Importance of Risk Assessment

Hari Krishna Mora

University of the Cumberlands

Table of Contents

[Chapter -1: Importance of Risks Assessment 4](#_Toc46664252)

[Importance of Risk Assessment to the Organization 4](#_Toc46664253)

[**Infrastructure** 4](#_Toc46664254)

[**Movement** 5](#_Toc46664255)

[**Interpersonal Layer** 5](#_Toc46664256)

[As an e-commerce organization, it is crucial to building trust among members in the security department. This ensures that employees do not share crucial credentials to other parties since it can place the company at risk. 5](#_Toc46664257)

[**Individual Behavior** 5](#_Toc46664258)

[**Practice and Threats** 5](#_Toc46664259)

[Chapter -2: Administrative and Technical Recovery Plans 5](#_Toc46664260)

[Chapter -3: Crisis Management Plan 8](#_Toc46664261)

[Plan Testing 9](#_Toc46664262)

[Chapter 4: Business Continuity Planning Policy 11](#_Toc46664263)

[Assessment of Risk 11](#_Toc46664264)

[**Determine Impacts on Business Operations** 12](#_Toc46664265)

[**Establishment of the Business Continuity Plan** 12](#_Toc46664266)

[**Strategy and Plan Development** 12](#_Toc46664267)

[**Testing and Maintenance** 13](#_Toc46664268)

[Chapter 5: Information Security 13](#_Toc46664269)

[References 15](#_Toc46664270)

# 

# Chapter -1: Importance of Risks Assessment

The fictitious company is E-Express. An e-commerce institution sells commodities and services through the internet. This firm has been in operation for the past ten years and managed to stand on a competitive edge in the market place. Since data is transmitted through the internet, the company has employed a team of experts in IT security management to ensure that the servers are secure. Technological inventions have led to the storage of data through the cloud systems that are prone to a security breach from hackers. Therefore, the security department is keen to enhance a safe infrastructure that manages to counter malicious activities in the servers. E-Express deals with essential details for their customers. These entail personal details, physical address, phone contacts, and e—payment credentials. If they get into the wrong hands, it could have significant consequences for clients and the firm (Torabi, Giahi, & Sahebjamnia, 2016). Hackers might manage to access financial accounts and even engage in ransomware attacks.

# Importance of Risk Assessment to the Organization

Companies are faced with various risks as they engage in their operations. Therefore, organizational leaders need to be prepared to counter different forms of risks that threaten the overall operations. The threats could emanate from internal or external sources. For E-Express, the security breach's risk is the primary area of concern since most of its operations are through the internet. It is essential to consider how security could be handled while utilizing the five layers of risk in the docket of a security manager. These are highlighted below.

## **Infrastructure**

This layer is crucial for the institution. It entails the space in which information moves into and out of the company’s cloud system. Since the workforce has access to the servers, they should be trained on practical usage where they should be keen to observe any malicious links presented to the platform. The online and offline spaces are sources of risk that should be taken into consideration (Alali et al., 2018).

## **Movement**

Here, information is shared with various stakeholders. As it moves from one source to another, it could be breached. It is essential to sensitize the clients using strong passwords for their accounts so that it can be difficult for third parties to gain access to the servers.

## **Interpersonal Layer**

## As an e-commerce organization, it is crucial to building trust among members in the security department. This ensures that employees do not share crucial credentials to other parties since it can place the company at risk.

## **Individual Behavior**

This entails the equipment that employees can access. Besides, the skills incorporated in the system determine whether the firm is ready to counter security threats. The tools provided by the management are to enhance further protection, ensuring that they are up to date.

## **Practice and Threats**

The layer allows security personnel to identify a particular threat. The behaviors that make the threat escalate are analyzed so that a potential solution can be formulated (Shameli, Aghababaei, & Cheriet, 2016). After managing to counter the risk, the firm continues with its smooth operations.

# Chapter -2: Administrative and Technical Recovery Plans

During the week, I identified an organization that adopts various elements that allow business continuity to be guaranteed. The selected element was recovery plans that are used during disaster recovery. The recovery plan aims to enable the organization to be reinstated in its previous condition before the disaster took place. When developing or assembling such a project for administrative recovery, several steps must be followed.

The first process is the identification of the scope of the recovery plan. The scope determines what is to be covered in the plan at the organizational level. With the scope of the recovery plan, it becomes easy to estimate what resources and expertise are needed. Further, the organization cannot set goals if the project's scope is not identified. The established scope helps the project team to set goals and objectives and the time when they can be achieved. Therefore, the scope of the project act as a roadmap to the rest of the project as it controls the operations of the project team.

The second process is identifying the key business areas of the company. Doing this is crucial since it identifies the key interests that need to be protected by the plan being developed. The key areas in the company include financing, accounting, marketing, operations, and management. They are termed as the key areas because the organization cannot run without them. They are viewed as the spinal cord of the organization because they control and guide virtually everything in the company. Identifying the functional areas is important as it enables the company to design a way of ensuring these functions are continuing normally.

