Challenges and Opportunities of Having an IT Disaster Recovery Plan

Mohamed Ziyad Ghannam
Challenges and Opportunities of Having an IT Disaster Recovery Plan

Abstract

There are various types of disasters and no one can expect when they will occur. IT disaster recovery plan (ITDRP) became one of the most important contingency plans for organizations in the event of disasters. Organizations started realizing the importance of having IT Disaster recovery plan but many hesitate to apply this plan before a disaster occurs. However, even when the importance of ITDRP is acknowledged in the IS field, most scholarly work has focused on the process and strategies while briefly looking at the challenges and benefits of the DRP. This paper aims to investigate the most common challenges associated with having an effective ITDRP and the opportunities associated with this plan. A qualitative study was conducted which consists 6 interviews within several organizations which have developed an ITDRP. The results show that top management support, staff issues, maintenance, and disaster recovery sites are the main challenges organizations face during DRP. While the benefits were data protection, reducing the interruption for business functions, enhancing the reliability for staff and IT services and speeding up the decision-making process.

KeyWords: IT Disaster recovery plan, IT Risk management, Business continuity, Business impact analysis, Disaster recovery site, Disaster

1. Introduction

Information technology became a key component for all organizations which rely on it to manage daily duties and to facilitate business functions. Moreover, IT can provide organizations with competitive advantage and enhance its positions in the marketplace (Shao, 2005). Continuity is an essential requirement for all businesses, many examples reveal that the disruption for IT services have a major impact on business functions causing major losses for organizations reputation and revenue (Alhazmi & Malaiya, 2013). Moreover, the disruption of IT infrastructure can decrease employee productivity and damage customer relationship (Nilson, 2006). Many organizations faced difficulties to survive after encountering a serious disaster because they do not have any strategy or contingency plan to contain the damage (Shao, 2005). On the other hand, many companies continue working without significant interruption as they adopted these emergency plans. Statistics prove that organizations which prepare for disasters were faster three times to recover and to decrease financial and human loose compared to the unprepared organizations (Nilson, 2006). There is need for a plan to address all types of disasters which can disturb and stop business operations. Basically, disasters range from local power outage to massive disasters like fire or
an earthquake. Without having a plan to recover from any disaster or event, no matter how large or small companies are, they may fail (Shao, 2005). Snedaker (2013) refer to fire disaster as the most common emergency (disaster) companies face. Around 40 to 50% of businesses that experience a major fire go out of business because most do not have IT disaster recovery plan in place. Therefore, IT disaster recovery plan (ITDRP) is receiving a significant attention from researchers and practitioners. IT disaster recovery plan has been one of the main concerns for IT management (Kappelman, McLean, Johnson, & Gerhart, 2014; Luftman & Derksen, 2014). Effective IT disaster recovery plan is essential for organizations to protect them from data loss (Hawkins, Yen, & Chou, 2000). According to the latest SIM study by Kappelman et al (2014), IT disaster recovery occupied the tenth place in top concerns for IT executives. Where the main purpose is to respond to any disastrous events at the earliest time possible, ITDRP can help the organization to ensure that their essential services and business processes continue operating in the event of a disaster (Hawkins, Yen, & Chou, 2000). ITDRP involves policies and procedures are associated with being ready to recover in regards to technological infrastructure that an organization runs on.

1.2 Aim

Although applying this plan is vital for all organizations to respond to the crisis, but this solution can be time and cost consuming and requires a huge effort for organizations to implement this plan Snedaker (2013). Previous research has been done in IT disaster recovery plan process and IT risk management. However, research have focused on the ITDRP strategies and process while briefly mentioning other aspects of ITDRP. Therefore, there is a lack of research in this field focusing only on the challenges and benefits of having effective IT disaster recovery plan. Therefore, the research question will be formulated as follows;

What are the main challenges as to develop effective IT disaster recovery plan and what are the advantages to having it?

The aim of this study is to reveal the main challenges and benefits associated with developing IT disaster recovery plan in organizations. Revealing the challenges and benefits will help organizations to gain a better understanding in order to develop this plan effectively, besides uncovering the potential opportunities. In order to answer the research question, a qualitative research study has been done which involved several organizations and interviewed different actors. These organizations realized the importance of developing contingency plan like IT disaster recovery plan in order to protect their IT services and their critical business operations.

2. Related Research

The concept of IT disaster recovery plan is deeply rooted and associated with three main streams of research as presented in the table one; business continuity, IT risk management, business impact analyze.
<table>
<thead>
<tr>
<th>Stream of research</th>
<th>Definition</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan BCP</td>
<td>Procedures that an organization have to considered to keep critical business functions continue working during and after a disaster.</td>
<td>• (Herbane, Elliott &amp; Swartz, 2004) • (Wallace &amp; Webber, 2010)</td>
</tr>
<tr>
<td>Risk Management IT</td>
<td>The process to identify all threats, vulnerabilities and critical business processes</td>
<td>• Fallara (2003)</td>
</tr>
<tr>
<td>Business Impact Analyze BIA</td>
<td>The process to identify and evaluate the effects of an disruption to critical business operations as a result of a disaster.</td>
<td>• Fallara (2003)</td>
</tr>
<tr>
<td>IT Disaster Recovery Plan DRP</td>
<td>Activities that are used to ensure recovery for information system services with an affordable downtime when a disaster strikes.</td>
<td>• (Hawkins, Yen, &amp; Chou, 2000)</td>
</tr>
</tbody>
</table>

Table 1, Research stream for IT Disaster recovery plan

2.1.1 Business Continuity

According to Wunnava (2011), Business Continuity Planning (BCP) and IT Disaster Recovery Planning (ITDRP) are the main contingency plans that are implemented by organizations in order to keep business going on and to respond to unexpected disasters. BCP is a process used to enhance the continuation of business functions before, during and after the disaster and disruptive events (Nicolette & Schmidt, 2001). BCP involves collection of several activities and information which is developed and sustained to in the case of a disaster (Rozek & Groth, 2008). The emphasis of business continuity plan is on the protection of all parts of a business operation rather than just information technology system. The Information technology is addressed in business continuity plan in the terms of its support to the business process (Fulmer, 2004). Information systems have a major effect and influence of supporting organizations duties to meet business goals. Interruption or failure of information system has a significant effect on business practices; put differently has a major effect on business continuity. Due to the increasing dependency on Information Systems to achieve business objectives with an organization, every company that uses IT must address
the need for business continuity and disaster recovery planning regardless of the company size revenues (Snedaker, 2013).

