
- Low crop (Spain: €121.40) and animal (France: €112.8) prices

It should be noted, however, that these countries showed higher rates of disaster occurrence. Still, given the geographical distance between these locations and the main Pampered Pets' warehouse, these should serve well to diversify the supply chain area to reduce risk.

2 4.2 Cyber Security Risk Mitigations

Cyber security mitigations are more technical in nature, involving recommendations from the CAPEC ATT&CK taxonomy (Mitre, 2021). Relevant attack categories and proposed mitigations are listed in Table 8.

Table 8: CAPEC Mitigation Recommendations

Attack Category	Mitigation recommendations
Excavation	● Reduce error/response, only necessary warnings

	● Remove all non-essential information
Hardware Integrity Attack	● No unauthorized access to the system
Malicious Logic Insertion	● Use Anti-Virus software to detect/isolate viruses ● Cease operation of compromised applications
Manipulation During Distribution	● Cross-check all vendor shipping sources ● Tamper-evident packaging
Metadata Spoofing	● Validate authors, timestamps, statistics ● Authenticate open-source code/products ● Leverage automated testing techniques
Modification During Manufacture	● Ensure the authenticity of digital certificates ● Buy hardware only from trusted vendors ● Implement configuration management security practices
Resource Location Spoofing	● Monitor application activity log for unauthorized use
Software Integrity Attack	● Validate software updates before installation ● Implement DAWG and KPTI ● Disable ‘Copy-on-Write’ between Cloud VMs

4 4. Disaster Recovery

Disaster recovery (DR) in the event of a natural disaster or security breach can allow a business to “[replicate an] application state between two data centres; if the primary data centre becomes unavailable, then the backup site can takeover” (Cecchet et al., 2010: 1). There are a number of benefits with and repercussions without the implementation of a DR plan (Table 9).

Table 9: DR Benefits & Repercussions

Benefits With	**Repercussions Without**
GDPR Compliance	GDPR non-compliance
Continued operation	Loss of sales/revenue
Fast resumption of service	Regulation penalties
Lowered Cost and hazard risk	Loss of contract/penalties
Increase in trustworthiness	Loss of trustworthiness

Given the specification of <1 minute RTO and <1 minute RPO, the use of VMWare to consolidate virtual data (Figure 1) is recommended in coordination with Amazon’s AWS and Pampered Pets' current local system (Figure 2). Table 10 demonstrates the reasoning behind this recommendation (VMWare, n.d.a; Amazon, n.d.a).

*Figure SEQ Figure * ARABIC 1: VMWare Cloud Recovery Scheme (VMWare, n.d.b.)*

*Figure SEQ Figure * ARABIC 2: Pampered Pets' AWS/Cloud Structure*

Table 10: Benefits of VMWare & Amazon AWS Utilization

VMWare	Amazon AWS
Virtual Machine creation	Cross-Cloud service with VMWare
Local and Cloud storage options	Cognito ID service
Less Bandwidth/electricity use	API Gateway
Lowered IT costs	Kinesis data streams
Instant company asset replication	Dynamo DB cloud database
Snapshot recovery	S3 bucket storage and encryption
Active-Active/Hot-Standby capability	Active-Active/Hot-Standby capability

Having an Active-Active/Hot-Standby server will allow a <1 minute recovery for both RTO and RPO. In addition, VMWare implements a detailed data protection lifecycle (*Figure 3*), along with three key areas of GDPR compliance (*Figure 4*). This combination satisfies several GDPR requirements of organization supply chain management (GDPR, 2018, VMWare, 2017).

*Figure SEQ Figure * ARABIC 3: GDPR Compliance -- 3 Key Areas (VMWare, 2017)*

Amazon AWS utilizes a similar compliance program (Table 11), which enables a comprehensive security scheme compatible with diverse needs (AWS, 2022). It should be noted that AWS employs a “shared responsibility security model,” (AWS, 2022: 3) which requires customers to set many data privacy settings independently, is thus dependent on end-user settings and must be cross-examined to be fully GDPR compliant (GDPR, 2018, AWS, 2022).

