Disaster Recovery Framework for Commercial Banks in Sri Lanka

Mueen Uddin[1], Sandun Hapugoda[2] & Roop Chand Hindu[3]

[1]Department of Information Systems Faculty of Engineering
Effat University P.O. Box 34689 Jeddah Saudi Arabia
[2]Asia Pacific University of Technology & Innovation, Technology Park
Bukit Jalil 57000, Kuala Lumpur, Malaysia
[3]Faculty of Economics and Management, University Putra Malaysia,
43300 Serdang Malaysia
[*]Email: muuddin@effatuniversity.edu.my

Abstract. The banking sector is the backbone of the entire financial economy of a country. In today's globalized world, most organizations use online transaction processing systems for transferring money and doing business. Natural or man-made disasters can lead to data loss which in turn can cause millions of dollars of money lost. This study focuses on disaster recovery practices in commercial banks in Sri Lanka. From our preliminary findings, it was concluded that commercial banks only have ad-hoc disaster recovery standards and practices, as there is no standard framework available. Fourteen (14) banks were selected for data collection and relevant authorities were interviewed. The results were translated as qualitative observations to understand the best practices. Similarly, international standards, compliance requirements of the central bank, and existing researches were used to develop a disaster recovery practice framework. The proposed framework was then validated for its efficiency and usefulness among commercial banks and found to be acceptable by the banking industry.

Keywords: *banking sector; business continuity; contingency planning; cross case pattern matching; disaster recovery.*

1 Introduction

Crisis management has been an expanding area of interdisciplinary research for some years. It has been brought more into the spotlight by recent well-publicized events. The International Federation of Red Cross and Red Crescent Societies (IFRC) found 7184 disasters from 2000 to 2009, ranging from the Bhopal disaster, the tsunami in Indonesia in 2004, hurricane Katrina in 2005, the Haiti earthquake in 2010 and the Chernobyl explosions to the September 11th attack on the World Trade Centre in New York. They caused an estimated 986,691 million of dollars of economic damages, millions of casualties while billions of people were affected [1]. Other high-profile incidents, such as the Enron scandal and the Potters Bar rail accident, together with recently

Received February 16th, 2015, Revised October 27th, 2015, Accepted for publication November 20th, 2015.
 ISSN: 2337-5787, DOI: 10.5614/itbj.ict.res.appl.2015.9.3.4

heightened concerns regarding terrorist activity, have been cited in academic and trade journals, led managers to consider the importance of adequate crisis planning and management. Despite the enormity of such events, they form only part of an increasingly complex set of factors to be considered as potentially significant threats for many businesses, which also include data fraud, intellectual property theft, and product liability, not to mention the normal commercial risks associated with doing business.

Continuous business is vital for any organization in order to survive in a competitive environment. It is even critical when we consider the organizations dealing with financials and online data processing, where a minute may be worth several millions of dollars. In today's environment, most organizations depend on systems and online transaction processing. Hence, data for a few seconds can lead to million dollar losses to an organization. Therefore, most CEOs are well-concerned about having a proper contingency plan in order to face various types of natural disasters and planned terrorist activities. One incident that drew the attention of the international community towards disaster recovery were the 9/11 attacks of the World Trade Centre twin towers in New York in the year 2001. This incident forced governments of every country to emphasize the significance of disaster recovery strategies to their key organizations. However, in Sri Lanka attention for disaster recovery aspects came in play way before the above incident. In Sri Lanka, most organizations started to think about disaster recovery strategies after the attack by terrorists aimed at the Central Bank of Sri Lanka on January 31, 1996.

The banking industry dominates the financial sector of Sri Lanka by representing 55% of the total assets of the entire financial system at the end of 2011 [2]. The banking industry in Sri Lanka has shown a robust growth throughout recent years by expanding its network domestically as well as globally. The number of licensed commercial banks increased from 22 to 24 from 2009 to 2011, while the number of banking outlets increased by 22% from 5,000 to 6,100 during the same period. Further, the number of automated teller machines also grew, from 1,800 to 2,200 from 2009 to 2011, that is a growth of 21% [2,3]. All these banks are governed by the Central Bank of Sri Lanka, which is the regulatory body for the banking and financial institutes. Among these banks, there are 12 foreign banks and 12 local banks. Of the local banks, two are state-owned while the others are private entities [2,3]. The Sri Lankan banking sector strengthened its presence in areas affected by civil war with 34 and 38 banking outlets being opened in the Northern and Eastern provinces, respectively [2].

