**GROUP – 03**

**Assessment Part 2:**

# Development Team Project: Executive Summary

**Module Name - Security and Risk Management March 2023**

**Word Count - 1994**

1. **Quantitative risk modelling approach:**

Expected monetary value (EMV) risk analysis: This is the simplest form of quantitative risk analysis. An EMV analysis is one of two techniques used in quantitative risk analysis. This statistical concept considers all probable future outcomes to calculate the average outcome (Tuomas, 2022) . In an EMV analysis, all we need is the expected cost of a risk we face and the probability of that risk occurring. We often set these values through a combination of analyzing data, consulting with experts, and estimating from experience. By multiplying the cost of each risk by its probability and adding up all the resulting numbers, we generate an overall projected risk amount for the project.

2. **Internal supply chain risks include risk events caused by** (Shahram, et al., 2013)**:**

A. Disruptions of internal operations.

B. Price Increases: Rising prices are caused by changes in supply or demand, currency instability, and customs tariffs.

C. Shortages: These can arise from lacking a component, material, or part needed to produce a finished product.

D. Supplier Relationships

E. Quality Failures: Quality failures occur when shipments of certain parts do not meet the specifications.

F. Delivery Failures: Carrier and logistical issues can result in late deliveries, damaged packages, or lost shipments.

G. Supply Shocks: Sudden worldwide or industry-wide drop in supply.

H. The calculation is done using the formula:

**Expected Monetary Value (EMV) = Probability * Impact** (Wagner & Shiraji , 2019)

Where:

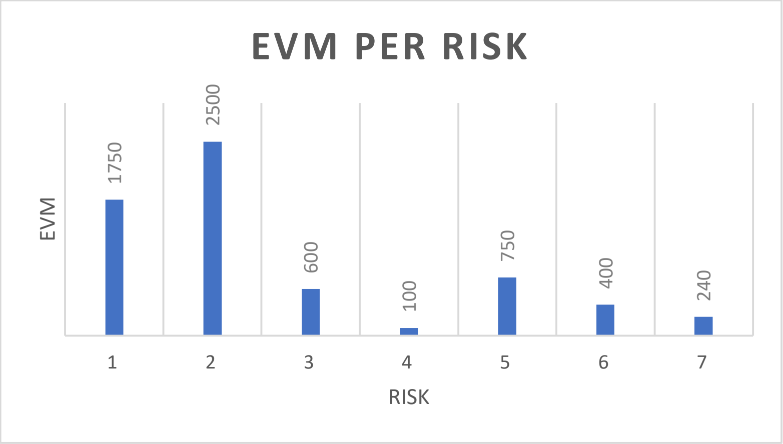
**Impact:** the impact is the amount you will spend if a given identified risk occurs.

**Probability**: probability is the likelihood that any event will occur.

The following table performs the calculation needed using data from similar supply chain risk.

| Id | Risk | Probability | Impact ($) | EVM ($) |
|---|---|---|---|---|
| **1** | Disruptions of internal operations | 35% | 5000 | 1750 |
| **2** | Price Increases | 25% | 10000 | 2500 |
| **3** | Shortages | 20% | 3000 | 600 |
| **4** | Supplier Relationships | 5% | 2000 | 100 |
| **5** | Quality failure | 15% | 5000 | 750 |
| **6** | Delivery Failures | 10% | 4000 | 400 |
| **7** | Supply Shocks | 8% | 3000 | 240 |

3. The quantitative risk analysis resulted in the the following list of risk as shown by the following graph.



Which shows that four risks were of EVM above 500$. These risks need immediate mitigations which are:

- Disruptions of internal operations
- Price Increases
- Shortages
- Quality failure

## Summary of the results and recommendations

EMV can be used to estimate a loss or a gain due to an event. From the above analysis, EMV value from different risks can be seen, which shows the potential loss due to a certain risk if it occurs. Below are the details of the risks with the EMV of above 500$ and some recommendations.