Table 11: Amazon AWS GDPR Compliance

AWS Compliance Framework	
The CISPE code of conduct	Custom permissions settings
Data access controls	Custom boundaries for regional service access
Identity & access management	Application access controls
Temporary tokens (AWS STS)	Application monitoring and logging
Multi-factor authentication	Data encryption

5 5. End Summary

Supply chain safety and product quality are essential aspects of risk management. In this report, a simulated risk assessment performed on Pampered Pets found elevated levels of risk concerning Cloud server security, data integrity, order distribution assurance, and quality ingredient assurance. Relevant mitigation suggestions, including optimal order/restock ratios and alternative warehouse locations, were discussed. In addition, a Disaster Recovery plan with <1 minute RTO and RPO was outlined along with relevant GDPR compliance.

6. Appendices

1 6.1. Appendix I

2 To find the proportion and probability of the disaster data, the following steps were performed:

1. Isolate and index each country dataset (Figure 5)

2. Sum the various categories of disaster by subtype and country using =COUNTIF (Figures 6 & 7)

3. Sum the subcategories into main categories by country (Figures 8 & 9).

4. Calculate the disaster proportion by country using P=C/T, if P = proportion, C = disaster category, T = total disasters (Figures 10 & 11).

*Figure SEQ Figure * ARABIC 5: EM-DAT Country Data*

*Figure SEQ Figure * ARABIC 6: =COUNTIF Excel Formula*

*Figure SEQ Figure * ARABIC 7: =COUNTIF Results*

*Figure SEQ Figure * ARABIC 8: Category Totals Excel Formula*

3

*Figure SEQ Figure * ARABIC 9: Category Totals Results*

*Figure SEQ Figure * ARABIC 10: Category Percentage by Country Excel Formula*

*Figure SEQ Figure * ARABIC 11: Category Percentage by Country Results*

6.2. Appendix II

The TOPSIS calculation for CAPEC Supply Chain attack severity in Section 2.2 involves 7 steps (Mathew, 2018):

- Calculate the normalized matrix
- Calculate the weighted normalized matrix
- Calculate the ideal worst value (V-)
- Calculate the ideal best value (V+)
- Calculate the Euclidean distance from the ideal best (S+)
- Calculate the Euclidean distance from the ideal worst (S-)
- Calculate the Performance Score (Pi)

4 To perform this analysis on Excel, the following steps were undertaken

6.2.1. Calculating the Normalized Matrix

1. CAPEC data was collected and indexed according to the ‘Attack Likelihood’, ‘Attack Severity’, and ‘Skill Level Required’ of a vulnerability (Figure 12)
2. Each Severity is assigned a number on a scale of 5-0, Very-High - Very Low. Each rating is then squared (Figure 13 & 14)
3. A sum of the squares for each category are found (Figure 15)
4. The Normalized Matrix equation (x/(s)^.05) is then performed on individual category scores, where x = AL/TS/SR scores and s = the summed square root, finding the

*Figure SEQ Figure * ARABIC 12: CAPEC Supply Chain Vulnerability Index*

Normalized Matrix (figure 16 & 17)

*Figure SEQ Figure * ARABIC 13: Excel formula for Severity Rating and Squared Value*

*Figure SEQ Figure * ARABIC 14: Severity Rating and Squared Value*

*Figure SEQ Figure * ARABIC 15: Sum of the Square Values*

*Figure SEQ Figure * ARABIC 16: Normalized Excel Formula*

*Figure SEQ Figure * ARABIC 17: Normalized Matrix Score*

5

6

7

8

9

10 6.2.2 Calculating the Weighted Normalized Matrix

1. Weights for Attack Likelihood, Typical Severity, and Skills Required are assigned to the Normalized Matrix categories (Figure 12 & 13). For this calculation, each have the weight 1/3.

