ARDEN
UNIVERSITY

| |
|---|
| **Awarding Body:**<br>Arden university |
| **Programme Name:**<br>BUS7011D |
| **Module Name (and Part if applicable):**<br>Risk Management |
| **Assessment Title:**<br>Assignment: Part 1 |
| **Student Number:** |
| **Tutor Name:** |
| **Word Count:**<br>2500<br>Please refer to the Word Count Policy on your Module Page for guidance |

## Table of Contents

# INTRODUCTION

Risk management identifies, evaluates, and manages threats to an organisation's resources and profits. Financial uncertainty, legal liability, technological problems, strategic management mistakes, accidents, and natural disasters are a few potential causes of these risks. Effective risk management allows businesses to consider all the threats they encounter. Risk management also analyses potential threats affecting an organisation's long-term objectives (Ross, 2018).

Geetway Ltd. manages investments and other financial resources. Before Geetway became a management consulting firm in 2017, its risk team lacked visibility into and authority over the company's interconnected IT infrastructure. As part of its expansion strategy, the company abandoned its reliance on manual spreadsheets in favour of automated, scalable systems. Tim Moore, the Project Controls Manager of Geetway, said, "a new parent body organisation acquiring control of Geetway in 2018 was the chance for transformation." Until then, risk management was a company's afterthought, not a core competency. They wanted the organisation to demonstrate the benefit of our risk procedures for the new scalability; therefore, they requested a more holistic approach, a broader point of view, as well as tools from the field of Risk Management.

# TASK 1 – ANALYSING RISK MANAGEMENT'S CENTRAL IDEAS AND PRECEPTS

In order to prevent the data breach, management at Geetway Ltd should have assessed the potential threats by using a predetermined standard or framework. The following are some ground rules that might be implemented.

## *The Organizational Setting*

As a result of not considering these elements, the organisation is more vulnerable to the dangers they pose (Lee, 2021). These include political considerations, legal factors, technological factors, social aspects, etc. It is safe to presume that Geetway Ltd.'s data breach and the subsequent exposure of sensitive patient information were caused by a failure to account for technological considerations adequately. Talented Risk Management would have bolstered the company and made its operations stronger.

### *Stakeholder Participation*

The decision-making process is the most crucial stage of any business, as it is there that the long-term objectives of the company are decided upon, and the strategies and policies to attain those objectives are developed (Force, 2018). Geetway Ltd should have thought about everyone who would be affected by their data risks advice before making any recommendations.

### *Mission Statement of the Group*

Risk management at Geetway Ltd. should have been included in the company's goals, as those goals need to be accomplished in the end. If Geetway Ltd.'s goal is more crystallised, it will be easier to make an informed choice about whether or not to take certain risks, and the company will also have a clearer mental picture of its overall situation.

### *Reporting*

Geetway Ltd has probably overlooked the importance of management communication, even though it is crucial to the company's approach to risk. More open and obvious information should be used to verify its veracity and inform the choice. When people can share more knowledge, they have access to a broader perspective (Naude & Chiweshe, 2017).

### *Responsibility Assignments*

Geetway Ltd might have been put in a precarious position if it had neglected to detail the functions and duties of its human resources specialists in the risk management process and the decisions made at each level. Open communication and collaboration are critical components of effective risk management.

### *Assisting Framework*

The system in place emphasises the value of the risk management group. The Geetway Ltd. employee in charge of risk management should have been adaptable and quick to learn new information. All parties involved in the management lifecycle should know the potential for conflict at each step (Rane et al., 2019).

### *Potential Danger Signs*

Each member of Geetway Ltd should be given the responsibility and authority to monitor and respond to the earliest indicators that the risk is becoming a severe issue. Early warning indications may be monitored thanks to constant contact between all parties involved.

### *Review Methods*

Especially in the realm of information technology, where breakthroughs are reaching for the stars and hackers are constantly on the prowl for an easy target, it is essential to keep up with the times (Kure & Islam., 2019). Geetway Ltd needs a mechanism to ensure that its policies are regularly reviewed and updated as necessary in light of new data and technological advances.

### *Culture of Encouragement*

If the top brass makes all decisions at Geetway Ltd, and there is no culture of questioning or addressing the topics, then occurrences like these are likely to occur because individuals are more likely to step up and talk about issues when they feel safe doing so, and when they are part of a culture that encourages that.

### *Enhancements That Never Stop*

Due to a variety of causes, time inevitably creates a chasm. However, Geetway Ltd management should have studied a plethora of developments in IT and amended their rules to prevent such situations. Timely and appropriate responses might strengthen the system and make it more reliable (Suprin et al., 2019).