2.1.2 IT Risk Management

Fallara (2003) argues that risk management is closely related to disaster recovery because they both deal with the prevention of risk. Risk management emerged to keep data protected and secured and to help the organization to realize which risk have to be addressed first. The main role for IT risk management is to protect IT resources such as data, hardware, software, personnel and facilities from all external disasters (e.g. natural disasters) and internal disasters (e.g. technical failures, sabotage, unauthorized access). This will enhance organizations abilities to achieve their goals and objectives (Hawkins & Chou, 2000). Many researches have been conducted in this field and highlighted the importance of risk management role in organizations. Tohidi (2011) argues that risk management goal is to support organization in order to have better management of risks associated with their activities and to provide more protection for IT systems. Solms and von Solms (2008) refer to IT risk management as an important procedure aim to address all potential risks associated with the use of information technology and to identify strategies to mitigate such risks to an acceptable level. IT risk management involve procedures that contribute to identifying vulnerable associated with information system and the process to handle it (Fallara, 2003). Threats are diverse and differ from organization to another. The table below presents the most common threats according to Stoneburner & Feringa (2002).

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural</td>
<td>Earthquakes, floods, electrical storms</td>
<td>These kinds of disasters have a major effect on IT infrastructure as they damage a large geographical area</td>
</tr>
<tr>
<td>Human</td>
<td>network-based attacks, malicious software upload, and unauthorized access to confidential information</td>
<td>Events that are enabled by human beings, such as deliberate actions</td>
</tr>
<tr>
<td>Environmental</td>
<td>Long-term power failure, pollution, chemicals,</td>
<td>Disaster-related to environmental change</td>
</tr>
</tbody>
</table>

Table 2, Disaster Category

2.1.3 Business Impact Analysis

Business impact analysis is the heart for disaster recovery plan (Fallara, 2003). Where the
IT risk management identifies business process and then rank them based on how critical they are to the all business process, business impact analyses determine the impact of the business processes if it become out of service for a period of time (Fallara, 2003). Hawkins & Chou (2000) State that purpose of business impact analyses is to identify the critical business resources that are crucial for an organization to keep going, and to estimate the acceptable time for an organization to resume their business functions after suffering from disaster. According to Snedaker (2013) there are four primary purposes of the business impact analysis. First is having better understanding of the most critical business operations of the organization. Second is to prioritize the critical business operations and set the timeframe for the resumption of these after an impulsive interruption. Third, reporting to the top management about maximum outage for each business operation. While the Fourth is about having information about the most suitable recovery strategy to be considered.

2.1.4 IT Disaster Recovery Plan

IT Disaster Recovery Plan (ITDRP) is a comprehensively documented plan consistent action to be taken to protect an organization from data losses and restoring data in case of disaster (Hawkins & Chou, 2000). Disaster is any event that can cause disruption to Information System services or IT infrastructure for a period and affect the business operations of organizations (Arnell, 1990). IT disaster recovery plan involves a group of policies and procedures that are used to monitor, recover and maintain Information Technology services during and after a disaster (Hawkins & Chou, 2000). Snedaker (2013) defines disaster recovery plan as a set of business continuity plan and deals with the immediate impact of an event. Therefore, companies need to address the potential disasters that will tackle their ability to continue business operations and earn revenue. Organizations can be affected by several kinds of disasters. Table 2 below presents disasters that faced by the organizations during a five years period from 2007 to 2012 (Alhazmi & Malaiya, 2013).

<table>
<thead>
<tr>
<th>Cause</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power outage/failure/issues</td>
<td>70%</td>
</tr>
<tr>
<td>Fire</td>
<td>69%</td>
</tr>
<tr>
<td>Configuration change management</td>
<td>64%</td>
</tr>
<tr>
<td>Cyber-attacks</td>
<td>63%</td>
</tr>
<tr>
<td>Malicious employees</td>
<td>63%</td>
</tr>
<tr>
<td>Data leakage/loss</td>
<td>63%</td>
</tr>
<tr>
<td>Flood</td>
<td>48%</td>
</tr>
<tr>
<td>Hurricane</td>
<td>46%</td>
</tr>
<tr>
<td>Earthquake</td>
<td>46%</td>
</tr>
<tr>
<td>Tornado</td>
<td>46%</td>
</tr>
<tr>
<td>Terrorism</td>
<td>45%</td>
</tr>
<tr>
<td>Tsunami</td>
<td>44%</td>
</tr>
<tr>
<td>Volcano</td>
<td>42%</td>
</tr>
<tr>
<td>War</td>
<td>42%</td>
</tr>
</tbody>
</table>
2.2 ITDRP Opportunities

The process of developing ITDRP helps the organization in recovering data from loss and protect IT services. Hawkins & Chou (2000) summarize the main benefits of having ITDRP into three. The first was data protection which is one of the most valuable resources for all organizations. Therefore, the main concern is to keep it protected and secured. ITDRP policies and procedures cover all the aspects to protect data through offering various backup methods like local backup and off-site backup. In case of a disaster strikes causing damage for data then the organization can restore it immediately. The second was reducing disruption to business operations. ITDRP emphasis on the existence of alternative sites besides having a professional team to deploy and follow up ITDRP, that will be vital to recover essential IT services within the minimum possible time and reduce the interruption for business operations. Lastly, offering alternatives solution during a disastrous event by developing an ITDRP before a disaster occurs, top management will have the required time to consider all possible solutions to disaster recovery.

2.3 Effective factors for ITDRP

According to the prior research, there are several factors should be considered for effective ITDRP.

- Top management support: ITDRP is a long-term process that requires a significant investment by an organization. Therefore, this plan requires top management support to secure resource and money for developing, testing and maintaining the ITDRP plan (Rothstein, 1988). According to Wold (2006), management should be responsible for coordinating the activities of disaster recovery plan and confirming the effectiveness regarding this plan within the organization. Moreover, management has to acquire the resources like time and budget in order to develop an effective plan (Snedaker, 2013).

- Sufficient financial support: the big challenge associated with initializing effective ITDRP is the total cost for developing, testing and maintaining this plan. This cost is considered too high besides that the ITDRP has no immediate return on investment. Therefore, sufficient financial support is crucial to achieve successful ITDRP (Chow, 2000).

- Alignment of ITDRP objectives with business goals: the business aims of an organization have to aligned with ITDRP objectives. These objectives of ITDRP define and set during the initial phase of ITDRP, and these objects can be considered as a guide for ITDRP (Chow, 2000).