2. AL/TS/SR Scores are then multiplied by the assigned weight to find the weighted Normalized Matrix score (Figure 18 & 19)

*Figure SEQ Figure * ARABIC 18: Weighted Excel Formula*

*Figure SEQ Figure * ARABIC 19: Weighted N. Matrix Score*

6.3.3 Calculating the Ideal Best/Worst Values

1. Calculating the ideal best (V+) and ideal worst (V-) values use a variation of the same equation (Figure 20). The transposition of this equation into an Excel formula is demonstrated in Figure 21, wherein the maximum and minimum AL/TS/SR scores are obtained.

   It should be noted that ideal best scores can be as high as 1 and ideal worst scores can be as low as 0.

*Figure SEQ Figure * ARABIC 20: Vi+/- Equation (Matthew, 2018)*

*Figure SEQ Figure * ARABIC 21: Ideal Best/Worst Value Excel Formula*

*Figure SEQ Figure * ARABIC 22: Ideal Best/Worst Value Scores*

6.3.4 Calculating the Euclidean Distance from the Ideal Best/Worst Values

1. Calculating Euclidean Distance for ideal best and worst values uses a variation of the same equation (Figures 23 & 24).

*Figure SEQ Figure * ARABIC 23: Euclidean Distance Equation (Matthew, 2018)*

2. The Weighted AL/TS/SR scores are subtracted from V+/V-. This result is then squared

3. The squared sum of the three categories are added together and then squared by 0.5

4. The resulting number represents the Euclidean distance (figure 25)

*Figure SEQ Figure * ARABIC 24: Si+, Si-, Pi, Occurrence, & Percentage Excel Formulas*

*Figure SEQ Figure * ARABIC 25: Si+/-, Pi, Occurrence & Percentage Scores*

6.3.5 Calculating the Performance Score (Pi) and Percentage

1. Calculating the performance score involves the equation P = B/(W+B) (*Figure 24*). This equation will result in a decimal number between 1 and 0, 1 signifying the best rank and 0 signifying the worst (*Figure 25*).

2. Calculating the percentage provides the rate of occurrence of an individual attack. This calculation can be performed with the equation P = A/T, where P = percentage, A = the individual attack, and T = the total attack count, which is 76 (Figures 24 & 25).

11 6.3 Appendix III

12 The Monte Carlo simulation () was used to simulate both a quantitative risk probability and an optimal reorder uptake point for limited supply chain disruption in the event of a natural or man-made disaster.

6.3.1 Calculating the Probability of Risk Occurrence

1. Find the quantitative probability (*Figure 26*)

   - Identify 8 risk IDs and their contributing factors

- Randomly sample each risk 3 times and record the average for each
- Run this average in the Monte Carlo Simulation for 1000 repetitions
- Record the MIN and MAX variables using =COUNTIF for value/ratio matching to find the probability

2. Calculate the 90% Confidence Interval (*Figure 26)*
    - Use a lognormal distribution to calculate the mean and standard deviation from the lower and upper ranges
    - Find the financial impact using =lognorm.inv(rand()(lower range,Upper range)
        - Lognormal distributions can be used on large positive number sets that may skew in one direction

    - Results for these formulae can be seen in Figures 27, 28 & 29.
3. Calculations with Yasai
    - There were two different inventory analyses:
        - both contained 7 individual scenarios that ran through 5000 simulations (Figures 28 & 29)
    - Different scenarios included:
        - changes to product re-order quantities and re-order points in rolling stock numbers (Figure 27)
        - Comparing re-order quantities and re-order points to one another to optimize the numbers for a mitigation scenario (Figure 28)