# TASK 2 – ADVICE TO BOARD AND CEO

While Geetway Ltd is understandably anxious about expanding its market share and winning over new customers, it would be wise for the company to invest in top-notch risk management, particularly in the area of information technology risk management, in order to head off similar mishaps in the future and keep its clientele trusting it (Firmenich, 2017). The following are factors that should be taken into account while creating risk management plans:

## ENTERPRISE RISK MANAGEMENT (ERM)

Enterprise risk management (ERM) is a strategic business approach focused on planning to recognise, evaluate, and mitigate the risks associated with any threats to an organisation's ability to carry out its mission. However, Enterprise Risk Management (ERM) does not come with a cookie-cutter template that can be applied to every company and is expected to be a perfect fit for their unique structure and set of needs (Hopkin, 2018). In order to make informed decisions, Geetway Ltd's management must first conduct a risk assessment. This analysis must consider the threats both internal and external elements pose.

A cross-section of the organisation, including Finance, Human Resources, Information Technology, etc., should be consulted and asked, "What do they see about the largest risk to the firm, both now and in the future?" As well as the most manageable danger. Following a thorough analysis of potential threats, this data may be utilised to shape strategy. In-depth familiarity with the exposure o potential dangers that might affect the business would be used to establish the company's risk appetite and risk tolerance. In other words, a company's risk appetite is the level of uncertainty it is willing to take on (Greuning & Brajovic-Bratanovic., 2022). When applied to organisations, risk tolerance may be considered the degree to which leaders are willing to tolerate shifts in the organisation's stated goals. Geetway Ltd.'s success hinged on identifying and implementing the optimal degree of maturity for the company.

## DISTINCTIONS BETWEEN STRATEGIC AND OPERATIONAL DANGERS

### *Dangers Associated with Daily Operations*

Cyber hazards to operations include possible disruptions and diversions that might result in a loss. Cybersecurity officials are doing their utmost to deal with the influx of such incidents over the previous few years. Cyber risk in operations can be caused by several factors, including outdated systems, careless employees, inefficient software, and even criminal activity (Husin et al., 2019).

### *Exposure to Potential Danger in a Strategic Position*

Although an assault on an IT company is unlikely to compromise its most sensitive information, it might compromise other, less obvious, strategic assets, such as trade secrets or an edge in the market. The highest levels of management at many companies take the issue of cybercrime very seriously and are working to improve their strategic risk management skills. It is easy to say but challenging to do in practice (Ross, 2018). Geetway Ltd. is just one of many companies that have yet to grasp the gravity of the threat posed by cybercrime entirely. Both of these categories apply to strategic risk.

### ***Threat to an Organization***

The board's decision on the company's service and product offerings may pose a threat. There is always the chance that something will go wrong while creating and promoting a product, whether it be a change in the product's cost or the economy or a shift in the market's perception of the product's worth due to technical advancements.

### ***External Threats***

A threat has nothing to do with the service or commodity being provided. Possible explanation: making use of capital set aside for the long haul. Risk can be affected not just by decisions made by the board of directors but also by the actions of the organization's rivals (Lee, 2021). Then, the manufacturing process could take on new costs due to rivals' technological advancements, driving up production costs.

## THE GEETWAY LTD.'S UNIQUE STRATEGIC THREATS

Geetway Ltd has the following strategic risks as a result of the recent incident:

### *Reputational Danger*

Following the data breach and the subsequent unlawful access to customer email accounts, Geetway Ltd's reputation took a severe hit.

### *The Dangers of Technology*

Using outdated equipment increases the risk of a data breach since cybercriminals actively seek out vulnerable systems built using obsolete technologies (Force, 2018).

### *Legal Exposure*

Geetway Ltd has, in a sense, failed to fulfil its obligation to its customers (patients) by adequately protecting their personal information and confidentiality.

### *Probability of Inadequate Protection*

The security risk threatens the company's IP, integrity, brand positioning, consumer confidence, and reputation.

### *Potential Danger from Noncompliance*

There is a chance that Geetway Ltd will violate the rules and regulations set out to protect the personal information stored in their system (Naude & Chiweshe, 2017).

## A DISCUSSION ON THE ROLE OF TECHNOLOGY IN RISK MITIGATION

Risk management, which relies heavily on data, has also felt that the effects of IT are pervasive. From initial risk assessment to ongoing monitoring, IT is a crucial enabler of effective risk management at every stage. Risk management relies heavily on cutting-edge tools like enterprise resource planning (ERP), analytics, risk management, and governance and compliance systems (Rane et al., 2019). Those in management positions or those looking to make changes from the outside should make use of cutting-edge technologies. Better management may be achieved by carrying out the following actions, reducing the risks involved.