Out of the 24 commercial banks, six are systemically important banks (SIB), comprising the two state-owned banks and the four largest private domestic

commercial banks. SIBs represented around 64 per cent of the banking sector assets at the end of the year 2011 [4]. The sustainability of the banking sector largely depends on the performance of the six SIBs. Apart from the licensed commercial banks, Sri Lanka had 9 licensed specialized banks (LSB) at the end of 2011 [2]. The number of LSB banking outlets increased from 650 to 775 from 2009 to 2011 [2,3]. Further, the Sri Lankan financial sector operated with 11 primary dealers in order to cater to the population, which is just above 20.4 million people, and also to the corporate sector on the island [2].

The banking industry of Sri Lanka has shown a significant growth in terms of market and products throughout the last couple of years. The industry was resilient to the present internal as well as global financial shocks as a result of strong prudential measures and less exposure to toxic financial instruments. The number of new branches opened during the year 2011 was 194, while the number of other banking outlets opened was 80. More importantly, the focus towards electronic banking transactions was further enhanced in the year 2011, in which 220 ATMs were launched while the total number of electronic fund transfer facilities at the point of sale machines was 27,073 the end of 2011 [2]. During the year 2011, the Sri Lankan banking institutions introduced various new products and services on the local market in order to gain a competitive edge among the internal as well as global players. These products mainly included new credit facilities, saving schemes, project financing tools, investment banking tools, mobile banking, and new e-banking facilities. Several commercial banks introduced new integrated payment systems during that year, such as new payment cards, mobile payment facilities, and money transferring methods with various advanced features, reflecting the increased inclusion of information technology in the banking business. As the intensity and volume of the banking services increased, the key payment and settlement systems of the country, such as Real Time Gross Settlement (RTGS), Cheque Imaging and Truncation (CIT) and the Sri Lanka Interbank Payment System (SLIPS), also showed a considerable improvement.

Along with the expansion of the branch network and development of sophisticated financial products, the inclusion of automated systems and usage of advanced information technology in the industry has largely increased. Consequently, the operational risks in the banks are exposed due to large dependency on automated systems and centralized databases have become critical. Accordingly, the banking sector has recently implemented various risk mitigation and disaster recovery strategies. Also the Central Bank, as the regulator, has laid out several guidelines on risk assessment and business continuity mechanisms to ensure the soundness and safety of the banking industry.

2 Problem Background

In a challenging business environment, continuous operation of the business is critical. According to Doughty, important objectives of the disaster recovery plan are: to minimize the duration spent making up for damaged productivity while the systems are not operational; to alleviate maintaining some semblance of usual business activities including creditor payments, receipting and banking activities; to reduce fraud and errors occurring during these periods [5]. Therefore, availability of information and a documented process are very important in facing a contingency situation [6]. According to a survey, there has been a significant increase of about 36% and a modest increase of 53% of global disaster recovery planning resources [7]. Despite these figures in today's environment, contingency planning is vital, even for a small business, for survival.

When considering banking and the financial sector, it was found that 59.7% of the functions are mission-critical in the financial industry and 32.3% of the mission-critical activities need a recovery time objective (RTO) of less than 4 hours. Furthermore, 96.9% of the functions should be recovered within less than 72 hours [8]. According to the above statistics, the RTO may be even more reduced for certain banks considering their operation levels and information criticality. Therefore, an information loss of a few seconds may lead to a business loss of several millions. Hence, the top management of each bank must consider disaster recovery situations as a top priority. As highlighted by Gregory Morwood, "Even the simplest of BC plans will require a series of complex and interdependent tasks to be executed in a coordinated manner under adverse conditions." Therefore, not only a documented process but also regular drills and training are very important [9]. The British Standards Institution has developed a code of practice in 2006, i.e. BS25999-1: 2006 and specification (BS25999-1: 2007), accepted by the international community in 2007. Also, ISO standards were published in the year 2008, i.e. ISO/IEC 24762:2008, in order to refer as a guideline for disaster recovery [10].

