SARM Unit 11 Assignment

Individual Project: Executive Summary

40% weighting; 2000 words

Assignment Brief

Cathy has decided to start the digitalisation process. In addition to the changes you recommended, she has decided to add an international supply chain and a number of automated warehouses worldwide. The changes immediately attract the attention of two very high-profile new customers – HRH the King and Prince Albert 2nd of Monaco. However, both are concerned about the effect of these digitalisation changes on the world-famous quality of the products and the security of the supply chain.

Produce an Executive Summary which provides an estimate of the probabilities that changes to the operations of the business and the supply chain could endanger both the quality and availability of the company's products. Note that the associated grading criteria are highlighted in the requirements below, to be reviewed alongside the criteria grid located in Module Resources.

Executive Summary

Checklist:

1. Enumerate the potential risks to the quality and supply chain for the company (Knowledge and Understanding weighted at 10%, Use of relevant sources weighted at 10%). This should include:
    1. The selection of quantitative risk modelling approach(es) with justification for the method chosen.
    2. Explanation of the calculations carried out, including detailed lists of assumptions and sources of data selected (where appropriate).
    3. Results of the quantitative models used.
2. Based on the quantitative modelling above, produce a summary of the results along with your recommendations around the potential risk of loss of quality (with

the probability of it occurring); the potential risk of supply chain issues including a list of potential issues with associated probability of them occurring. See the reading for specific chapters of your core ebook that provide data and guidance on the techniques used above. (Knowledge and Understanding weighted at 10%, Criticality weighted at 20%, Use of relevant sources weighted at 5%).

3. Ms O'dour has also recommended that if the business is to be digitalised, there should also be put into place a business continuity/ disaster recovery (DR) strategy that will ensure that the business' online presence could continue in the event of a disaster affecting the shop premises. The online shop needs to be available 24/7/365 with a less than 1 minute changeover window should DR need to be invoked. She has also recommended that the business cannot afford to lose more than 1 minute of data. Your team are tasked with the job of designing a DR solution that meets Ms. O'dour's requirements. She also wants you to recommend the platform that should be chosen to host the solution and to provide advice on vendor lock-in. (Knowledge and Understanding weighted at 10%, Criticality weighted at 10%, Use of relevant sources weighted at 5%).

Presentation and Structure of your findings (weighted at 10%) includes spelling, organisation, as well as evidence of proofreading. You will also be assessed on the correct use (and format) of citations and references in your work (Academic Integrity weighted at 10%).

Note that the executive summary should organise any recommendations in order of the priority to the business' commercial needs. The organisation is particularly interested in how well they meet current security standards (including the new GDPR directive) and expect to see any mitigations required to meet such standards clearly called out as important business requirements.

Please also note that appendices should not be used to extend the core report as reports should stand alone, complete and concise, without the appendices. They should really only be used if required, and only for supplementary and/ or supporting information (for example, to provide details of calculations). One key part of the exercises in this module is the need to be to be able to express ideas succinctly, concisely and with necessary brevity.

Plan

1. Read the Assignment Brief Thoroughly
    - Advice: Understand the requirements, grading criteria, and expectations. Highlight key points and make notes of important details to refer to later.

WEDNESDAY

2. Identify Potential Risks
    - Advice: List all potential risks to the quality and supply chain due to digitalisation, including international supply chain and automated warehouses. Use sources such as industry reports, academic papers, and case studies for insights.
3. Select Quantitative Risk Modelling Approach(es)
    - Advice: Research different quantitative risk modelling methods (e.g., Monte Carlo simulations, fault tree analysis). Justify your choice based on the context of the business and the type of risks identified. Explain why the chosen method is appropriate for estimating probabilities.
    - Watch YouTube videos on quantitative analysis techniques
    - Read recommended quantitative reading and take notes
    - Find some articles on quantitative analysis
4. Gather Data and Make Assumptions
    - Advice: Collect relevant data from credible sources (e.g., historical data, industry benchmarks). Clearly list all assumptions made during the modelling process. Ensure assumptions are realistic and based on sound reasoning.
5. Conduct Risk Calculations
    - Advice: Use the selected quantitative methods to calculate the probabilities of the identified risks. Document each step of the calculation process, ensuring clarity and transparency. Validate your results by cross-checking with existing literature or expert opinions.
6. Summarise the Quantitative Model Results
    - Advice: Present the results of your risk calculations in a clear and concise manner. Use charts, graphs, or tables to enhance understanding. Summarise key findings, highlighting the most significant risks and their probabilities.
7. Provide Recommendations on Risk Management
    - Advice: Based on the quantitative results, recommend strategies to mitigate the identified risks. Address both quality and supply chain issues. Prioritise recommendations based on their potential impact on business operations and commercial needs.
8. Design a Business Continuity/Disaster Recovery (DR) Strategy
    - Advice: Develop a comprehensive DR plan that ensures the online shop's availability with less than 1-minute downtime. Consider backup solutions, failover mechanisms, and data replication strategies. Recommend suitable platforms (e.g., cloud providers) and address vendor lock-in risks.
9. Recommend a Hosting Platform and Discuss Vendor Lock-in