- Conduct off-site Backup: off-site storage backup is a critical part during applying ITDRP, it provides organizations to restore their information in case of disaster. Off-site backup involves backup hardware, software, and data files. Arnell (1990) argues that location of the off-site storage should place in an area far enough from the organization.

- Choosing an alternative site: create an alternative site to replace the original site is vital of having an effective ITDRP. The alternative site considers an optimal solution to respond to the natural disaster like earthquake or flood which can destroy the original site (Chow,
There are multiple options to be considered when building the alternative site such as hot, cold site. All these options are possible to choose based on the budget and the acceptable length of downtime (Wong, 1994).

- Maintenance and update of ITDRP: efficient ITDRP have to be updated and maintained. Therefore, ITDRP must reflect the new changes in business strategy and the changes in information systems including hardware and software (Chow & on Ha, 2009). The importance of maintenance ITDRP is to reduce wrong decisions, decrease the stress of disaster recovery team during the recovery process and to keep the plan updated with changes in information technology and business operations (Chow & on Ha, 2009). Once ITDRP plan is developed, there is need to monitor changes in the organization which have a significant impact on ITDRP (Snedaker, 2013). The changes in IT infrastructure, systems and the business operations have the biggest impact on IT disaster recovery plan. Beside the changes in IT infrastructure and business operations which requires to update ITDRP. Changes in operations, legal and regulatory have to be monitored and considered in ITDRP (Snedaker, 2013).

- Continuous test of ITDRP: ITDRP should be tested periodically in order to make sure that ITDRP complete and valid (Chow & on Ha, 2009). Recovery team members have to perform simulation exercises. These exercises includes training to handle all kind of disasters. Conducting such exercises will make IT disaster recovery plan more accurate (Snedaker, 2013). The test of ITDRP is vital to train team members on how to use this plan on their duties and roles and how to communicate across the organization. Moreover, testing this plan will help to correct the wrong steps, procedures and checklist (Snedaker, 2013).

- Adequate trained Staff: having a staff with proper training is vital to have an effective ITDRP to solve problems in case of disaster occurs (Chow & on Ha, 2009). Staff members have to understand their duties and responsibilities to ensure accurate and fast deploying of ITDRP procedures (Hawkins & Chou, 2000). Snedaker (2013) argues that developing a clear and measurable outcome from the training is essential to have more effective training. This includes the basic requirements for the training and the expected learning outcomes. Moreover, he mentioned that the training on IT disaster recovery plan should involve training staff members on the specific roles and activities during implementing IT disaster recovery plan. Chow & on Ha (2009) argue that training is essential to ensure that all staff members understand their roles, to reduce the potential operational errors and the chance for the miss communication when the plan is implemented. Many companies have a limited time or funds available for training. The training on IT disaster recovery plan and is considered more difficult compared to the normal training (Snedaker, 2013).

- Perform Risk assessment and business impact analysis: risk assessment and business impact analysis have to conduct in order to have cost-effective ITDRP (Hawkins & Chou, 2000). Risk assessment address all possible threats to IT services and information systems. Business impact analysis determines the impact of the business processes if it become out of service and determines the maximum allowable downtime (Fallara, 2003).
2.5 Disaster Recovery Strategies

Basically, disaster recovery strategies can include but not limited to backup methods, alternative sites, and equipment’s replacement (Fallara, 2003).

*Backup methods.* In the case of a disaster event, it is important for any company to keep data protected and secured. Based on that, companies perform a daily backup of the critical data (Fallara, 2003). According to Hawkins & Chou (2000), it is important to consider off-site backup as the main backup method. This process will protect data against all kind of disasters.

*Alternative site.* Considering alternative site option is optimal to recover all IT services in case of major disaster (Fallara, 2003). ITDRP emphasis on the geographical separation of the primary and alternative sites (Alhazmi & Malaiya, 2013). Choosing alternative site should be considered if there is a risk to lose the primary site in a disaster such as a flood, war or earthquake (Wood, Cecchet, Ramakrishnan, Shenoy, van der Merwe, & Venkataramani, 2010). There are many types of alternative sites like cold sites, warm sites, hot sites, mobile sites and mirrored sites (Fallara, 2003). Lawler, Szygenda & Thornton (2007) argue that alternative site increase the redundancy and high availability for IT systems but on the other hand, the IT infrastructure and IT services will be more hard to manage and complex to maintain.

*Equipment’s replacement.* This option can consider in order to replace damaged hardware and software immediately (Fallara, 2003). Having redundant hardware and software components can mitigate the potential risks by working as backup facilities to prevent disastrous consequences (Shao, 2005).

3. Research Method

This section is concerned with the research methodology used in this thesis. The section begins with an explanation of methodology choice, followed by data collection and sampling, data analysis and ends with ethical considerations and limitations.

3.1 Choice of Method

The main aim of this thesis is to explore in depth the challenges and the potential benefits for developing DRP associated with organizations. The qualitative research methods have been chosen for this research since qualitative methods are the most appropriate approach to try to interpret a phenomenon or understand concept under research (Creswell, 2003). Strauss and Corbin (1998) argue that qualitative research is the best approach to interpret issues about experiences, cultural phenomenon, and social interactions. Three important factors make the qualitative approach the best to answer the research question and reveal the non-numerical insights within Phenomena context. First, qualitative research methods are the most suitable to interpret and understand a concept or phenomenon (Creswell, 2003). Second, qualitative research methods have the flexibility regarding the process which being investigated. Third, qualitative approach is valuable to understand the complexity regarding human behavior and relationship (Sofaer, 1999). ITDRP is a complex process which involves planning with many stakeholders in different levels in timely manner. Moreover, qualitative
research methods consider the best approach to gain depth knowledge (Patton, 2002). In addition, ITDRP is still considered an under-researched area and quantitative research would be not be preferable.