In the Sri Lankan Banking sector, the only guideline issued by a regulatory body is a circular issued by the Central Bank of Sri Lanka mentioning the requirements of a disaster recovery plan. However, the viability of the DR strategies adopted by the commercial banks is questionable. This research was carried out to support the streamlining ad-hoc DR plans developed by each bank. In today's challenging business environment, continuous operation of the business is essential. This is highlighted by the fact that 89% of organizations have started to direct their attention to business continuity and disaster recovery concerns [11]. According to a survey done by Disaster Recovery Journal for the state of business continuity preparedness in the year 2009, it was found that

approximately 90% of the organizations were getting executive-level support for BCP and DR. But only 23% of the top-level executives thought of BCP and DR as top-level critical activities. Also, it was found that 50% of the organizations had invoked their BCP and DR plans for the last 5 years and 3% of the organizations had invoked the same for five times or more. Due to this, it was found that 77% of the organizations already had a contingency plan and 18% of the organizations were planning to have a documented process within the next 12 months. Therefore, we assume that almost 95% of organizations have a BCP and DR plan [12].

2.1 Disaster Identification

Cegiela defines a disaster as a "course of events that causes serious physical damage to IT facilities located in a primary location and used by the organization on a daily basis, such that it renders them useless" [13]. Paradine defines DR as a plan that permits reinstating the actual state of business after it suffered some sort of major detrimental or another disastrous event [14]. Yiu and Tse define DR as a range of procedures that are practiced to ensure the recovery of relevant data within an appropriate downtime when a disaster has occurred [15]. Rosenthal and Sheinink define disaster recovery as an arrangement for emergency business and data center operations together with recovery planning following a disaster [16]. Salkowe and Chakraborty define disaster as "a shocking scenario that seriously disturbs the functioning of IT, community or society, by causing material, human, economic or environmental damages that are not in the control of local authorities through standard of procedures (SOP)"; additionally, it may be fruitful to clearly differentiate the terms disaster recovery (DR) and business continuity planning (BCP) [17]. Researchers have used both terms interchangeably, however, there is a difference between them. Disaster recovery normally employed in IT systems is the practice an institution executes in response to a crisis and is the process of recovering or regaining access to lost data, hardware and software to continue critical business activities after a natural or human-made disaster [18]. Business continuity planning is a procedure to ensure that an institution can survive a crisis, thereby mitigating its impact; in short, BCP is a practice that is taken into consideration before an incident has occurred, whereas DR is taken into consideration during or after an incident has occurred [19]. Wiboonrat defines DR as: "A set of activities executed once the disaster occurs, including the use of backup facilities to provide users of IT systems with access to data and functions required to sustain business processes" [20]. Hutt describes it as a concern for IT or computer security that provides alternatives for the organization's core contingency events that could be prejudicial to the functions usually performed. However, in today's business environment not only physical damage to the IT infrastructure is considered a disaster but also virtual and

intangible threats, such as unexpected system downtimes, virus attacks, system hackings, and many more are considered to be disasters [21].

From the top ten (10) IT disasters of all time compiled by Colin Baker, it is clear that major IT contingency situations have occurred due to natural disasters causing damage to the IT infrastructure, but also by planned human activities and unexpected system failures. Therefore, it is vital to have a look at all various types of possible threats that organizations may face [22]. There can be many reasons for a system downtime. However, Bajgoric lists the following 6 as the most important causes for system downtime [23]:

1. Software defects/failures
2. Planned administrative downtime
3. Operator errors
4. Hardware outages/maintenance
5. Building/site disasters (i.e. fire)
6. Metropolitan disasters (i.e. storms, floods)

The financial sector can't endure any system downtime unless they have a proper methodology to continue their operations during the system downtime. According to Bajgoric's survey, brokerage operation and credit card/sales authorization systems are the most critical systems. Both of these systems are categorized under the financial and banking sector and accordingly they hold an average hourly cost of $6,450,000 and $2,600,000. Neither CEOs nor CIOs will accept such amounts of losses due to a contingency situation. Therefore, they are willing to invest huge amounts of money and resources in a proper contingency plan to address these disaster situations [23]. Balaouras stated that 59% of decision makers on disaster recovery are concerned about natural disasters and extreme weather. In this multiple-answer study, it was highlighted that only 39% of the decision makers are concerned about IT failures. However, it is vital to be concerned about all possible factors while creating a disaster recovery plan for an organization [12].