1. Disruptions of internal operations: Disruption of internal operations has the highest probability (35 %) due to many factors; it can be caused by several factors including cyber-attacks, human errors, system failure or a natural disaster which can put significant impact of the quality loss of the business. This risk requires immediate mitigation to cause further loss in quality. There are a few steps that can help to overcome the loss from these risks. **(N, Micheline & C, Nigel., 2017)**
    A. Risk identification: It is crucial to identify the type of risk in the first step to reduce the impact.
    B. Risk assessment: After the identification of the risk, evaluate them based on occurrence (Probability) and harm.
    C. Risk measurement and mitigation: By transferring risk to a different organization such as insurance or cybersecurity companies.
    D. Monitoring and Reporting: monitor the risks and check whether they are being controlled and report them on a regular basis.

2. Price Increases: Price increase (25% probability) depends on multiple factors including material supply, demand, and availability. On time decision can minimize the

loss, it can be controlled by various strategies, including **(S-B, Tanya & C, Derek., 2015)**

A. Value based pricing: Putting prices on goods based on the customer demand and value in market.
B. Penetrating price strategy: the selling price for goods at the start is lower than the market and increases with the passage of time by attracting more customers.
C. Price skimming: setting high price for a new product and lowering the price with the passage of time as competition grows.

3. Shortages: Shortages (20% probability) is referred to having a limited number of resources including labor, material, energy, and capital **(D, Ivanov & A, Dolgui., 2022)**. It is crucial to have knowledge about what is going on around the world and its impact on businesses. There are few recommendations to mitigate this risk and its loss:

A. Supplier data analysis: it is important to know what is happening at the supplier's end such as their management, performance, and relationship management with other businesses as it can interrupt the supply chain.
B. Links with different suppliers: It is important to not rely on only one supplier because if something wrong goes on their side, it can affect the full supply chain. Having links/relations with multiple suppliers is important.

4. Quality failure: Quality failure (15% probability) refers to not meeting the required specifications for a certain product. It can be either not fulfilling the consumer's requirements or exceeding the requirements. Quality control is a core factor in any

business because the consumer only wants that product to be perfect. Below are some recommendations **(A, Kumar. N, Suresh., 2008):**

A. Standardised system: There are some standardised systems to be followed to maintain the quality and minimize quality failure, for example ISO certifications (Such as ISO 9000). Some businesses are required to have ISO compliance.

B. Total quality management: Total quality management puts efforts to ensure customer loyalty by making on demand products. It highly focuses on quality control to fulfil consumer's requirement.

C. Continuous quality improvement: CQI focuses on continuous improvement in quality. The Plan-Do-check-Act (PDCA) is one of the most popular CQI models.

All quality management systems have key elements including quality policy, quality objectives, customer satisfaction and data management.

## Business continuity/ disaster recovery (DR) strategy

Business continuity and disaster recovery (BCDR) is a collection of procedures and tools that enables a business to recover from a disaster and continue regular business operations. Data recovery, reducing the impact of an interruption on business operations, and fast recovery to normality following a disaster are the three main objectives of BCDR planning (Marget, 2023).

Two important metrics in disaster recovery and business continuity planning are recovery time objective (RTO) and recovery point objective (RPO). RPO specifies the point in time to which the business will restore their data after a disaster, and RTO specifies the amount of time it should take to restore all applications and systems following a disruption. It specifies how much data a company can afford to lose before it has an impact on productivity and revenue and sets a limit on how far they may roll back their recovery (Mesevage, 2022). In this scenario, it is maximum 1 minute. DR solutions often cost more to operate the smaller RTO and RPO values are.

Reduced RPO and RTO are the major targets of a BCDR plan. Although there are numerous cloud computing services available, Disaster Recovery as a Service (DRaaS) can be selected as the most suitable for this company's DR. In comparison to standard disaster recovery solutions, this is primarily a low-cost solution. This business should consider using this solution as DRaaS can instantly recover from any disaster with a minimum of user intervention and is adaptable in copying data digitally or physically (Hamadah and Aqel, 2019).

