**Task:** Write an essay
**Topic:** Information System Project Management
**Type:** Information system project management
**Length:** 6 pages

**Formatting:** APA

**Requirements:** Provide a set of recommendations as to how the project can be managed.

# INFORMATION SYSTEM PROJECT MANAGEMENT

Student's name

Name of institution

## Introduction

Our life has several imperatives that cannot be argued by anyone. Life has a beginning and an end. We cannot guarantee that we are absolutely safe without regard to place or time we are at any given moment of living. Therefore, any human activities are also affected by the same imperatives. Everything has its beginning and an end. Nothing could be protected from risks for a hundred percent. These concepts lead us to the following conclusions: we can assess the risks we face and develop protective measures that could either let us avoid them or mitigate their aftereffects.

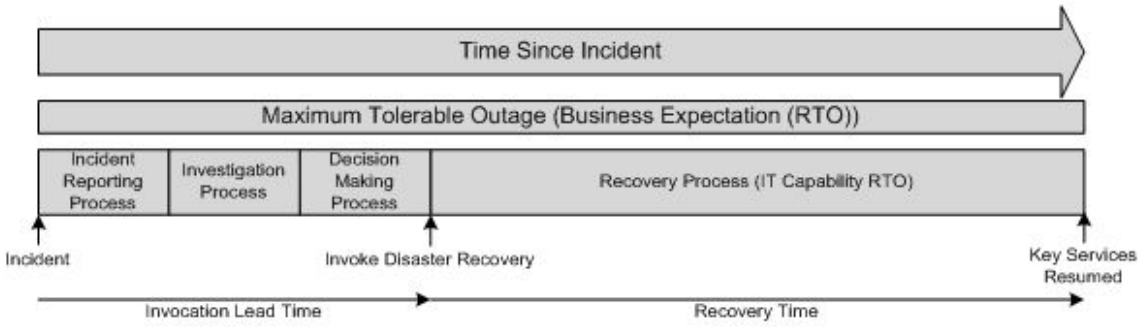
Business is the industry that completely depends on continuity as the main key to success. Any event that interrupts business processes for some time could influence substantially the position and situation of any company or organization without regard to market and country. The only way to protect business from such course of events is to develop the appropriate procedures that would allow avoiding particular risks and mitigating the aftereffects of others. The set of these procedures is called disaster plan that includes two substantial parts: disaster planning is aimed to describe activities that have to performed in case of natural or manmade disaster (hurricane, for example, and terrorist attack); and business continuity planning that describes what all interested parties must perform in order to assure the continuity of business processes.

This paper is aimed to present the plan of disaster recovery and business continuity actions that would allow for XYZ company to prepare for any situation that could happen in such potentially dangerous area as Miami. The major goal is to develop such a plan that would cover most of the situations that could affect business activities of the company and provide the appropriate solutions. The major parts of the plan are explored and evaluated in order to provide the appropriate recommendations in the conclusion section.

## Disaster Planning

Planning of the activities that should be performed in case of any disaster is a complicated process that involves many variables. However, probably the main measurement for any business is the time that this business could survive without any substantial consequences from the moment of disaster happening. It also can be called maximum tolerable outage (MTO) (Bradbury, 2007). In general, only the well-coordinated actions of the trained personnel and third parties involved into disaster recovery plan could help a company to save the situation with minimal loses. The diagram on Figure 1 (Bradbury, 2007) presents the correlation between the processes that gradually launch after the event:

Figure 1. Processes' Correlation

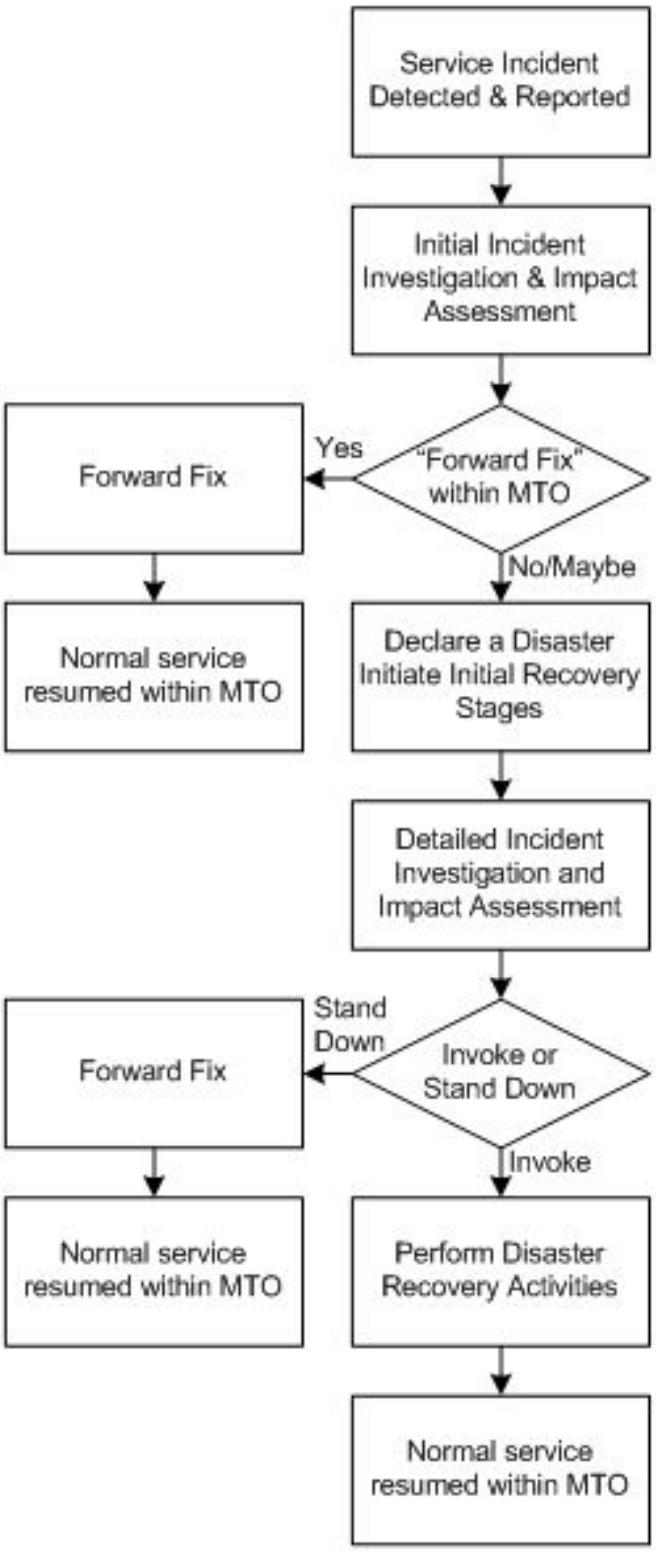



On this figure, we can see that the less time is spent on incident reporting process, investigation process, and decision-making process, the more time

could be spent on recovery processes. Therefore, knowing this ‘lead time’ could help planning the appropriate incident management activities.

Thus, the disaster recovery (DR) invocation flow could look like the following diagram that we can see on Figure 2 (Bradbury, 2007) that presents systematic steps that should be performed right after the moment the incident has occurred:

Figure 2. High Level Incident Management




An incident is reported using the standard processes.

How serious is the incident and what is the impact to the business.

Can the critical services be forward fixed with the maximum tolerable outage (yes or no/ maybe)

Declaring a disaster at this stage will invoke the initial stages of recovery, You may invoke or stand down at a later stage

Understand the full impact of the incident. Assess if forward fixing within MTO is achievable or if recovery at an alternate site needs to be performed

Invoke full disaster recovery or stand down and forward fix

Perform full disaster recovery activities as detailed in the Disaster Recovery Plan

The diagram provides us with understanding of the steps and their particular sequence that is needed to launch disaster recovery plan.