2.2 Related Disaster Recovery Methods

The accepted practice among any critical organization is to have a coordinator handle contingency situations. Also, a documented BCP and DR process is an essential factor. Hence, the proactive creation of a DR plan helps organizations to survive and continue with their business during a contingency situation is required. Vijayan highlighted six directives that organizations have to consider when creating a disaster recovery plan. They are [24]:

1. Pre-emergency preparations
2. Emergency declaration and actions

3. Post-emergency response
4. Steps for return to normalcy
5. A timeline that lays out the actions in the response plan
6. Identifying alternative actions depending on predictability

According to the model developed by the Disaster Recovery International Institute (DRII), there are 10 subject areas which organizations and DR coordinators needs to be thorough with. They are:

1. Program Initiations and Control
2. Risk Evaluations and Control
3. Business Impact Analysis
4. Business Continuity Strategies
5. Emergency Response and Operations
6. Business Continuity Plans
7. Awareness and Training Programs
8. Business Continuity Plan Exercise, Audit, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies

Until the year 2001, there were not many accepted international standards for disaster recovery. However, after 2005 many international institutions developed standards for DR and BCP. The British Standards Institute is one of the pioneers in developing international standards for business continuity. Their proposed standard BS25999-1:2006, includes the best practices in business continuity management (BCM) and disaster recovery [25]. It describes the basic outlines and needs of deploying a BCM environment in order to manage the business-to-customer and business-to-business relationships. In 2007 the British Standards Institute released another specification, namely BS25999-2:2007, widely accepted by the business community: "BS 25999-2 specifies requirements for establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving a documented Business Continuity Management System (BCMS) within the context of managing an organization's overall business risks" [10].

Sheth argued that the BS25999 standard does not discuss the survival probability of a business in a disaster situation but focuses on the implementation of a business continuity management system (BCMS) [26]. In 2008, BSI introduced another standards specification: BS 25777:2008. This was introduced as a code of practice for Information and Communication Technology continuity management. BSI have identified that not only the IT infrastructure but also the communication infrastructure is vital for the survival of a business. This guideline caters for a better framework in order to achieve a

high-level preparedness for disasters [10]. Another guideline for disaster recovery was introduced by ISO, namely ISO/IEC 24762:2008. According to the ISO web portal, "ISO/IEC 24762:2008 provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management, applicable to both 'in-house' and 'outsourced' ICT DR service providers of physical facilities and services" [27].

According to a survey done for the Sate of Business Continuity Preparedness, it was found that 7% of organizations follow the BS 25999 standards to a great extent, while 56% of organizations are not using BS 25999 standards completely. Further, 6% of organizations are using ISO standards for business continuity, namely ISO 27001 and ISO 27002 to a larger extent and 45% of organizations have not considered ISO standards at all [12]. However, the above figures neither indicate that these standards are not being used by a limited number of organizations nor do they say that most of the companies do not use any international standard at all. Most of the above organizations are considering at least one or two guidelines in order to build their business continuity plan. However, these figures prove the fact that a DR plan cannot be implemented exactly by using a template or guideline, but international standards can be considered and they will be helpful when creating a customized disaster recovery plan to cater for the business requirements.

2.3 Types of Disaster Recovery Techniques

Disaster recovery is a huge area that covers end-to-end solutions in order to cater for contingency situations. The Basel Committee on Banking Supervision of the Bank for International Settlements has announced 7 main principles that an organization should follow while creating a disaster recovery solution. Below is a summary of these seven principles [28].

Principle 1: Organizations should realize and emphasize the requirement of having a disaster recovery plan. Top-level senior management and board of directors should take the responsibility of having a proper contingency plan in place.

Principle 2: Management should advise the organization to have a proper DR plan in place.

Principle 3: Each business group should develop their own business continuity plan considering the criticality of their contribution to the business. In this, it is vital to identify the critical systems and the tolerance level of downtime for the same. Therefore, the recovery objectives can be derived.

Principle 4: Emphasize the critical importance of the internal and external communications and build up a proper mechanism in order to cater for disaster situations. This is important to build up external customer trust and confidence.

Principal 5: Highlight the importance of cross-border communications. There can be situations in which organizations have to deal with external institutions and regulatory bodies.

Principal 6: Disaster recovery plans should be well documented and they should be reviewed in periodic basis. This can be achieved by applying periodic disaster recovery tastings and drills in order to identify new requirements and changes in the existing disaster recovery plans.

Principal 7: Ensure and keep reviewing the appropriate approaches and ensuring the possibility of reaching the recovery objectives set by each business group.

Considering the research scope, business factors and processes were not considered. IT integration along with the availability of systems and data was evaluated. Therefore, the recovery strategies mentioned in the research focused on the technical aspects of the banking systems and not the business functions and processes. In common practice, banks have an alternative disaster recovery plan, located either in some other branch or at a separate alternate site dedicated for disaster recovery, depending on the ability and capacity of the bank. Mathew Varghese specifies an alternative site as, "a location (other than the original premises of an organization) that is used to ensure the critical activities of that organization in the event of a disaster". Mathew suggests a distinction between the original site (Primary Site) and the disaster recovery backup site (Alternate/Secondary Site) [29]. Cecile defines primary and secondary sites as follows [13]:

Primary location: Premises where computer hardware used to process data and provide services to users before the disaster is located.

