

## Everyone's Smart University

### Project (Spring 2021)

|              |                             |               |
|--------------|-----------------------------|---------------|
| Student Name | Mohammed Naser Akram Alsati | اسم الطالب    |
| Students I.D | 2021200588                  | الرقم الجامعي |

|                                 |                            |             |
|---------------------------------|----------------------------|-------------|
| Section                         | Date                       | Course Code |
| Master of Project<br>Management | Thursday<br>11 / 05 / 2021 | (PMG510)    |

## Project Risk Management

---

### Project:

#### **Risk Identification and Analysis (Based on the project you chose in APM)**

The objective of this report is to identify project risks, prepare a risk probability matrix, and carry out an analysis of selected risks. Referring to the project you select in **Advanced projects management APM course**, your task is to prepare a risk management plan that identifies potential risks in **the selected stage of the project** and identify risk management strategies.

From the course content and readings, you know that the overall purpose of risk planning is to anticipate possible risk events and be ready to take appropriate action when risk events occur—to eliminate or reduce negative impacts on the project.

You may wish to begin this exercise with a brainstorming about potential risks to get candidate risks “on the table” for consideration. And then identify and refine that wording for risks that have some realistic chance of occurring in this stage. For example, potential weather problems present a real obstacle to completing field data collection by the planned completion date. It is also an issue that the project manager will ultimately have to plan for, as opposed to other issues such as a major disaster (e.g., your office burning down), is not a high-enough probability event that requires much time in planning. As described below, you will select several of the identified risks and carry out a risk analysis.

You will use the distilled list of risks to make a risk probability/impact matrix. The matrix will have at least three categories (high/medium/low) for probability and impact.

Remember that it is important to name risks effectively—use words that describe the risk event and point to the impact on the project (e.g., “injury of field technician disrupts data installation work”).

After completion of the risk matrix, document a risk analysis for the selected risks. This detailed documentation for that selected risk will include:

- a description of the risk and potential impacts (schedule, quality of work, cost, etc.) on the project.
- indicators or triggers that would be monitored to help identify the risk as early as possible.
- specific risk response strategies to take.

Using probability and impact matrix calculate the **Expected Monetary Value (EMV)** for all risks that have the impact in terms of cost \$\$.

## The Answer:

### Background:

It has been seen that there are different types of investment risks, regulation risks, operational risks, and cash management risks, which tend to increase the overall risks for the organization's cyber security system. The business is rising, and it is constantly investing to improve its role and credibility, according to the advanced project management assignment. The company's stock price is high, which attracts more buyers. Different aspects of the company are considered when making financial decisions. It has contributed to the company's increased market value and position. It is expected that the company will achieve the best IT infrastructure in the future, and this will help in improving the overall market position.

### Project Risks:

The three external factors that might affect success of an effective cyber security system are negative work habits, lack of education and skills, and self-control. Gender equity and performance evaluation is a major challenge across all of the departments. Also, if the organization desired to learn more, most of the international institutions do not provide specialization opportunity to the next level. Further, careers like marketing manager or event planner may require pursue a range of confidential data of the corporation.

During daily activities of the organization, risks will also raise in the area of ethical principles from following laws and moral standards. It needs to learn business ethics and as a marketing communication strategist, the team will contribute to positive development of people, spread constructive knowledge, avoid misconduct (follow legal and ethical advertising practices), establish trust, discard discrimination, and ensure privacy and confidentiality (Sweeting, 2017). The organization must try to deliver the best quality knowledge to its people.

There is a lack of communication of decisions from the top management to the bottom level employees of the company. There is a possibility of applying the chosen structure through the company's five divisions, from preparation to procurement, production, delivery, and return. The management tool must specify business rules, as well as ensure performance, data collection, and efficient resource utilization (Price et al., 2017). Furthermore, the system is unable to determine whether to build and construct facilities, as well as the organization's contract execution, regulatory enforcement, and risk management.

When the data security architecture is applied to an enterprise, the model offers a "ordinary" approach to address a variety of information management issues. It can, for example, introduce gaps or errors during the manufacturing process while also improving product and service reliability. As a result, customer satisfaction with the company's goods decreases.

### Risk Probability Matrix:

The Risk Probability Matrix is presented below,

| Threat                                                               | Vulnerability                                                                  | Asset                      | Impact                                                                                                                                | Likelihood                                                                         | Risk                                                     | EMV                | Improvement Recommendations                           |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------|-------------------------------------------------------|
| System failure –<br>Particularly during rush hours<br><b>High</b>    | The current cyber security system is ten years old.<br><b>High</b>             | Servers<br><b>Critical</b> | Security threat to all services (official corporate website, social media pages, customers data, employee records)<br><b>Critical</b> | Current number of errors in a single department is around 5 per day<br><b>High</b> | Potential loss of \$5000 per occurrence<br><b>High</b>   | $1 \times 5 = \$5$ | Install a new cyber security system cost \$3000 cost. |
| Malicious disruption from human capital (DDOS attack)<br><b>High</b> | Firewall is configured efficiently and has good DDOS mitigation.<br><b>Low</b> | Website<br><b>Critical</b> | The official corporate website shows malfunction, unusual posts on social media pages.<br><b>Critical</b>                             | DDOS was renewed on every first month of year.<br><b>Medium</b>                    | Potential loss of \$3000 per occurrence<br><b>Medium</b> | $2 \times 3 = \$6$ | Monitor the progress of current system                |

It has been found that small number of people of the company (top management and bottom level) is influenced by the cyber security system. It is also noted that the effect on the current system is because of the technological risk buffer as used to forested extent of awareness top-bottom, which is 250 people in the company. The risk assessment shows that the current level of the company is vulnerable to the cyber security system in the forested departments like sales and marketing. Provided that the department is currently surrounded with the current development and radiant exposure by the cyber security with the adjacent department can be mitigated through the clearing and development which occurs among the departments and the site from other buildings. The riskiest time of an individual's employment could also be a good opportunity for a firm, i.e. hiring and parting ways. underlying are a few of the areas where one can see organizations exposing themselves to risk when recruiting new employees, while avail good chances to get success.

#### Analysis of Selected Risks:

A variety of Information Technology (IT) cyber security systems will help the business achieve its aim of flourishing in the sector in the future. The business can access and monitor information from logistics and shipping, transportation, and delivery by using technology throughout the industry. The data will be altered without the need for manual intervention. The organisation is advised to use the technology to provide a decentralized data structure framework. All accounting details will become accessible for the responsible individuals in each department, according to Haywood et al. (2017).

The three risk mitigation strategies are getting more knowledge and experience from strengthen collaborative relations, working hard, and practice problem-solving tactics. It would provide manuals and talk to more people to improve the system in future. A system failure that the company has experienced in life was lack of focus on the technology. It is learnt the lesson about mess of the system, including personal relationships with stakeholders and professional success of each. In future, the

company needs to work hard to get good achievements as well as the desired job position in the reputed industry and the entire world.

#### References:

- Haywood et al., (2017). Contextualizing risk within enterprise risk management through the application of systems thinking. *Environment Systems and Decisions*, 37(2) 230-240.
- Price et al., (2017). Repeat prescribing of medications: A system-centered risk management model for primary care organizations. *Journal of evaluation in clinical practice*, 23(4) 779-796.
- Sweeting, P. (2017). *Financial enterprise risk management*. Cambridge University Press. UK.