Rand Prob Of Sub Prob	Quantitative Probability	distribution	LR and UR std.dev	LR and UR mean	(Financial impact) 90% CI of LR and UR lognormal rand distribution	Rand result of financial cost (zero when event did not occur)
=IF(RAND() < 0.2,1,0)	=R27	lognormal	=(LN(K6)-LN(I6))/3.29	=(LN(K6)+LN(I6))/2	=LOGNORM.INV(RAND(),P6,O6)	=IF(RAND()<0.2,LOGNORM.INV(RAND(),(LN(K6)+LN(I6))/2,(LN(K6)-LN(I6))/3.29),0)
=IF(RAND() < H7,1,0)	=R28	lognormal	=(LN(K7)-LN(I7))/3.29	=(LN(K7)+LN(I7))/2	=LOGNORM.INV(RAND(),P7,O7)	=IF(RAND()<H7,LOGNORM.INV(RAND(),(LN(K7)+LN(I7))/2,(LN(K7)-LN(I7))/3.29),0)
=IF(RAND() < H8,1,0)	=R29	lognormal	=(LN(K8)-LN(I8))/3.29	=(LN(K8)+LN(I8))/2	=LOGNORM.INV(RAND(),P8,O8)	=IF(RAND()<H8,LOGNORM.INV(RAND(),(LN(K8)+LN(I8))/2,(LN(K8)-LN(I8))/3.29),0)
=IF(RAND() < H9,1,0)	=R30	lognormal	=(LN(K9)-LN(I9))/3.29	=(LN(K9)+LN(I9))/2	=LOGNORM.INV(RAND(),P9,O9)	=IF(RAND()<H9,LOGNORM.INV(RAND(),(LN(K9)+LN(I9))/2,(LN(K9)-LN(I9))/3.29),0)
=IF(RAND() < H10,1,0)	=R31	lognormal	=(LN(K10)-LN(I10))/3.29	=(LN(K10)+LN(I10))/2	=LOGNORM.INV(RAND(),P10,O10)	=IF(RAND()<H10,LOGNORM.INV(RAND(),(LN(K10)+LN(I10))/2,(LN(K10)-LN(I10))/3.29),0)
=IF(RAND() < H11,1,0)	=R32	lognormal	=(LN(K11)-LN(I11))/3.29	=(LN(K11)+LN(I11))/2	=LOGNORM.INV(RAND(),P11,O11)	=IF(RAND()<H11,LOGNORM.INV(RAND(),(LN(K11)+LN(I11))/2,(LN(K11)-LN(I11))/3.29),0)
=IF(RAND() < H12,1,0)	=R33	lognormal	=(LN(K12)-LN(I12))/3.29	=(LN(K12)+LN(I12))/2	=LOGNORM.INV(RAND(),P12,O12)	=IF(RAND()<H12,LOGNORM.INV(RAND(),(LN(K12)+LN(I12))/2,(LN(K12)-LN(I12))/3.29),0)
=IF(RAND() < H13,1,0)	=R34	lognormal	=(LN(K13)-LN(I13))/3.29	=(LN(K13)+LN(I13))/2	=LOGNORM.INV(RAND(),P13,O13)	=IF(RAND()<H13,LOGNORM.INV(RAND(),(LN(K13)+LN(I13))/2,(LN(K13)-LN(I13))/3.29),0)
Average Quantitative probi						Total potential distruption cost
	='probability range'!E17					=R6+R7+R8+R9+R10+R11+R12+R13
	from 1000 simulations of eac					

*Figures SEQ Figure * ARABIC 26: Major Simulation Formulae*

*Figure SEQ Figure * ARABIC 27: Optimal Results from a Order-Size/Re-Order Point*

Figure : Results of an Optimal Re-Order Yasai Simulation

*Figure SEQ Figure * ARABIC 29: Results of a Quantitative Risk Yasai Simulation*

13

14 6.4 Appendix IV

A SMART score was calculated from historical data of 10 key agricultural areas in the EU. As country participation can vary yearly, all data was used from the last applicable year and no data sources have more than a two-year report gap (Eurostats, 2022).

As SMART scoring involves subjective opinion of category importance and weight (Olsen & Wu, 2008), all decisions were assessed with product quality and supply chain safety as the benchmark. Calculating the SMART score on Excel required the following (Wk portfolio, 2021):

1. A Table must be created with data from the earliest available year with not more than a two-year report gap (Figure 30).

2. Each row in the category column must be given a subjective rank from 0-100, 0 being the worst and 100 being the best (Figure 31).