The third process is identifying critical functions. Critical functions are certain activities at the organizational level that cannot be postponed during a disaster. The critical functions include processes and activities that should be restored in case there is a disaster to safeguard the resources and assets, gratify regulations, and meet the company's needs. Further, critical functions may entail the group of operations usually performed by the unit, which must be continued within a month or less, after a disturbance in service. Therefore, the critical functions are important in the organization, and they must be restored as soon as possible to promote the normal running of the operations.

Critical activities need to be secured using contingency plans since they could lead to huge losses if canceled or postponed. Once this has been done, the business should determine the dependencies between the key business functions and business areas (Phillips, 2016). The process allows management to have a better idea of some of the processes that can be put in place to ensure that no disruptions are observed in the workplace. Besides, the crucial activities must be protected to reduce the time the company needs to go to normal operations after an incident.

The fifth process that should be undertaken is ascertaining the downtime of each critical function. The assessment is made to come up with solutions to address any disruptions that may take place in the future. The approximation of the downtime of every critical function provides the organization with an insight into what will be affected most (Phillips, 2016). Some critical functions are affected by an incident than others; this varies with the nature of the disaster. For instance, when the organization is experiencing a power outage, some critical functions are affected than others. The assessment of every critical function ensures that the organization is cognizant of a possible downtime and prepared accordingly.

The sixth and last process that should be included in the development of the recovery plan is actualizing the plan in line with the daily operations of the company. The alignment of the plan with the basic business is important as it ensures that the organizational departments work toward achieving the goals set in the project. Further, it creates a harmony that is important in ensuring the project team has a common goal (Torabi, Giahi & Sahebjamnia, 2016). When this plan is actualized, the employees and other players in the company can see it as a feasible or achievable project. Lastly, the final process is very critical to the success of the recovery plan. One mistake at this point could hinder the project from being successful.

In short, the process required in the administrative disaster recovery starts from establishing the scope of the project to actualizing the project by aligning it to the operations within the organization. The recovery plan is not as easy, and people think this is because of the downfalls that are involved in the process. Proper planning and ensuring that all the needed resources are available contributes to the success of the recovery plan.

# Chapter -3: Crisis Management Plan

Crisis management plan depicts the steps that the organization must follow in the time of emergency in order to restore the condition to normal. The primary goals of this plan include giving direction on communications, staffing, and minimizing risk (Jackson, 2018). The crisis management plan should encompass restoring the business activities to normal while alleviating some of the impacts of the crisis.

**Mitigation**

In the crisis management plan, mitigation encompasses all the activities that focus on alleviating the unavoidable effects of the crisis. These mitigation activities entail land use management and zoning, susceptibility assessment updates, and others (Jang, Kim & Shin, 2017). Reducing the impact of the disaster is important as it enables the organization to handle various matters pertaining to disaster and restore most business operations.

**Preparedness**

Preparedness is a pivotal step in disaster management because it ensures that the organization is well prepared to deal with the emergency (Jang, Kim & Shin, 2017). This step includes training the employees in order to equip them with the relevant skills needed in crisis management. The other important step is to introduce warning systems and assemble all the required resources. When the company is prepared for an emergency, it becomes easier to manage it.

**Response**

Response encompasses all the efforts of the organization to reduce the risks depicted by an organization. The activities carried out under the response are directed towards handling the actual risks. The goal of the response is to give prompt support to improve the morale of the impacted persons, improve health, and maintain life.

**Recovery**

In the course of controlling everything, the impacted persons have the ability to carry out activities purposed on restoring their normal living and the substructures that support them. Most of the events are aimed at restoring everything to normal. The recovery also focuses on restoring the business operations and ensuring that the critical infrastructure is operational.

# Plan Testing

Properly written and conducted test plans guarantee that all product or project elements are comprehensively covered and tested in disaster recovery of a continuity plan. A reliable test plan must contain all the requisite details of the testing scope, communication plan, test deliverables, products, or projects to be tested, features not tested, and elements to be tested. Additionally, in order to achieve the objectives of a test, other external aspects such as the test environment, schedules, roles and responsibilities, risks, and contingencies need to be considered. Test plans are essential because they enable planners to confront the challenges that await them and focus on critical topics. Moreover, adopting a test plan adds value, structure, and accountability to the question and answer cycle within a business continuity structure (Lindstedt, Armour, Noakes-Fry, 2017).

Below is an example test plan of disaster recovery and business continuity plan, outlining the necessary steps covered;

1. Formulate and exercise an eventuality plan that outlines a succession plan for senior management.
2. Have a backup of the trained workforce to perform emergency tasks. Full-time employees might not always be available.
3. Lay down crisis communication plans and determine offsite meeting venues for top management.
4. Invest in alternate communication means in case the primary channels break down, or are slow.
5. Involve all employees and senior management in the organizational exercises to accustom them to respond to emergencies.
6. Develop realistic business continuity exercises to accommodate employees' emotions to monitor their reactions in case situations become stressful.
7. Engage in partnerships with local emergency response firms such as police departments, firefighters, and local administration to establish a cohesive working relationship.
8. Evaluate the company's performance during each test. Work towards definite constant improvement.
9. Carry out checks of the continuity plan very regularly accommodate changes and embrace technology (Phillips, 2016).