**3.2 Data Collection and Sampling**

Data collecting process in this thesis was done by semi-structured interviews. Semi-Structure interviews were chosen as the most suitable method due to many reasons. First to help the author to figure out how organizations develop IT disaster recovery plans, and to understand problems and challenges do they face during this process and what are the main benefits associated with this plan. Semi-structured interviews used when the researcher wants to probe deeply into a specific topic and according to the provided answers the researcher can gain more understand (Harrell & Bradley, 2009). Semi-structure interviews involve the use of preformatting questions which can help the researcher to get more details and seek the required clarification. Using the interviews in a semi-structured way will give the opportunity to ask questions regarding new aspects mentioned by the interviewers and enhance the information quality in this study. Besides the flexibility for semi-structure interviews, this type of interviews was also used because of the nature of the research question that needed interaction with IT managers to understand their view of the challenges and benefits to implement IT disaster recovery plan. According to Doody and Noonan (2013) the semi-structure interviews are the most common type of interviews in the qualitative research. In order to collect the same data from all participants, interview guide was developed (check Appendix 1) and this guide created a sense of order (Doody & Noonan, 2013). Semi-structured interviews allow the interview to be more flexible by having open-ended questions and the opportunity to discuss issues that arise spontaneously (Doody & Noonan, 2013). A minor change in the interview guide was made that included adding some questions and drop some of them based on the role and experience for each participant and the available time for each of them. The criteria for choosing these interviewers based on their experience in IT field and their knowledge for adopting ITDRP. A copy of the interview guide was sent to every respondent before the interview starts based on the belief that this will enhance the quality of the interviews and the data. Through this step, the participants can draw attention to the nature of the questions and give a good time to think about the answers.

The process to find appropriate participants started with connections that the author has worked with. More participants were identified through business social networks like linked-in network. Overall, six participants were interviewed for this study. This involved two ICT officers, Technical services officer, IT strategist, IT chief and the last person is DRP and BCP specialist. Participants were from several organizations. The ICT officers and the technical services officer were engaged in the planning and deploying process of ITDRP, and they work in the humanitarian field. The fourth participant is working as IT Strategist in the educational field. The fifth participant is working as IT chief is in industrial field. The last participant working in the health field. All participants have experience in either BCP or DRP in terms of planning or deploying. This research focus was to explore the challenges and opportunities of ITDRP in organizations. Since, this research acts as a first step and building block for future research just focusing on challenge, it deemed reasonable in the author point
of view to interview people from different fields and organizations to gain a wide view on the challenges and benefits. All respondents have both technical and managerial skills, and that will provide depth understand of how adopting this kind of contingency plan will help the business process to survive. To get more accurate data, some of respondents were given the option to choose between English or their native language that will make them more comfortable and help to avoid any misunderstanding regarding language barrier. To built connection with the interviewer, the interviews started with personal questions before starting with interview guide. All the interviewee's job roles and duration of interviews listed in the following table:

<table>
<thead>
<tr>
<th>Interviews</th>
<th>Job Role</th>
<th>Interviews Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviewee 1</td>
<td>ICT Officer</td>
<td>35</td>
</tr>
<tr>
<td>Interviewee 2</td>
<td>ICT Officer</td>
<td>100</td>
</tr>
<tr>
<td>Interviewee 3</td>
<td>Technical services officer</td>
<td>40</td>
</tr>
<tr>
<td>Interviewee 4</td>
<td>IT Strategist</td>
<td>30</td>
</tr>
<tr>
<td>Interviewee 5</td>
<td>IT chief</td>
<td>35</td>
</tr>
<tr>
<td>Interviewee 6</td>
<td>DRP and BCP Specialist</td>
<td>65</td>
</tr>
</tbody>
</table>

Table 2: List of interviewers, respective IT roles, and interview duration

3.4 Data Analysis

After data collection process ended, the recorded interviews were transcribed and translated to English. Thematic analysis method was used to approach the data, based on Braun and Clarke (2006) method which consists of five steps. The first step is to read through the transcribed texts and generate a list of ideas about the content of data, then extract the most important ideas regarding this data. The second step is to generate initial codes from the data. These codes identify the features of the data, then collating data relevant to each code. The third step involves sorting codes list into potential themes; group all data relevant to each potential theme. Fourth step was done by reviewing themes by checking if the themes work about the codes then skips themes which do not have enough data and keep the others. the last step is to define and name the themes by refining the specifics of each theme and define the name for each theme clearly. Thematic analysis method is widely used and it helps to organize and describe data with rich details (Braun & Clarke, 2006) and this fits the summarized answers that I got from the transcripts of the interviews. Decision to use the thematic analysis method came as this approach is flexible, easy method to learn and can be accessible to researchers with a little experience of qualitative research. Besides that, it can
offer a deep description of data set and sum up features of large data. Moreover, this method can point out the similarities and differences across the data set.

3.5 Ethical consideration and limitation
All the interviews were recorded after gaining permission from respondents beside that all respondent had informed about the ethical considerations. All the participants had been informed that the record interviews would be used only for research purpose. The most critical ethical aspect in this thesis was to protect the respondents by hiding all personal information that could possibly lead to identify them. An agreement was reached with the participants to mention only their job title also it was decided to keep their contribution in the final copy of this thesis as anonymous. Data collection process in this research conducted by interviews and questions guide has been developed and submit to the interviewers before the interview started. That made the participants more aware of the essence of this research. Moreover, it gave the participants the chance to avoid some questions for security and privacy reasons. For example, confidential information about IT infrastructure and recovery site specification. The main challenge in this study was data collection process. A good effort was put into finding respondents who have a good knowledge and experience in business continuity and IT disaster recovery plan in order to make the results more accurate.

4. Results
In this section, the empirical results are presented under the various conceptual themes were generated from the analysis. Four themes associated with challenges of adopting disaster recovery plan: top management support, staff issues, ITDRP maintenance and disaster recovery site. In addition to three themes related to IT disaster recovery plan benefits: data protection and reduce the interruption for business functions, enhance the reliability for staff and IT services and speeding up the decision-making process.

4.1 Challenges of Adopting Disaster Recovery Plan

4.1.1 Top Management Support
According to most of the respondents in this research, top management support seems to be the critical factor and key aspect to have an effective disaster recovery plan; respondent three had this to say.

"Top management support is the essential component to have successful disaster recovery plan" (Respondent three)

On the same topic, most of the interviewees talked about challenges related to adopting an effective IT disaster recovery plan. They emphasized on the awareness of top management support to realize the benefits of this plan to keep the business process going on. Top management should be aware of the risk of discontinuing business operations if any disaster happens and they do not have any prepared plan to handle it. The top management that is
aware about this plan will help the disaster recovery team by allocating more resources to implement an effective disaster recovery plan; participants two and three had this to say.

"Top management should be aware of the advantages of having this plan. This will help ITDRP manager to have the needed authority and resources to implement an efficient ITDRP" (Respondent two).