On the other side, DRaaS relieves the company of the responsibility of disaster planning and places it in the hands of disaster recovery specialists. Compared to hosting our own disaster recovery system in a remote place with an IT team on call in case of emergency, this is inexpensive. This can save the company money by removing the need to set up and maintain a dedicated off-site disaster recovery infrastructure. However, business should examine and understand service level agreements. For example, what happens to recovery times if a huge natural disaster affects both the company and the provider simultaneously (VMware, 2022).

DRaaS works by duplicating and hosting servers at a third-party vendor's facilities rather than at the actual location of the company that owns the workload. In the event of a disaster that shuts down the main site, the disaster recovery plan is put into practice at the third-party vendor's facilities. The company can purchase DRaaS plans either as regular subscription models or a pay-per-use models that enables them to pay only when a disaster happens. The ideal choice for this business is *Managed DRaaS*, where a third party undertakes all responsibility for disaster recovery, as this company lacks the expertise to run its own disaster recovery. To keep updated on all changes to the infrastructure and applications, the company must maintain constant contact with its DRaaS provider (VMware, 2022).

Business requires disaster recovery platforms and hosts to safeguard their data, apps, and systems in the case of a disruptive situation. To guarantee business continuity and reduce downtime, these platforms and hosters provide a variety of services and solutions.

Even though there are several Cloud Platforms available like Amazon Web Service and Google Cloud Platform, we can suggest the Microsoft Azure Cloud-based disaster recovery model, because of its extremely popularity among businesses due to its high availability storage, networking and file synchronization, automatic data replication as well as automated backup and recovery features. Regardless of the ecosystem's scope, complexity, and differences among physical locations, this company can integrate it into their architectural design. The Azure Cloud Disaster Recovery plan provides outstanding safety and high compatibility in terms of key management and data protection (Cloud4C, n.d.).

The backup site or DR site, which will be utilized for data storage and quick recovery in the event of a disaster, is another important part of a BCDR plan. According to Ms. O'dour's requirements, Hot site is the finest choice for this company.

It is an exact duplicate of the primary business location. A hot site can execute near real-time backup or replication of crucial data since it has all the required devices, software, and network access. It guarantees no data loss and minimum downtime. It is assumed that a hot site will operate continuously and without interruption to maintain data synchronization across the sites. However, among the three, a hot site is the most expensive choice. To lessen the likelihood that a hot site would be impacted by the same disaster as the primary site, it is essential to make sure that this sort of DR site is situated far away from the primary location (Reed, 2019).

In the context of BCDR, the term "vendor lock-in" describes a situation in which a business becomes extremely reliant on a single disaster recovery provider or platform, making it difficult to transfer to an alternative solution without paying a sizable expense, effort, or disruption. Several things, including unique technology, data formats, legal commitments, or integrated connections, might lead to vendor lock-in (Lopez, Moreno and Tous, 2019).

The following factors should be considered to reduce the dangers of vendor lock-in in disaster recovery,

A. selecting BCSR solutions that follow industry guidelines.
B. Not depending too heavily on unique technologies that restrict flexibility and make migration challenging.
C. Verify if the DR solution enables simple data migration and transfer between multiple platforms.
D. Thoroughly go over the terms and conditions of legal contracts, paying attention to the transferability, ownership, and exit clauses.
E. Create a long-term DR strategy that involves regular performance and requirement reviews of technology.

(Opara-Martins, Sahandi, Tian, 2014)

It is important to recall that, despite the difficulties vendor lock-in might cause, using a disaster recovery provider or platform is not always a wrong decision. To minimize the effects of vendor lock-in and make sure that the chosen solution is in line with the long-term objectives and demands of the business, it is important to thoroughly investigate the risks and take proactive measures.

