Checklist to do:

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:
    a. The selection of quantitative risk modelling approach(es) with justification for the method chosen.
    b. Explanation of the calculations carried out, including detailed lists of assumptions and sources of data selected (where appropriate).
    c. 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. **(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%)**.

The plan is to complete each part over the next three weeks and so the goal for the week of the 3rd October is to come up with

- the list of risks for the supply chain of the company
- the selection of the risk method with justification of why this was selected
- explain the calculations used
- list the assumptions
- and justify the sources of data

In terms of the risk modelling then a tool called **Yasai** can be used, the advantage of this is that it has a good data set but the team needs to research the credibility of **Yasai** from a data perspective and which companies or universities use the data and where is it sourced from.

Risks that could hinder business continuity (to the supply chain of the company) as from (Rodriguez, 2019)

- Financial risks: Includes undesirable or unplanned changes in budgets thus leading to budget overruns, additional funding due to missed milestones, supplier's bankruptcy, etc.
- Scope of schedule risk: schedule changes due to reasons like natural disasters (hurricanes, fires, floods, etc.) or technological changes from the market.
- Legal risks: includes misuse of intellectual property, violation of laws and civil lawsuits, not meeting the regulations, standards or requirements included in the terms and conditions, etc.
- Environmental risk: it's important to know the negative impacts to the environment created by your supplier or contractor.
- Socio-political risk: is when the institution finds it difficult to adopt to regulatory environment changes due to new government, or new laws
- Project organization risk: lack of important people or equipment at the right place or time
- Human behaviour risk: project may be negatively affected because of an injury, illness, departure of a key personnel
- Reputation risk:
- Cybersecurity risk: today's supply chains are more vulnerable due to the multiple layers (foreign manufacturers, importers, third-party logistics companies, agents, transport companies, international end consumers, etc.), that cyber attackers can target. Attackers could cause damages just from unauthorized access to

sensitive information, DoS, etc. BYOD been one of the leading ways the attackers infiltrate the systems. (Rauniyar, et al., 2022)

- Information risk: includes unauthorized access to information thus resulting to a significant disruption and damages (Rauniyar, et al., 2022)

The table below is derived from (Rauniyar, et al., 2022), (Rodriguez, 2019) and (Anon, N.D.)

Risks	**Associated Potential issues**	**Probability of it happening**	**Solutions**
Financial	• Budget overruns • Additional funding due to missed milestones • Bankruptcy • Incomplete project • Reputation damage		•
Scope of schedule	• Change of schedules		•
Legal	• Misuse of intellectual property, • Violation of laws		• Having insurance covers like cybersecurity insurance cover, etc.

	• Civil lawsuits and fines • Not meeting the regulations, standards or requirements included in the terms and conditions,		• Regular verification and monitoring of insurance coverage. • Transparency •
Environmental	•		•
Socio-political	• Corruption • Ethics • Issues of trust, • Bureaucracy		•
Project organization	•		•
Human behaviour	• Data breaches • Change of schedules • Negative impact on the budget, project/business continuity		• Employing enough and highly skilled human resources. • Employee training in efficiency, cybersecurity, etc.
Reputation	• Loss in demand		• Transparency

	• Loss in investment and morale		
Cybersecurity	• Reputation damage • Hacking of BYOD and IoT • Denial of Service attacks • Malware and virus infesting the system(s) and end user devices • Software security vulnerabilities in supply chain management • Counterfeit hardware		• Authentication and authorization • Monitoring Security requirements of everyone included i.e., vendors, suppliers, end-users, management, etc. • Enabling Access controls •
Information	• Data breaches • Lawsuits and Fines • Reputation damage • Bankruptcy • Third party data banks		• Monitor Information security practices of end user including the suppliers • Authentication and Authorization • Encryption of data

			• Include policies and regulations e.g., GDPR

Top 10 free and commercial risk assessment and risk management tools in the market.

https://www.softwaretestinghelp.com/risk-management-tools/

References

Anon, N.D.. *Best Practices in Cyber Supply Chain Risk Management.* [Online]
Available at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
[Accessed 17 October 2022].

Rauniyar, K. et al., 2022. Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology. *Industrial Management & Data Systems.*

Rodriguez, D., 2019. *7 Basic Types of Supply Chain Risks.* [Online]
Available at: https://precoro.com/blog/7-basic-types-of-supply-chain-risks/
[Accessed 5 October 2022].