"The most important thing is the awareness from the top management side. Managers should know the consequences of facing a disaster without having a disaster recovery plan. This will affect the business process. So convincing the management about the importance of having ITDRP is vital “(Respondent three).

Most of the interviewees express their concern to convince top management to finance this plan, especially when the company or organization operates in a stable environment and no major disaster happened before. Managers always think that IT infrastructure is safe and the probability of facing a threat like a natural disaster or a fire that can damage it is low. Therefore, there is no need to finance this kind of plans; respondent one had this to say.

"Some managers might not be easily convinced about the benefits of ITDRP especially when the business located in a stable and safe environment which might limit budget resources to support ITDRP. The management often thinks that the place of the data center is safe and there is no threat like a fire or flood can affect it, the disaster could not be like earth quick or flood, but it could be a human mistake" (Respondent one)

Respondent six added that the poor technical skills of top managers are an important challenge. Therefore, it is hard for them to realize the major effect of IT infrastructure on business process. In the same context, respondent six suggests being as clear and simple as possible when explaining to them the importance of this plan. He emphasized on showing managers statistics which prove that many businesses failed because they do not have any plan to recover. Meanwhile, many firms survived after facing a major disaster because they developed an effective disaster recovery plan; respondent six had this to say.

"Convincing the top management is still a challenge because usually they do not have a good technical background which make it is hard to convince them of the importance of this plan. DRP managers should be as simple as possible in explaining the consequences of not having an ITDRP. It is important to show managers statistics for companies which failed to recover from a major disaster because of not adopting any contingency plan to face disasters “(Respondent six)

On the other hand, respondent five claimed that top management is not a challenge in his organization. He argues that management realized the role of Information technology and
the alignment between IT and business process. He continued, managers are quite aware that if the Information technology services stopped working, business operations will stop as well. As a result, the reputation of his company will be affected and might lose many of its customers; respondent five had this to say.

“I think it is not a problem to convince the management about the importance of this plan. Today IT role is integrated with IT business process, and the top managers are aware about the importance of IT. They know if the IT services stop working, the business process will stop as well and our customers will be furious. So, they realize that if the IT systems stopped working then the whole company will stopped working “(Respondent five)

Respondent four stated that allocating budget for this plan was not a problem as the top management appreciates the importance of this plan to protect the business process; respondent four stated.

"If you ask me if the top management has a problem with the high cost of adopting a disaster recovery plan, I will say no because they realize the importance of the plan. So, I do not think getting the support of the top management is a big problem." (Respondent four)

4.1.2 Staff issues
A major component of having IT disaster recovery plan is to have a professional and trained team. This team should be able to apply and test IT disaster recovery plan in parallel with performing its regular duties. Most respondents consider applying ITDRP as time-consuming and an overhead for IT team as they have to respond to their duties in addition to apply ITDRP exercises. Respondent two stated that one of these problems is that IT staff cannot always find enough time to perform ITDRP practices while the priority for them is to achieve their regular duties; respondent two had this to say.

"ITDRP requires the IT staff to allocate a considerable amount of time to apply it, especially when the team is working under pressure then there is no time for them to follow up this plan" (Respondent two)

Respondent five mentioned that high availability systems associated with ITDRP require time to be operated by IT staff; respondent five stated.

"It is a little bit overhead for IT staff to respond to ITDRP practices. For example, if you decide to build a system which requires a high availability solution then it will take more time to manage and to recover by IT staff "(Respondent five)

On the same topic, all of the respondents emphasized on having enough number of IT staff that have high technical skills and experienced in implementing ITDRP. Respondent three
considers the lack of staff as a challenge because sometimes ITDRP involves practices which the current staff cannot handle; respondent three had this to say.

"One of the primary concerns associated with deploying disaster recovery plan is to have adequate qualified staff that can apply and manage this plan. So, having an experienced team is considered as a significant challenge" (Respondents three)

Respondent two expressed his concern about performing IT practices when the company has a small number of IT staff with many daily duties to perform; respondent two had this to say.

"If the company has a small IT team with many duties, it will be a challenge to apply this plan" (Respondent two)

All respondents emphasized on offering the IT staff good training to respond to unexpected scenarios. Respondent six stated that ITDRP team must have to understand the new technologies which are applied in the data center. These new technologies like virtualization, clustering and distributed technology associated with ITDRP can offer the high availability, redundancy, and replication solutions; respondent six had this to say.

"Another challenge is to train your team on new technologies related to ITDRP like virtualization, clustering and distributed technology" (Respondent six)

Respondent six continues stating that the training has to involve simulation to check and follow-up the current status of this plan. Based on the results, many problems and issues might arise and need to be handled and that is considered as challenge; respondent six stated.

"Even if you have a qualified team with excellent technical skills, you should offer them a proper training. This training should involve simulation and test for the current status for the ITDRP. Based on the results many issues might arise and should be solved and this is considered as a challenge" (Respondent six)

4.1.3 ITDRP Maintenance

Maintaining ITDRP is one of the biggest challenges for IT disaster recovery plan. This plan needs continuous support and review. The importance of the maintenance process is to reflect all changes in IT infrastructure and business functions. Respondent four mentioned that one of the difficulties of deploying IT disaster recovery plan is that the deployment process needs continuous work and update; respondent four stated.

"The problem is that the work on this plan is not just during the deployment process. It requires continuous work to maintain and update it after the deployment process is finished" (Respondent four)
Respondent four continues stating that having updated ITDRP is the biggest challenge. The plan should be accurate and reflect all changes of the IT infrastructure and the business process; respondent four had this to say.

"If you ask about the top challenge associated with ITDRP, I will say it is updating this plan. This plan has to be accurate and reflect all changes (respondent four)"

Changes in IT systems often have the biggest impact on ITDRP. After systems are modified, upgraded, or terminated, the changes should be considered in ITDRP plan. Respondent two mentioned the challenge of creating a solid disaster recovery plan for IT Infrastructure and services since IT systems are always changing. Organizations always need to update their IT infrastructure to serve better their business needs. These new IT systems come with new improvements like better data handling, larger storage and so on. Based on these changes in IT infrastructure, there is a continuous need to review and update ITDRP; respondent two stated.

"Creating an ITDRP for IT infrastructure and IT services is so complicated since IT systems change rapidly. When new systems are applied to IT infrastructure, the old systems will be terminated. Many new systems come with new features and technologies that require updating the ITDRP in order to keep it effective "(respondent two)

Respondent three mentioned that updating ITDRP is not limited by changes in IT infrastructure but also changes in business functions. Organizations can decide which business processes are more critical to consider in ITDRP. These priorities can change from time to time and this will affect ITDRP; respondent three stated.