Secondary location: Premises where computer hardware used to process data and provide services to users after the disaster is located.

However, this definition about the alternate site is not sufficient when considering the current competitive market environment. Due to the high demand and the criticality of the IT systems, especially the online transaction processing system (OLTP), organizations may not be in a position to bear a system downtime even for a few minutes. As argued by Wiboonrat, organizations should have a standby/parallel site apart from the main and active

location. It will be helpful to have a copy of the data retained at the primary location. However, the acceptable time lapse after which the data should be available at the alternate site should be decided by the business considering the criticality of the data and the business impact [20].

There are several types of alternate disaster recovery sites. Operation at the disaster recovery site can be varied from one organization to another depending on the requirements and affordability. Wiboonrat has defined a module for disaster recovery locations with 7 tiers and categorizes them into four main categories [20].

1. Cold Site: This is an alternate location with a minimum number of IT resources. Organizations planning to implement a cold site should have a high tolerance for system downtime. There will be no manpower available on the site and the location is used when needed. RTO is 2 hours to 3 days and RPO should be within 24 hours.

2. Warm Site: Organizations planning to have a warm alternate location should have a moderate level of fault tolerance time. Systems should be available within one day and the entire critical operational-level activities should always be prepared at the location. Generally there won't be any manpower kept at a warm site due to the high overhead cost. RTO should be within 24 hours and RPO should be 5-30 minutes.

3. Hot Site: Organizations with fault-prone systems may prefer to have a hot site. The time period of data loss during a disaster will be very short. IT and process-oriented infrastructure should be available and ready at the location on a standby mode. Therefore, manpower or full time vendor support is required for this alternate location. RTO would be within 12 hours and the acceptable maximum RPO would be 10 minutes.

4. Fault Tolerance Site: This is a fully fledged disaster recovery solution with an infrastructure similar to that of the primary location. All equipment, communication links and the ability to manage the user load should be similar to those at the primary site with automatic failover, remote users may not realize from which site they are actually accessing. General acceptance is zero data loss and RTO can be 1 hour.

2.4 Problems with Banking Disaster Recovery Strategies

There are 24 licensed commercial banks in Sri Lanka with more than 1600 branches [2]. As specified by the Bank Supervision Department of the Central Bank (BSD), each bank has developed its own business continuity and disaster

recovery plans. However, still some problems, mentioned below, persist [30]. Most Sri Lankan banks have not considered international guidelines/standards while developing IT strategies. However, they have built their own DR plans. Most of the banks have no strategies on updating/reviewing DR plans regularly. Many banks do not conduct regular DR drills with the collaboration of business groups and use poor categorization and identification of critical and non-critical activities and processes. Even though CBS [31] has emphasized that all commercial banks, primary dealers and clearing and settlement service providers must have a BCP/DR plan (seven main guidelines), it does not specify a deployment framework. Yet the circular clearly specifies the fact that is it not a step-by-step guideline and banks can consider it as the minimum requirement. All widely accepted international standards were developed after the first and last circular, which was issued on March 29, 2006. These guidelines were not developed considering the Sri Lankan context. The guidelines insist on geographical separation of the primary site and the DR site but this not possible considering banking operations in Sri Lanka and the fact that the country is an island. Monitoring of the DR strategy and assessment of the DR environment was not carried out properly.

3 Proposed Work

It is an accepted fact that Sri Lankan banks should consider the international standards while developing DR strategy. However, adopting an existing international standard would not be feasible since there are specialized systems and banking processes in Sri Lanka such as the Cheque Imaging and Truncation System (CITS), the Sri Lanka Interbank Payment System (SLIPS) and the Real Time Gross Settlement System (RTGS). Also, there will be unique systems and processes in the near future, such as the Common Payment Switch (CPS) and online connectivity between banks for CITS, which are under discussion. Therefore, the best alternative would be to review all of the existing DR practices in Sri Lankan Banks and to develop a framework in order to streamline the international standards, also taking compliance matters into consideration.