Actual disaster recovery activities could be divided into two following categories: prevention and mitigation. Each category should be explored, as the part of disaster recovery planning procedure however, both of them should be evaluated separately. It is necessary because mitigation of the aftereffects is a standalone plan that is invoked when prevention plan fails (Bradbury, 2007).

Prevention. Despite the fact that disaster is not possible to prevent, some particular steps could be performed in order to lower the risk of its crucial impact on a company. In order to understand how it can be done in each particular situation, it is necessary to assess the risks and possibilities of the most possible disasters to happen. XYZ company is located in a tidal flood zone so our particular case is connected with such possible natural disasters as flooding, hurricanes, tropic storms, etc. and manmade disasters as possible terrorist attack, human error, etc. Therefore, we can conclude that these two directions of disaster preventing should be considered as the threats with high level of risk. We have a clear understanding regarding the climate that provides Miami with mostly hot and damp weather. It is not appropriate for the IT infrastructure of any company (Bradbury, 2007).

The following steps should be performed in order to prepare for inevitable hurricanes, tropic storms, and floods that strike the Western coast of the U.S. from time to time every year: all communication lines should be additionally protected from the possible hostile environment, which water is by default; major communication nods and storages should be substantially protected from hurricanes and storms by placing them into special rooms with reinforced structures (solid walls, ceiling, floor) that should be additionally protected from water intrusion; these structures should be located separately from the main offices in order to have easy access to the equipment in case building collapses; such structures should be also protected by security measures to prevent an unauthorized access; all interested parties should be instructed regarding the up-to-date situation with IT infrastructure and its protective measures (Bradbury, 2007).

In order to prevent a terrorist attack or planting of a bomb (which is unlikely but should be considered as well), main lobbies of the offices should be equipped with metal detectors in order to prevent people with criminal intent and weapons of any kind form entering the facility. An insurance company could be a rather interesting target for cyber terrorists and people involved into terrorist activities (Bradbury, 2007). Its storages contain databases with

sensitive information regarding substantial number of clients so as it was stated before, IT facilities should be additionally guarded. Security systems should be improved and updated in order to follow the latest trends in IT security industry.

Mitigation. If a disastrous event was not prevented because of its nature or other reasons, mitigation is the stage that plays a significant part in the future of a company. Only the accurate execution of the appropriate action can minimize the negative impact of incident on business processes. In order to develop the mitigation plan, the following actions should be performed: it is necessary to establish and implement teams, responsible for each sector of work (incident response team, disaster management team, and others); it is utterly important to define responsibilities in each team and make sure that people are aware of what they are supposed to do; finally, teams should have proper training and clear understanding of the course of actions in each particular situation (Bradbury, 2007).

In our case, the above-mentioned procedures have to be performed in the same manner. Therefore, unit leaders must have clear directions regarding the evacuation of the personnel in case of emergency; employees must be aware of the evacuation points in case of flooding or hurricane approaching; response teams should practice periodically and conduct training exercises and drills to

stay in shape. These trainings should either prove the efficacy of the mitigation plan or show weak spots in it in order to eliminate them (Bradbury, 2007). Mitigation planning is about response to the situation that has already happened so it could be possible to avoid more consequences that are negative only if each member of the response team knows perfectly what to do.

**Business Continuity Planning**

The final stage of disaster response activities is business continuity planning. The actions, developed on this stage, provide the company with opportunity to continue business operations or restore them within minimal time. Business continuity is the essence of any business. It is not possible to imagine a successful company that does not work from time to time because of some kind of problems (Bradbury, 2007). A top management team of any company realizes that without the appropriate plan it is not possible to operate in case of emergency. In our case, XYZ company that operates on the insurance market does not have any business continuity plan except, probably, covering their electronic equipment with plastic sheeting (Bradbury, 2007).