"Updating ITDRP is not limited to the changes in IT infrastructure, but also changes in business processes can affect ITDRP. These processes can change from time to time and you have to reflect these changes in your ITDRP" (Respondent three)

4.1.4 Disaster Recovery Site

Another area is that a major component for having IT disaster recovery plan is an alternative recovery site. Having two locations will enhance the availability of the critical business services. This solution is the best to save IT services and business functions against major disasters like earthquake or flood. Respondent five expresses the importance of having two sites working in parallel. The IT systems should be hosted in two sites. In case of a disaster strikes one of these sites, IT services will be recovered soon and users will continue working without any interruptions; respondent five stated.

"All the systems that are business critical should be located on two separate sites and synchronized together. So in a case of a disaster affects one of them, we can
move the IT services from one to another and the users work will not be interrupted." (Respondent five)

However, establishing this backup site is considered as a challenge for organizations and there are many obstacles to develop it. Respondent six stated that the operational requirements for the backup site will add more additional load on the IT staff and ITDRP manager. Having another site with the same requirements as the primary one requires securing more staff for the new site, more equipment and allocating a place in another building. The backup site will add the same workload as the main site. Another issue is that data in two locations should be secured and the connection has to be stable and secured between them; respondent six had this to say.

"Having a backup site adds additional load on IT staff and ITDRP manager regarding the basic requirement for the new site. For example, the new site needs additional staff, new equipments and a new place. Therefore, this site will add the same overload as the primary one. Besides that, the data and connection in the both sites should be secured so having a new site is a big challenge " (Respondent six).

Respondent five showed how it difficult and complicated to have a backup site to enhance the high availability solution. He stated that having the same service or equipment working in two locations will add more complexity to IT infrastructure. In this case, there is need to have IT team with advanced skills to manage it; respondent five stated.

"It is not easy to install and manage IT services if you want to build high an availability solution. For example, having active databases in two sites will be more complex to IT infrastructure. So, you have to have a high level of technical skills among the IT staff to handle this new situation" (Respondent five)

In the same context, respondent three have the same concern regarding the backup recovery site. He stated that having a high availability solution will enhance the redundancy for IT infrastructure, but on the other hand that will add more complexity to IT infrastructure. This infrastructure will expand and need more follow-up and monitoring; respondent three stated.

"The backup recovery site adds more complexity to the IT infrastructure as this redundant solution requires extra monitoring and follow-up " (Respondent three)

4.2 ITDRP Opportunities

4.2.1 Data Protection and reducing the interruption of business operations
All respondents mentioned that data protection is the main benefit associated with deploying IT disaster recovery plan. They emphasized on applying procedures which can protect data in case of disaster strikes. These procedures like off-site backup will provide more safety and protection for data; respondent two had this to say.

"The most important part associated with deploying ITDRP is to save data through conducting backup for all data and sent the backup tapes for another site." (Respondent two)

Another important point associated with deploying disaster recovery plan is to recover IT services in the shortest time after the disaster occurred. ITDRP strategies like having an alternative site or redundancy equipment besides having a qualified team trained to handle all types of disaster can improve ITDRP efficiency. These strategies mitigate the effect of disaster and reduce the downtime for IT services and business operations. Respondent two refers to the importance of having ITDRP to recover all IT services which are critical for business operations; respondent two had this to say.

"With developing ITDRP you have the ability to recover IT services in the shortest possible time." (Respondent two)

In the same context respondent four shares the same opinion. He explained how having two sites helped to recover IT services and business function immediately after electricity outage happened; respondent four had this to say.

"When a disaster occurs, it is possible to recover IT services faster and reduce risks by using different scenarios. For example, we experienced electricity blackout in the primary site, but we recovered all IT services from the backup site and users continued working without any interruptions"(Respondent four)

4.2.2 Enhance the reliability of IT Staff and IT services

Having this plan will increase the reliability of IT systems as ITDRP aims to enhance the recovery process by following several strategies in case of a disaster occurs. Users will still receive complete information of the highest possible timeliness. Some of the participants mentioned the importance of IT disaster recovery plan as this plan will provide a high level of availability of IT infrastructure. This plan improves the performance and quality of the IT services and increases trust among users; participant two stated.

"Implementation of this plan increases the reliability and stability of all IT systems. This will improve users' trust and help to facilitate their duties” (Respondent two)

In the same context, some of the participants argue that developing this plan will increase the awareness among IT staff. They will get a better understanding of IT services and the impact of these services on business process. This plan will enhance the technical experience sharing
and the knowledge of the IT infrastructure among IT staff. As a result, the IT team members will be more qualified to replace each other in their duties; respondent two had this to say.

"When you apply an ITDRP, all IT staff will be more aware of the IT services. This enhances the harmony regarding the individual knowledge of IT systems that the team works with. Also, this improves the flexibility of the IT staff and make its members more capable of replacing each other" (Respondent two)

Respondent five expresses how having this plan helps to reduce the impact of possible IT risks since it requires that all IT staff should be trained to face a different kind of disasters. As a result, the reliability and confidence among the staff will be improved and they will be less stressed when a disaster occurs; respondent five had this to say.

“Developing ITDRP helps to improve the reliability of the staff members. Because it involves many exercises and practices to handle all kind of disasters” (Respondent five)

4.2.3 Speeding up the decision-making process
Another benefit associated with developing ITDRP is reducing the time for decisions making when a disaster occurs. All respondents expressed the importance of this plan to speed up the actions when a disaster strikes. Respondent two described the benefit of having a tested contingency plan like ITDRP. He stated that developing ITDRP acquires allocating various types of resources such as time, budget and human resources to respond to any disaster. Allocating sufficient resources for the plan will speed-up the process of decisions making. Applying the IT disaster recovery plan would be almost as easy as applying a common task in normal conditions; respondent two stated.

"When a company has a tested ITDRP, it means that the company has already enough resources to apply this plan to respond to a possible disaster. This will speed up the actions and decision-making process in case of a disaster occurs" (Respondent two)

he continued,

"Applying and testing ITDRP in a correct way means that recovery process will be more like applying a routine process than creating and applying a new spontaneous process" (Respondent two)

In the same context respondent five mentioned the importance of having ITDRP to save the time and speed up the decision-making process. He mentioned that unless the company has a plan that can be followed, discovering a course of action will be a long and messy process; respondent five had this to say.
"By having ITDRP, we can speed up the decision-making process and save time. Without this plan we need a long time to decide and analyze what to do, which order and who is going to contact our customers" (Respondent five)

5. Discussion

In this section we will discuss the results of interviews which generated from this thesis and related them with related research presented in chapter two. That will be essential to answer the research question: What are the main challenges as to develop effective IT disaster recovery plan and what are the advantages to having it?