- Advice: Evaluate different hosting platforms (e.g., AWS, Azure, Google Cloud) based on reliability, scalability, and compliance with security standards. Provide a rationale for your chosen platform. Discuss strategies to mitigate vendor lock-in, such as using multi-cloud solutions or open-source technologies.

10. Ensure Compliance with Security Standards
    - Advice: Identify relevant security standards (e.g., GDPR, ISO 27001) and ensure your recommendations comply with these. Highlight any specific mitigations required to meet these standards, emphasising their importance to business continuity and customer trust.
11. Organise and Draft the Executive Summary
    - Advice: Structure your executive summary logically, starting with an introduction, followed by risk identification, quantitative modelling results, risk management recommendations, DR strategy, and hosting platform choice. Ensure it flows well and covers all required aspects succinctly.
12. Review Presentation and Structure
    - Advice: Check for spelling, grammar, and coherence. Ensure the report is well-organised and professional. Use headings, subheadings, and bullet points for clarity. Proofread multiple times and consider peer reviews.
13. Use Correct Citations and References
    - Advice: Follow the required citation style consistently. Include in-text citations for all sources referenced and compile a bibliography. Use tools like citation managers (e.g., EndNote, Zotero) to keep track of references.
14. Prepare and Include Any Necessary Appendices
    - Advice: Use appendices only for supplementary information, such as detailed calculations or raw data. Ensure the main report is complete and self-contained.
15. Final Proofreading and Submission
    - Advice: Do a final review of the entire document. Ensure all requirements are met, the document is polished, and all sections are clearly written. Submit before the deadline, ensuring all files are correctly formatted and attached.

Digitalisation Risks

	Quality of product	Security of supply chain
E-commerce	Larger customer reach may mean higher production and potentially lower quality	Integration with existing supply chain is another moving part to protect
Online marketing/blogs	Any poor reviews may have greater effect on perceived quality	Information may provide OSINT for attack reconnaissance

International supply chain	Geographical distance may affect ability to evaluate quality	Differing standards and unfamiliar legislation
Automated warehouse	Less human intervention with product testing	IoT devices may have unproven security measures
ERP system	Risk of data corruption	Integration with other systems may introduce a weak link if not properly configured

Technological failures
Supply chain risk - logistical delays
Data security risk - supplier and vendor
Regulatory compliance - GDPR, digital supply chain
Technology integration

Potential Risks to Product Quality

1. Data Integrity Issues:
    - Risk of data corruption or inaccuracies within the ERP system affecting product specifications and production processes.
    - Impact: Inconsistent product quality and customer dissatisfaction.
2. Automation Errors:
    - Risk of errors in automated warehouse systems leading to incorrect handling, storage, or picking of products.
    - Impact: Damaged or incorrect products being shipped to customers.
3. System Integration Problems:
    - Risk of integration issues between new digital systems (e.g., ERP, e-commerce) and existing systems.
    - Impact: Disruptions in production processes and quality control measures.
4. Loss of Human Oversight:
    - Risk of reduced human intervention in quality control due to increased automation.
    - Impact: Missed defects and quality issues that automated systems might not detect.
5. Supply Chain Disruptions:
    - Risk of international supply chain issues affecting the availability and quality of raw materials.
    - Impact: Variability in product quality due to inconsistent material supply.