## References

- Metsänen, T. (2022) *Application of decision tree analysis and expected monetary value technique in quantitative risk management : Evaluation of less risky investment strategy.*, *Osuva*.Available at: https://osuva.uwasa.fi/handle/10024/13879 (Accessed: 22 May 2023).
- Gilaninia, S., Ganjinia, H. and Mahdikhanmahaleh, B.A. (2013) *Difference between internal and external supply chain risks on its performance*. Available at: https://singaporeanjbem.com/pdfs/SG_VOL_1_(8)/2.pdf (Accessed: 22 May 2023).
- **Wagner, D. & Shiraji, K., 2019. Calculating project risk contingency Expected Monetary Value (EMV) vs Monte Carlo Analysis. Synergy**.

- Naude, M.J. and Chiweshe, N. (2017) *A proposed operational risk management framework for small and Medium Enterprises*, *South African Journal of Economic and Management Sciences*. Available at: https://sajems.org/index.php/sajems/article/view/1621/983 (Accessed: 22 May 2023).
- Sammut-Bonnici, T. and Channon, D. (2015) *(PDF) pricing strategy - researchgate*, *https://www.researchgate.net*. Available at: https://www.researchgate.net/publication/272352932_Pricing_Strategy (Accessed: 22 May 2023).
- Ivanov, D. and Dolgui, A. (2022) *Full article: The shortage economy and its implications for supply ...*, *https://www.tandfonline.com*. Available at: https://www.tandfonline.com/doi/full/10.1080/00207543.2022.2118889 (Accessed: 22 May 2023).
- Kumar, S. and Suresh, N. (2009) *Operations Management* , *DSpace at VPM's V. N. Bedekar Institute of Management Studies: Home*. Available at: http://dspace.vnbrims.org:13000/jspui/ (Accessed: 22 May 2023).
- Marget, A. (2023) *What is a business continuity plan and how can it improve business resilience?*, *Unitrends.com*. Available at: https://www.unitrends.com/blog/business-continuity-plan (Accessed: 22 May 2023).

- Hamadah, S. and Aqel, D. (2019) *Proposed virtual private cloud-based Disaster Recovery Strategy*, *https://www.researchgate.net*. Available at: https://www.researchgate.net/profile/Darah-Aqel/publication/333229207_A_Proposed_Virtual_Private_Cloud-Based_Disaster_Recovery_Strategy/links/5cee80f992851c53956fe5fa/A-Proposed-Virtual-Private-Cloud-Based-Disaster-Recovery-Strategy.pdf?origin=publication_detail (Accessed: 22 May 2023).
- VMware (2022). What is Disaster Recovery as a Service (DRaaS)? | VMware Glossary. [online] VMware. Available at:

https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas.html.

- Cloud4C. (n.d.). *Azure Disaster Recovery | Azure DR & BCP*. [online] Available at: https://www.cloud4c.com/azure-cloud-services/azure-draas#:~:text=Azure%20Disaster%20Recovery%20as%20a [Accessed 21 May 2023].
- Mesevage, T.G. (2022) *The importance of RPO and RTO*, *Datto Backup Solutions Provider*. Available at: https://www.datto.com/uk/blog/the-importance-of-rpo-and-rto (Accessed: 22 May 2023).
- Cloud4C. (n.d.). *Azure Disaster Recovery | Azure DR & BCP*. [online] Available at: https://www.cloud4c.com/azure-cloud-services/azure-draas#:~:text=Azure%20Disaster%20Recovery%20as%20a [Accessed 21 May 2023].
- VMware (2022). What is Disaster Recovery as a Service (DRaaS)? | VMware Glossary. [online] VMware. Available at: https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas.html.
- Reed, J. (2019). Comparison Of Disaster Recovery Sites: Which one to Choose? [online] Nakivo. Available at: https://www.nakivo.com/blog/overview-disaster-recovery-sites/.
- **Lopez, J., Moreno, V. and Tous, R. (2019). Vendor lock-in in cloud computing: A comprehensive literature review. Journal of Systems and Software, 157, p.110401.**
- 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*, *SpringerOpen*. Available at: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z (Accessed: 22 May 2023).