5.1 Top Management Support

Prior research on IT disaster recovery plan points out top management support as one of the most critical components to have an effective ITDRP. Top management support remains one of the greatest challenges to implement successful IT disaster recovery plan as described by many participants in this study. Participants described the gap to convenience top management in order to develop this plan. They stated that most of managers still do not realize the importance of this plan’s role in facing any potential disaster and to keep business operations going on. The participants stated that managers have to know the impact on business processes in case if any disaster occurs and the organization has no plan to handle it. This view is supported by Wing, Chow and Ha (2009), they stated that the big challenge to develop successful ITDRP is to convince top management that the plan worth the investment. However, the results showed how the role of top management is important to have an effective IT disaster recovery plan. This role is vital to help ITDRP team to allocate the required resources like time, budget and human resources for developing ITDRP. This view is shared by Wold (2006) who argues that top management level has to support and participate in the implementation of the disaster recovery plan. Also, management should be responsible for allocating adequate time and resources to develop a successful plan. Moreover, top management has the responsibility for cooperation and coordination between all departments when ITDRP team starts to deploy the plan. The participants described the problem associated with funding this plan by top management level because this plan considers as a long-term plan. Therefore, the top management will not agree on funding this kind of plans when the company or organization has a stable situation. This view is supported by Hawkins, Yen, & Chou (2000), they stated that ITDRP is a long –term plan that requires a strong commitment and need high support from the top management. One challenging aspect of management support which prior literature on ITDRP has not paid much attention to is the poor technical skills for the managers. Therefore, they underestimate the importance of IT’ infrastructure for business continuity. Managers always think that IT infrastructure is safe and there is no potential for any threat to occur like earthquake or fire. Having a good knowledge about the IT besides the business skills from the managers will enhance the communication between them and the IT staff, and then they will be more aware about the importance of IT infrastructure and it’s impact on business continuity process.
5.2 Staff issues
Having a trained staff with good experience is essential for developing successful ITDRP. The results show that offering IT staff a proper training is vital to understand ITDRP practices and to apply them in case of disaster. The results are aligned with Lee and Ross (1995), they stated that the effective ITDRP should offer the staff members a proper training to understand roles and responsibilities for fast deploying of ITDRP practices. This point of view is confirmed by Wing, Chow & Ha (2009) who argue that training is essential to ensure that all IT staff members can reduce the operational errors and the miss communication when the plan implemented. One challenging aspect of staff issues which prior literature has not paid much attention to is the overhead and the time consumption for staff to implement this plan. The challenge is that the IT staff have to respond to their regular duties besides responding to ITDRP practices. This will be additional overhead for IT staff, especially if the organization has a small number of IT staff with many responsibilities. ITDRP plan involves many practices and needs to follow up on daily basis. Staff members should practice on different scenarios to respond to any potential disaster. Moreover, this plan needs to be tested and updated to keep accurate and to reflect all changes in business and IT. All of these duties associated with developing ITDRP consider as an overhead for staff members, and in many cases they cannot find adequate time to deal with all these tasks. Another challenge is offering IT staff training for the new technologies that associated with ITDRP. IT staff has to know the new technologies which applied in the data center like virtualization, clustering, and distributed technology. These technologies can grant the high availability of IT systems but the challenge here is that IT staff should adapt and learn the new technologies.

5.3 Maintenance
Maintain and update IT disaster recovery plan is one of the most critical components to have an effective plan. The participants emphasized on the importance of the maintenance process to track all changes in information technology and business operations. Chow (2000) supported this point of view, he argues that effective ITDRP has to maintain and to update on an enduring basis to reflect all changes in business strategy and IT applications. This point of view is also supported by Snedaker (2013) who stated that maintaining the plan is essential to continue readiness. However, maintaining process is one of the significant challenges associated with developing ITDRP. All participants mentioned the difficulties to keep this plan accurate and up to date as this plan need continuous working to reflect all new changes in IT infrastructure and business functions. Prior research has been done by Nelson (2006), he stated that the difficult process associated with having ITDRP is the maintenance process of this plan. The participants mentioned two major changes which require to be considered in updating ITDRP, changes in IT infrastructure and changes in business operations. The changes in IT infrastructure have the biggest effect on ITDRP, IT systems and technologies changing very fast as many IT systems are upgraded, swapped out or modified. All of these changes have to be considered in updating ITDRP. Beside the changes in IT infrastructure, the changes in business operations have a significant effect on ITDRP. This point of view is supported by Snedaker (2013), he stated that the changes in IT infrastructure have a major effect on ITDRP as IT systems rapidly changing. Also, he points out the changes in the critical
business functions as these functions are not static and can change from time to time. However, the update and the continuous working to maintain this plan is critical for business to keep going on and to recover all IT services in the case of disaster. This plan has to be reviewed and updated if any major change in IT infrastructure, IT systems and business process occurs.

5.4 Alternative site
Another critical factor to implement successful IT disaster recovery plan is to establish alternative recovery site. This site will enhance the availability of the IT systems which are critical for business operations. All interviewers emphasized on having a secondary site, they believe that alternative site will be the optimal solution to face any major disaster like flood, earthquake and so on. This point of view is supported by (Fallara, 2003), he argues that one of best disaster recovery strategies is to consider alternative site. This solution is vital if there is a risk to lose the primary site like war or flood. Another study that was conducted by Yiu and tse (1995) considered selecting alternative site crucial for ITDRP because the primary site will not longer available when the disaster strikes. Although having alternative site will enhance the availability of IT infrastructure and IT services, many challenges addressed to implement this solution. Most of the participants mentioned that this solution adds more complexity to IT infrastructure as the IT infrastructure will expand and need more effort to manage and monitor. Prior research conducted by Lawler, Szygenda & Thornton (2007), they argue that alternative site can increase the redundancy and high availability for IT systems but on the other hand, the IT infrastructure and IT services will be more hard to manage and complex to maintain. Another challenge addressed by the participants to implement alternative site is to secure adequate budget to finance this solution. They mentioned the main requirements for the alternative site such as more equipment, staff, new building and so on. The alternative site is the best strategy to handle any disaster, but this strategy is the most expensive one compared to the other strategies like backup methods or equipment replacement. However, every organization has to conduct a risk assessment to figure out the most critical IT services for business operations, and based on these results they have to decide if it worth to have an alternative site or not. For example, some organizations have a critical systems which are expected to be available 24/7. In these organizations, having an alternative site is vital to recover IT services and save the critical business operations. On the other hand, if a company has an IT system without critical data and with few number of users then it is better to apply the backup methods and there is no need to have an alternative site.