Potential Risks to Supply Chain Security

1. Cybersecurity Threats:
    - Risk of cyber-attacks targeting supply chain management systems.
    - Impact: Unauthorised access to supply chain data, leading to data breaches and operational disruptions.
2. Logistical Complexities:
    - Risk of complexities and errors in managing an international supply chain.
    - Impact: Delays, lost shipments, and increased vulnerability to fraud.
3. Vendor Reliability:
    - Risk of relying on international vendors who might face their own operational or security issues.
    - Impact: Inconsistent supply, delays, and potential compromise of supply chain integrity.
4. Data Synchronisation Issues:
    - Risk of inaccurate or delayed data synchronisation between ERP, e-commerce, and supply chain systems.
    - Impact: Inventory discrepancies and supply chain inefficiencies.
5. Physical Security of Automated Warehouses:
    - Risk of physical security breaches at automated warehouse locations.
    - Impact: Theft, tampering, or sabotage of products and materials.

Potential Legal Risks

1. Compliance with Data Protection Regulations:
    - Risk of non-compliance with data protection laws (e.g., GDPR, CCPA) when handling customer data through e-commerce and online marketing.
    - Impact: Legal penalties, fines, and reputational damage.
2. Intellectual Property (IP) Risks:
    - Risk of IP theft or infringement in digital marketing and e-commerce operations.
    - Impact: Legal disputes and financial losses.
3. Product Liability:
    - Risk of legal claims arising from defects or issues in products sold through digital channels.
    - Impact: Lawsuits, recalls, and financial compensation.
4. International Trade Regulations:

- Risk of non-compliance with international trade laws and regulations when managing an international supply chain.
- Impact: Fines, sanctions, and operational disruptions.

5. Consumer Protection Laws:
    - Risk of failing to meet legal requirements for online transactions, advertising, and product disclosures.
    - Impact: Legal action, fines, and loss of consumer trust.

Mitigation Strategies

1. Robust Cybersecurity Measures:
    - Implement advanced cybersecurity protocols and regularly update systems to protect against cyber threats.
2. Regular Quality Audits:
    - Conduct frequent quality control audits and inspections to ensure product quality and process integrity.
3. Reliable Data Management:
    - Ensure accurate data entry and synchronisation across all digital systems to maintain data integrity.
4. Vendor Management:
    - Develop strong relationships with reliable vendors and have contingency plans for supply chain disruptions.
5. Compliance Programs:
    - Establish comprehensive compliance programs to adhere to data protection, trade regulations, and consumer protection laws.
6. Training and Awareness:
    - Provide regular training for employees on new systems, cybersecurity best practices, and compliance requirements.
7. Disaster Recovery Plans:
    - Develop and test disaster recovery plans to ensure quick recovery from data loss or system failures

Risk to quality	Probability	Impact
Data integrity issues - corruption of ERP system affects production processes		
Automation errors - automated warehouse errors in production, packaging, picking		
Integration - Existing systems struggle to integrate with e-commerce, ERP system, international supply chain		