- Basic risk visualization programs
- Social Media
- Analytics and Data Integration
- Data Mining
- Cloud Computing
- The Internet of Things
- Digital Image processing
- Cybersecurity
- Artificial Intelligence

# TASK 3 – GUIDELINES AND MODELS FOR RISK ASSESSMENTAND MANAGEMENT

Geetway Ltd. suffered a devastating data breach and cybercrime attack due to inadequately managing the company's exposure to risk regarding the confidentiality, integrity, and availability of its data. In the company's pursuit of expanding its market share, Geetway's management temporarily overlooked the importance of strengthening its risk management practices (Kure & Islam., 2019). Now is the moment to implement globally accepted standards and frameworks that most businesses have embraced. Geetway Ltd may ramp up its risk-reduction efforts by adhering to specific standards and frameworks. Common and newer guidelines for assessing the security of information technology include;

- Guidelines for Risk Analysis and Management from The National Institute of Standards and Technology (NIST).
- ISO270005
- The ISACA Risk IT framework

Using the NIST Risk Management Framework (RMF) will allow Geetway Ltd. to have a more appropriate and detail-oriented framework to work within. There is not much difference in approach between the various frameworks; nonetheless, the NIST-developed framework is being outlined for Geetway Ltd (Suprin et al., 2019). Geetway Ltd. will adhere to the NIST framework (which entails the following procedures).

## FIRST STEP – PREPARE

When managing system security and privacy threats, Geetway Ltd must determine how much security is essential for the company. Geetway Ltd must assess its current capabilities and learn to appreciate the gravity of security threats. Things to do in advance might include;

- For the risk management process at Geetway Ltd, it is necessary to delegate responsibilities and establish roles.
- The willingness and ability to accept risk as part of a calculated plan are essential.
- The purpose, business processes, and operations of the desired supporting information system must be specified.

- It is essential to determine which assets, particularly information assets, are crucial to safeguard and prioritise their protection accordingly (Firmenich, 2017).
- Geetway Ltd. is responsible for conducting the risk assessment at the system level.

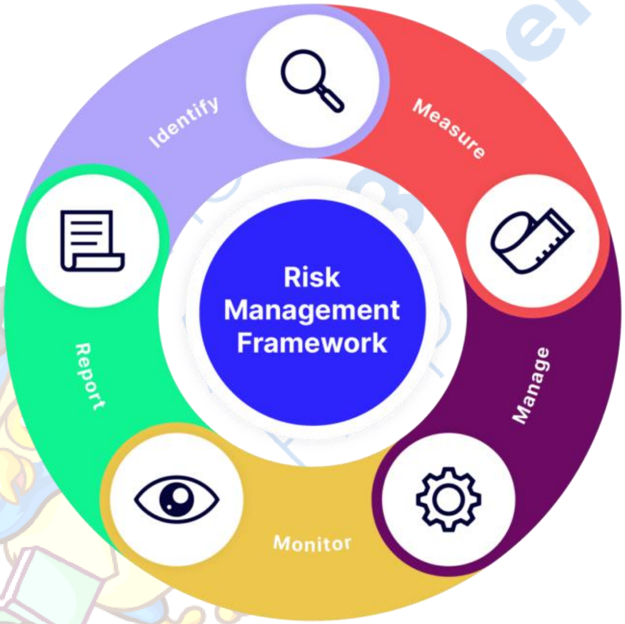

*Figure 1: Risk Management Framework (Source: https://www.hicx.com/wp-content/uploads/2021/06/risk-management-framework-hicx-e1623348888660.png)*

## SECOND STEP – IDENTIFY THE TYPES OF THE SYSTEM

The system's management must classify the system according to its security and level of security, bearing in mind the system's goal and aim. The system will do a practical analysis and use the results to influence its processing, storage, and transmission of data. To provide quality patient care, Geetway Ltd providers must classify their system according to the data they collect about their patients and maintain it in their databases (Ross, 2018). They have to choose a level of safety before proceeding, which data will be transmitted via which channel, who will be responsible for processing it, and what steps will be taken in the database to do so.

# THIRD STEP – CHOOSE THE ROLE OF CONTROL

The security control process's management is mainly in charge of deciding on and approving the chosen method. Software, hardware, and other technical modifications or ramifications can all be used as part of a security control system's risk management process to meet requirements and provide a robust security control environment. Organizations should draw up plans for keeping tabs on the effectiveness of their new security measures (Husin et al., 2019). In order to ensure the safety of patient data and prevent future data breaches, Geetway Ltd must invest in the best possible infrastructure, software, technical support, and employees for handling these responsibilities. The following is a list of the essentials for putting in place.