5. 5 ITDRP Opportunities
There is a lack of research regarding the benefits of having an effective ITDRP. According to the author knowledge, there is one paper which focused and discussed DRP benefits. The aim was to confirm the results of the previous research in this area and trying to find more benefits which not mentioned before. The results showed several opportunities that are associated with having an effective IT disaster recovery plan to save data, IT infrastructure and to keep critical business operations working in case of an event of disaster.
respondents emphasized on having IT disaster recovery plan to keep data secured and protected. Prior research conducted by Hawkins & Chou (2000) agrees with the results by arguing that the main benefit of having effective IT disaster recovery plan is to keep data protected and secured, and that consider the main concern for all organizations. Another major advantage which is mentioned by all participants is the fast recovery of IT services which is critical for business operations. This point of view is also confirmed by Hawkins & Chou (2000) who stated that applying IT strategies like having a disaster recovery site is vital to recover all business operations at the earliest possible time. This point is important because that fast recovery of IT services and business operations in the event of disaster will reduce the financial loose for organizations. Moreover, many organizations have critical business operations which should be accessible by customers and need to stay active 24/7. In case of a disaster strikes and the company has no effective ITDRP, there is a risk to lose many customers and damage its reputation. Another opportunity for having effective IT disaster recovery plan which is mentioned by the participants is the speed up of decision-making process during the disaster. When the disaster occurs, organizations have a short time to take actions to mitigate the effect of the disasters. Therefore, having effective ITDRP will help to take immediate steps to fast recovery for IT services. This point of view confirmed by a prior research conducted by Hawkins & Chou (2000), they stated that having tested ITDRP will save the time and speed-up the decision-making process. One advantage of developing ITDRP which prior literature has not paid much attention to is increasing the awareness among the IT staff. The participants argue that developing effective ITDRP will help the IT staff to get better understanding of IT infrastructure and IT services and the impact of these services on critical business operations. Moreover, developing ITDRP will enhance the communication among the IT staff as they will exchange the information and experiences to perform ITDRP tasks. The final point is that effective ITDRP will increase the reliability and flexibility among IT staff as everyone knows his responsibility and roles. In case a disaster strikes, IT staff can deploy ITDRP as smoothly as applying a normal task.

6. Research limitation

Finally, a number of important limitations need to be considered. First is the lack of literature on this topic. As most of the prior research focus on disaster recovery plan activities and processes, while less research have been conducted on how to handle IT disaster recovery plan challenges and opportunities. Therefore, a few of old research had been used in the literature review to support the participants’ results. Second, the process to find respondents to participate in this research was difficult. The difficulty is that not many of the participants have a good experience in IT disaster recovery plan challenges. Moreover, IT disaster recovery plan involves confidential information about the IT infrastructure and technologies. For example, disaster recovery plan sites specifications that prevent many persons to participate and some of them ask for time to have the confirmation from top management.
7. Conclusion and suggestions for future Research

The purpose of this thesis was to investigate the challenges and benefits associated with having an effective disaster recovery plan in organizations. The research question in this thesis was: What are the main challenges to develop effective IT disaster recovery plan and what are the advantages to having it? In order to answer the research question a qualitative research has been done with six semi-structured interviews with IT managers and DRP specialist who are experienced with ITDRP implementation. As a concluding answer on the research question I can argue that there are many challenges of having an effective IT disaster recovery plan. The challenges which identified are the top management support, staff issues, maintenance and review and having alternative recovery site. Besides the challenges, the potential opportunities of having an effective ITDRP were investigated. The current findings add substantially to our knowledge about the challenges that organizations face in ITDRP which can help organizations tackle this problem. The main benefits were data protection, reducing the interruption for business functions, enhancing the reliability for staff and IT services and speeding up the decision-making process. This contributes to our knowledge of why having an effective ITDRP is crucial for organizations. The research sample is small and from multiple sectors which makes it hard to generalize the results to firms. However, the purpose of this research focus was to explore the challenges and act as a building block for further research that can dig deeper to the challenges. Further research can investigate the challenges in specific sectors or dig deeper on how to tackle these challenges. There is also a need for more live case studies in organizations who have used the ITDRP.

8. Acknowledgement

In the end of my thesis I want to thank all my participants for the time and for valuable information they mentioned in the interviews. I want also to thank my supervisor Jonny Holmström for his support and valuable feedback throughout this thesis.
9. Reference


T. Wood, E Cecchet, K. K. Ramakrishnan, P. Shenoy, J. van der Merwe, and A. Venkataramani, " Disaster recovery as a cloud service: economic benefits & deployment \ challenges", Proc. 2nd USENIX Conference on Hot topics in cloud computing (HotCloud’10), Berkeley, CA, USA, 2010, pp. 8-8


10. Appendix

10.1 The interview questions

Personal introductory questions

- Name
- What is your role in your organization?
- For How many years have you been in this role?
- Could you please describe your main duties briefly?

- What are the threats to your business processes and infrastructure resources?
- Which service/product to prioritize while deploying an ITDRP? What are the strategies to implement first?
- Which technologies ITDRP relies on during implementations phase? Do you think of better alternatives?
- What are the main advantages that ITDRP gives you to enhance business continuity in your organization?
- How ITDRP assists your organization in protecting data and IT services?
- How IT disaster recovery plan helps to reduce disruptions and downtime for IT infrastructure?
- How ITDRP helps you to provide alternatives during a disastrous event? And how efficient is it?
- How ITDRP speed up the actions and decision-making process during the disaster?
- What are the main challenges related to planning ITDRP?
- Do you consider convincing the top management to deploy this plan as a big challenge?
- What is the biggest challenge associated with having ITDRP? And why?
- Do you consider having ITDRP as time and resource consuming process?
- Do think that having ITDRP adds complexity to your IT infrastructure?
- What is the challenge associated with having alternative site?
- How it is difficult for IT staff to respond to their normal duties and follow up ITDRP activates?