Seminar notes

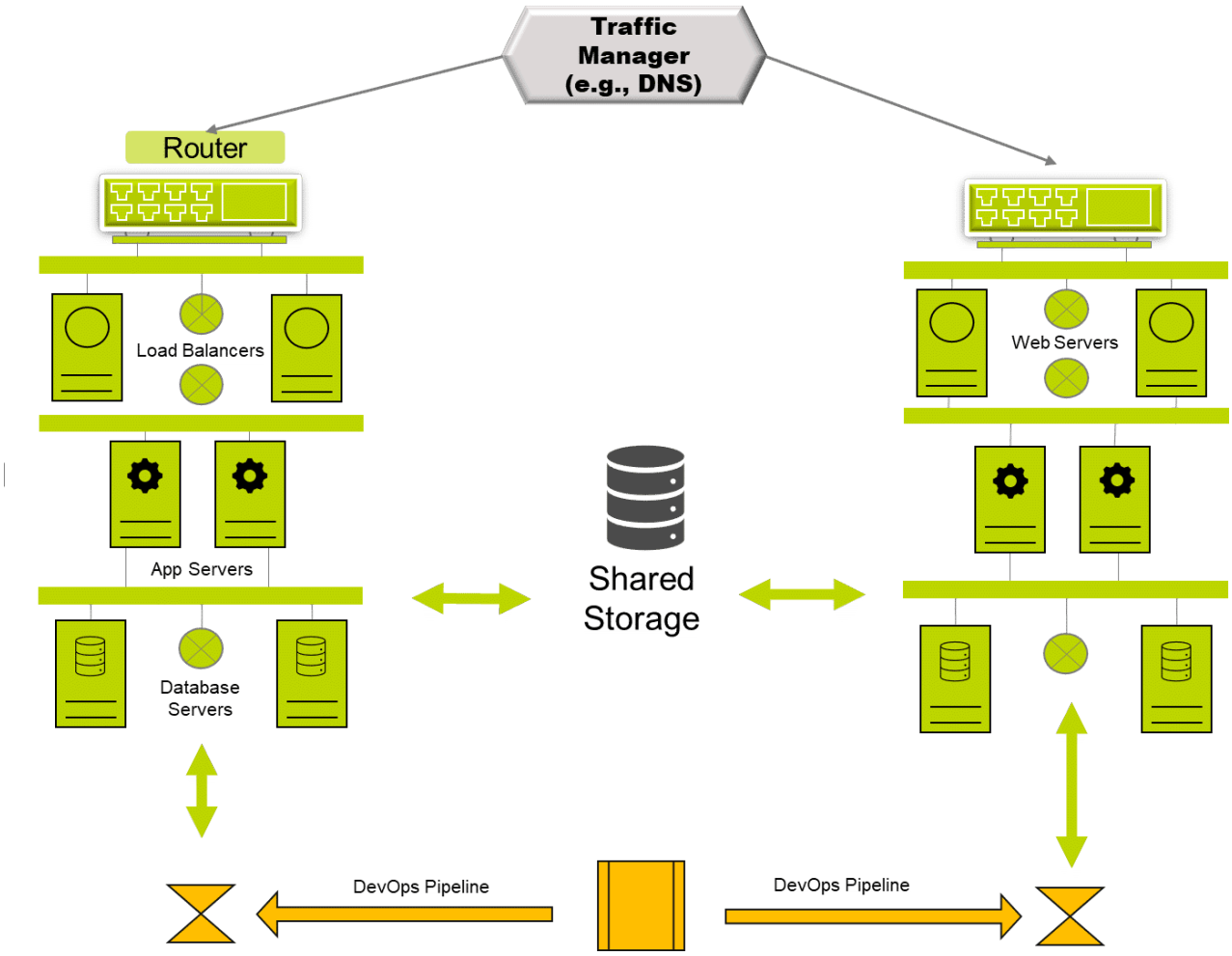
Checklist 1
Quantitative risk modelling with justification - digitalisation supply chain expansion - graphs - clear, numerical evaluation of risks - executives need to be able to read - results, summary of along with recommendations. Quality risks, supply chain risks, legal risks - mitigate the impact of all the risks

Checklist 2
Summary of results

CHecklist 3
Recommend host - comment on vendor lock in - AWS disaster recovery architecture - AWS Aurora global database. Regular monitoring and alerting - aws Lambda

DR

Use activity in prep for seminar 6



2 concurrent systems, ideally in different regions, traffic manager monitoring to detect fails and switch over to second without disruption. Code deployed simultaneously, option to use blue green strategy, database should be configured as AOAG groups or use CosmosDB. Data copied synchronously

CATEGORY	PROS	CONS	CAVEATS
Availability	Active-active provides immediate, tested always on service.	Cost of additional environments.	Applications must be designed to be active-active ready.

Recoverability	Synchronous copies means fast, highly recoverable service.	Recoverability by definition in paired region.	Need additional solution to cope with data corruption - sync copies will just copy corruption.
Resilience	Always on solution means that every component is replicated and always available - may reduce cost by not duplicating within region.	May require switch over to alt region.	Loss of a region will affect resilience; doesn't solve corruption issue.
Data Corruption	Small replication delays may help address corruption risks.	Replication delays means data loss and higher RPO.	Needs careful tuning to mitigate corruption and avoid data loss.

Regions	Single vendor may make replication and switching easier.	Vendor errors may affect ALL regions - DR will not help.	Consider multi-vendor solution - more complex, possibly higher cost.

Cost is a downside as two full systems need to be paid for - but both could be used as applications can be configured to be stateless

System is highly recoverable as both run identically

Major issues

- Data corruption as both sites loaded synchronously
- Vendor errors may be replicated to multiple sites