## *Software's*

The SAS framework is only one example of several available options for IT risk management. The following SAS software packages will be set up:

- Base SAS 9.4
- SAS Integration Technologies 9.4
- SAS LASR Analytic Server Access Tools 2.82
- SAS Office Analytics 7.4
- SAS Risk Governance Framework Server Configuration 7.4
- SAS Web Infrastructure Data Base JDBC Drivers 9.41
- SAS/ACCESS Interface to ODBC 9.4
- SAS/ACCESS Interface to PC Files 9.4
- SAS/CONNECT 9.4
- SAS/ETS 15.1

## *Hardware's*

The following hardware upgrades are needed in the system to apply updates, per the SAS website:

- Disk Space Consumed by Installed Products: 1067 MB
- Two SAS/ACCESS Engines and three SAS Metadata Bridges are included in the SAS Risk Governance Framework Server.

### *Back-Up Tech*

Companies that distribute software typically have a team of technical support staff available to customers. Basic instruction can be provided to some members of the respective organisations (Greuning & Brajovic-Bratanovic., 2022).

## FOURTH STEP – REVIEW EXISTING SAFETY MEASURES

An external auditor will evaluate the effectiveness of a company's planned security measures. In reality, an evaluator will identify problem areas and provide suggestions to improve the system. Following the implementation of those suggestions, a security plan may be improved. Due to a significant data breach or cybercrime assault, Geetway Ltd now needs a more robust and effective security strategy. So, it is best to have an impartial third party examine the security measures taken by Geetway Ltd's leadership, and that is why independent assessors are so important.

## FIFTH STEP – DATA AUTHORIZATION AND MANAGEMENT

The company must provide a risk assessment and valuation suite of endorsements. Once the mediator agrees on a course of action, they notify all involved parties of their decision (Hopkin, 2018). The Geetway Ltd. assessor will approve the system and report its value. The most appropriate and effective system of controls will be authorised by management. Finally, the method and rules for safeguarding the database will be implemented.

## SIXTH STEP – PROTECTIVE MEASURES SUPERVISION

The existing security control system is subject to constant monitoring by an external agency. Considering the necessary system adjustments, that business will also upgrade the security control system. Maintaining a high standard of safety through routine reporting and adjustments. Geetway Ltd must assemble a group of experts to oversee the system's operation and make any necessary upgrades (Firmenich, 2017). The Risk Framework operates in a repetitive loop. Geetway Ltd.'s management will be informed of any issues discovered by the monitoring teams, and they will then take the appropriate steps to address the issue and further strengthen the control system and framework cycle. If an error or poor control is detected, management will be compelled to revaluate the entirety of the company's risk management process.

# CONCLUSION

In order to effectively identify and address possible hazards, businesses need to use a process known as risk management. The process of reducing the impact of a threat is straightforward when it has been recognised. Another benefit of risk management is that it provides a firm with a solid foundation to build good judgement (Lee, 2021). The best way for a company to be ready for anything that can slow down or stop its growth is for its leaders to evaluate and control the company's risks carefully. A company's chances of success increase when it considers possible risks' impact on its operations and creates measures to counteract them.

# REFERENCES

Firmenich, J., 2017. Customisable framework for project risk management. Construction Innovation.

Force, J.T., 2018. Risk management framework for information systems and organizations. NIST Special Publication, 800, p.37.

Greuning, H.V. and Brajovic-Bratanovic, S., 2022. Analyzing banking risk: a framework for assessing corporate governance and risk management.

Hopkin, P., 2018. Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Publishers.

Husin, W.S.W., Yahya, Y., Azmi, N.F.M., Sjarif, N.N.A., Chuprat, S. and Azmi, A., 2019. Risk management framework for distributed software team: A case study of telecommunication company. Procedia Computer Science, 161, pp.178-186.

Kure, H.I. and Islam, S., 2019. Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems: Theory & Applications, 4(4), pp.332-340.

Lee, I., 2021. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), pp.659-671.

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, 20(1), pp.1-10.

Rane, S.B., Potdar, P.R. and Rane, S., 2019. Development of Project Risk Management framework based on Industry 4.0 technologies. Benchmarking: An International Journal.

Ross, R.S., 2018. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.

Suprin, M., Chow, A., Pillwein, M., Rowe, J., Ryan, M., Rygiel-Zbikowska, B., Wilson, K.J. and Tomlin, I., 2019. Quality risk management framework: guidance for successful implementation of risk management in clinical development. Therapeutic innovation & regulatory science, 53(1), pp.36-44.