Testing exercises need to be propagated holistically to guarantee all elements are well-thought through. By keeping all the benefits and drawbacks of using a test plan in mind, this paper has suggested adopting a modern test management tool to overwhelm the setbacks and hold back the benefits of embracing test plans in business continuity.

# Chapter 4: Business Continuity Planning Policy

Procedures and policies are an essential part of any organization because they tackle relevant issues like what entails best practices among the players or stakeholders during the disaster. Employing both procedures and policies in the course of decision-making, ensures that employees are constant in their decisions. With clearly stipulated procures, the workforce precisely comprehend team and individual responsibilities, thus saving resources and time. In the disaster preparation and management, procedures and policies ensure that the managers, supervisors, and employees work harmoniously towards a common goal (Järveläinen, 2016). This is important in ensuring the success of business continuity after the disaster.

Plan and procedures have an impact on the business continuity policy as they facilitate the effectiveness of such a project. They present a roadmap that outlines how various activities and operations should be completed during the business continuity plan. Furthermore, the procedures and policies affect how the organization manages and uses the available resources to facilitate the completion of various activities pertaining to the continuity of business operations.

## Assessment of Risk

The first step in the development of power in the business continuity policy is the risk assessment. This step involves assessing all the risks that surround the business and their probability of occurring. There are various risks that surround the organization; there are those who have a higher probability of occurring than others do. The organization must identify all the possible risks and group them according to their likelihood to occur. Along the same line, some risks have more effects on business operations than others do; this calls for the need for ranking them with their impacts on business operations.

## **Determine Impacts on Business Operations**

The second step is to create a business impact analysis, a strategic process that evaluates and determines the possible impacts of disruption of essential business operations because of an emergency. This is a crucial step because the company gains insights about the potential effects of an emergency on the business operations. This makes them prepare their customer for a disruption on services. Further, by identifying the business operations affected, the organization can devise a way of continuing them as soon as the disaster is over.

## **Establishment of the Business Continuity Plan**

The third step is establishing the business continuity plan, which stipulates how the business will resume its operations after the crisis (McCarthy & Gordon, 2016). This step encompasses the establishment of the actual plan to continue business operations. It should stipulate the changes that must be made in the organization to ensure that the business operations are running as usual even after the disaster.

## **Strategy and Plan Development**

 The fourth step is strategy and plan development, and the staff and other stakeholders should be included in the process. At this point, the organization must develop a strategy and plan on how to go about the recovery from the disaster and continue with the ordinary business operations.

## **Testing and Maintenance**

Finally, the testing and maintenance of the plan are done to assess the effectiveness of the plan. The reviews and assessments are essential in this plan to ensure that it works during the actual disaster. The above steps lead to the development of a successful continuity plan.

# Chapter 5: Information Security

Throughout the course, we have studied the critical role of information security in business continuity plans. When developing a security policy plan, various layers of security must be included in the plan. Each of these layers is important for data protection. One of the main layers is performing regular backups. Firms that fail to regularly backup their information resources expose themselves to huge risks that may affect essential information resources. Regular backups are essential because it ensures that all the data and information is stored in databases on the cloud should a system failure happen. The second layer of security that needs to be included is implementing strong data security protocols. Data security plans or protocols determine who in the organization has access to certain critical information sources. Through proper authorization, these protocols can ensure that access is only granted to personnel who have the required access.

The third layer of security that should be included in the security policy plan is encryption. Encryption is deemed to be one of the most effective ways to ensure that integrity is business data is guaranteed. When files are encrypted, a hacker or unauthorized person may not make sense of accessed information unless it is first decrypted (D'Agostino, 2019). Encryption should happen at the individual level for all pieces of information that are being received or relayed. Employee devices and servers should thereby be considered to ensure improved information security at the workplace. The fourth layer of security that could be included is by seeking external expertise. External expertise may be sought through outsourcing some of the areas that the company does not possess such expertise. The aim here is to ensure that the workplace has the latest technology in regard to information security.

# References

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cybersecurity using a fuzzy logic inference system. *Computers & Security*, *74*, 323-339.*approach.*Brookfield, Connecticut: Rothstein Publishing

D'Agostino, G. (2019). *Data security in cloud computing: Volume I*. New York, New York (222

East 46th Street, New York, NY 10017): Momentum Press.

Jackson, O. (2018). EU audit agency casts shadow on ECB crisis management plan. *International Financial Law Review*.

Jang, S. J., Kim, Y. H., & Shin, S. C. (2017). Korea's Terrorist Environment and Crisis Management Plan. *Korean Security Science Review*, (52), 73-91.

Järveläinen, J. (2016). Integrated business continuity planning and information security policy development approach.

Lindstedt, D., Armour, M., & Noakes-Fry, K. (2017). *Adaptive business continuity: a new*

McCarthy, D., & Gordon, K. (2016). SEC issues guidance on business continuity planning for registered investment companies. *Journal of Investment Compliance*.

Phillips, B. D. (2016). *Disaster recovery*. Boca Raton: CRC Press, Taylor & Francis Group.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201-218.