Business continuity plan for the company should contain the following steps: it is necessary to evaluate the specifics of damage produced by each possible event that has high risk of happening (hurricanes, tropic storms,

floods); then, it is important to determine the approaches that would allow to fix the IT infrastructure and equipment for the minimal time; in order to do so, managers of response teams should be aware of the contacts they should have with third parties that can be maximally effective in each particular situation (city engineers, electricians, computer technicians, communication engineers, etc.) (Bradbury, 2007); security measures should be also determined that must prevent information leaks (e.g. damaged hard drives and other storages of information should be under severe control of the security); all parties involved into recovery activities should be aware of the situation that could happen so it is necessary to notify them in case of upcoming disaster, like storm or hurricane, for example; the appropriate support teams should be also organized that would provide recovery teams with necessary technical support (food, water; other supplies) (Bradbury, 2007).

Business continuity planning is about considering the most important actions that should be performed during the recovery stage. It also provides recovery teams with information regarding prioritization of the activities. It means that business continuity planning team assesses all business processes and determines the most critical ones. Then, it is needed to develop the appropriate scenarios for each possible situation that could happen to these

critical processes (Bradbury, 2007). It is the only way to make sure that the company will resume its work within minimal timeframe.

On this stage, the management team understands what should be done to make business running again. In addition, it allows seeing what measures are taken at this moment and which of them are inappropriate. For example, the IT director takes the computer disks containing backed up data home every day and keeps them in a filing cabinet. Well, it is good that this person cares so much about the safety of the data and security of sensitive information that XYZ insurance company surely has on these disks. However, it is rather obvious that such actions compromise security more severely than any flood or hurricane. It is not possible to assure security of the company's database when computer disks with the data leave the secured room (Bradbury, 2007).

Therefore, the more logical and reasonable step in this situation is to backup data every day to the off-site storage that is controlled by the company's specialists. It is the only way to assure that data is up-to-date, safe, and secured. Business continuity planning allows distilling such issues from the everyday routine actions that mistakenly are not considered as serious threats. In this case, continuity planning assesses not only the direct threats to the business continuity

but also the indirect ones and evaluates the possible collateral damage that such inadequate actions might cause (Bradbury, 2007).

After the threats assessment and development of the appropriate counter measures to prevent disaster or mitigate its aftereffects, the last step is usually left to make sure that all these efforts are not useless. It is necessary to conduct series of tests in order to see if these plans would work in the stressful situation. As it has already been mentioned, it would allow finding flaws in plans so the managers could eliminate them or create new plans for mitigating the aftereffects of these flaws (Bradbury, 2007).

**Conclusion**

In summary, disaster planning is the process with numerous participants, sub stages, and variables. However, it has three main stages, such as prevention, mitigation, and business continuity planning. Each stage has its peculiarities and produces certain plan of actions in case of the most plausible situation. Recommendations regarding each stage were given above. The appropriate plan of activities could vary depending on situation; however, the main course should be the same. Miami is in the potential danger zone and hurricanes, floods, tropic storms, and other similar disasters are not rare in this region.

Therefore, the only way to mitigate the negative aftereffect of a hurricane, for instance, is to know how to react before, during, and after it (Bradbury, 2007).

Disaster plan provides an opportunity to systemize and sort every possible situation that might occur because of the disaster. Hence, it allows preparing before it happens and be ready to respond immediately to minimize damage. A company that pays appropriate attention to such kind of issues has the chance to recover from disaster. The one that does not have such plan depends on luck and God's will. Business is not the place where luck is the key to success. Disaster planning is utterly important for any modern company or organization.

Reference List

Bradbury, C. (2007). The IT Disaster Recovery Plan.

http://www.continuitycentral.com/feature0524.htm

**Overall Impression**

This paper has strange phrasing, unnatural-sound language, missing articles, informal language used in a formal paper, misspellings, incorrect usage of prepositions, subject-verb disagreement, incorrect word usage, run-on sentences and a lack of commas. There were so many issues, it was hard to count. The organization was decent, though there were not many transitions. Overall, it is a messy paper that is difficult to follow with all of its errors splattered on the page.