3. A subjective weight is given to each category, which is then standardized (Figure 32 & 33)

4. The standardized column weights are summed with the subjective row rankings (Figure 34 & 35), thus achieving the final weighted rank score.

Figure SEQ Figure * ARABIC 30: Initial Eurostats Table

Figure SEQ Figure * ARABIC 31: Ranked Eurostats Table

Figure 32: Category Weights

Figure 33: Category Weight Results

*Figure SEQ Figure * ARABIC 34: Total Weighted Score Formula*

*Figure SEQ Figure * ARABIC 35: Total Weighted Score Results*

6

7 References

AWS (n.d.a) Six lock-in considerations
Available from:https://docs.aws.amazon.com/whitepapers/latest/unpicking-vendor-lock-in/six-lock-in-considerations.html[Accessed 2 December 2022]]

AWS (2022) *Navigating GDPR Compliance on AWS AWS Whitepaper*. rep. Amazon: 1–27.

Bründl, M., Romang, H.E., Bischof, N. & Rheinberger, C.M. (2009) The risk concept and its application in natural hazard risk management in Switzerland. *Natural Hazards and Earth System Sciences 9*(3): 801-813.

Çelikbilek, Y. and Tüysüz, F., 2020. An in-depth review of theory of the TOPSIS method: An experimental analysis. *Journal of Management Analytics*, *7*(2): 281-300.

Chan, F.T. & Chan, H.K. (2006) A simulation study with quantity flexibility in a supply chain subjected to uncertainties. *International Journal of Computer Integrated Manufacturing 19*(2): 148-160.

Closs, D.J. & McGarrell, E.F. (2004) *Enhancing security throughout the supply chain*. Washington, DC: IBM Center for the Business of Government.

EEU (2022) *Database - Agriculture - Eurostat*. Available at: https://ec.europa.eu/eurostat/web/agriculture/data/database (Accessed: December 6, 2022).
EEU (2018) *GDPR Official Legal Text*, *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/ (Accessed: December 6, 2022).

EM-DAT (2021) *EM-DAT Public*, *Public.emdat.be*. Available at: https://public.emdat.be/ (Accessed: December 6, 2022).

Hubbard, D.W. and Seiersen, R., 2016. *How to measure anything in cybersecurity risk*. John Wiley & Sons.

Manning, L., Baines, R.N. & Chadd, S.A. (2006) Quality assurance models in the food supply chain. *British Food Journal*.

Mitre (2021) *Common attack pattern enumeration and classification*, *CAPEC*. Available at: https://capec.mitre.org/data/definitions/437.html (Accessed: December 6, 2022).

Power, M. (2005) The invention of operational risk. *Review of International Political Economy 12*(4): 577-599.

SMART Simple Multi Attribute Rating Technique (2021) *YouTube*. Available at: SMART Simple Multi Attribute Rating Technique (Accessed: December 6, 2022).

TOPSIS using Excel - MCDM problem (2018) *YouTube*. YouTube. Available at: https://www.youtube.com/watch?v=Br1NQK0Iumg (Accessed: December 6, 2022).

VMWare (n.d.a) The Benefits of DRaaS: Minimizing Time to Value. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-The-value-of-draas-ebook.pdf

VMWare (2017) *IT Management and the GDPR: The VMWare Perspective*. rep. VMWare: 1–8.

VMware (n.d.b) A Brief Overview of VMware Cloud Disaster Recovery. Available from:https://vmc.techzone.vmware.com/resource/brief-overview-vmware-cloud-disaster-recovery#protectedproduction-sites [Accessed 2 December 2022]

Wood, T., Cecchet, E., Ramakrishnan, K.K., Shenoy, P., Van Der Merwe, J. and Venkataramani, A., 2010. Disaster recovery as a cloud service: Economic benefits & deployment challenges. In *2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10)*.

Wu, D. & Olson, D.L. (2008) Supply chain risk, simulation, and vendor selection. *International journal of production economics 114*(2): 646-655.