The research reported in this paper fulfills disaster recovery requirements for different services in the banking industry of Sri Lanka. Initially, data were gathered and evaluated related to the existing banking practices and regulatory guidelines concerning existing DR practices and the IT infrastructure. Compression of various DR practices was conducted in order to identify the existing strategies. After a thorough analysis of the existing DR practices, gaps of the same were evaluated to identify the problems with the existing practices. As the artifact of this research, a framework was developed in order to streamline the DR practices of commercial banks in Sri Lanka. Finally, the

developed framework as shown in Figure 1 was distributed among selected technology heads or DR coordinators of commercial banks in order to get their feedback. The purpose of this was to assess the validity and correctness of the developed framework.

3.1 Disaster Recovery Infrastructure

It is well understood that the criticality of disaster recovery practices and procedures depends on the business type. The downtime that an organization faces varies according to the criticality of the failure and type of disaster. In order to define the timelines, banks should conduct a business impact analysis (BIA) of each system and the business group. According to Mathew Varghese, the business impact depends on the severity of the disaster occurring. He specified three severity levels for disasters summarized below [30].

Severity Level 01: Disasters that lead to some downtime of business operations. The downtime can be a measurable amount (2-10 hours) and no data losses will occur during this period. These types of disasters are the least severe disasters.

Severity Level 02: Disasters that incur partial or full damage to critical resources. The definition of the critical resources can vary from one organization type to another and each business should identify its critical resources.

Severity Level 03: These types of disasters extend beyond the organizational level, such as disasters affecting an entire city or metropolitan area and large-scale natural disasters can be categorized under this severity level.

As for the banking sector, a disaster recovery committee should consider all the above severity levels in order to attain a well-equipped DR plan.

3.1.1 Select Correct Technology

This is the most critical aspect of disaster recovery planning. Therefore, banks should think of the disaster recovery process and procedure even before procuring the critical banking solution. Even though the business impact analysis and the risk assessment are carried out for each application, it would be a better approach to evaluate the support for contingency situations before procuring critical applications.

Schmidt points out that in order to implement a disaster recovery infrastructure, the primary system must be available at the secondary site and it should have all applications, necessary configurations, and required data readily available [32].

Steinarcher emphasizes that the secondary site should have provisions for a backup facility of some sort, whether it is a cold, warm or hot site [33]. Supporting this, NIST mentions that data should be frequently backed up in a clearly defined policy, which is based on the criticality. This idea exactly matches the previous activity of conducting a business impact analysis and identifying the criticality and the sensitivity of each application. For this research we have identified the following five approaches and methods for data backup, which can also be used by the commercial banks in Sri Lanka [34]:

***1. Metro Cluster*:** This is a high-availability solution, installed in the same metropolitan area. However, for banks this would not be a good solution considering the implementation costs since they will have to set up another disaster recovery site in a distant area in order to comply with the regulatory requirements.

***2. Fast Restore*:** This is a high-availability solution typically managed within same datacenter. If something goes wrong with the primary application/database server, image on the high availability server will be restored to the primary site or the high availability server can be switched as the primary.

***3. Application-Level or Middleware-Level Clustering*:** Clustering is a good solution in order to cater for high-availability requirements. However, in case of a physical disaster this may really not help since there would be physical damage to the whole primary site and could affect all clusters.

***4. Application Data Mirroring*:** This is the disaster recovery method most commonly used in Sri Lanka. Most of the banks replicate the database logs of the critical applications real-time to the disaster recovery site. Therefore, the banks' approach is to minimize RPO on data, which is the correct approach.

***5. Disk Mirroring*:** Disk mirroring is part of every business application nowadays. This is a good approach to ensure the continuity of the business if there is a physical failure in a disk. However, this does not cater for any physical disaster or total system unavailability.

3.1.2 Setting Up Secondary Disaster Recovery Site

As per the study, it is evident that banks should have a site managed by bank staff without outsourcing the activity. However, it is the choice of the bank to decide whether to set up the DR in an own place or in a rented place depending on the affordability. Either way, banks should not have a shared disaster recovery site, which is practiced in other industries mainly due to the privacy impacts.

Selecting the location

As specified by Schmidt, "how far away the disaster-recovery site must be from the primary site is an organizational decision" [32]. NIST furthermore states that the location of the primary site and the secondary site should be determined on the basis of the potential threats identified and not merely by the distance between both. Supporting this argument, Sri Lankan commercial banks should also select the location to set up the DR site considering the threats identified during the risk evaluation exercise. This is why banks should come up with a realistic view on possible disasters rather than unrealistic disasters such as tectonic plate collapse [34].

As per the practice of the Sri Lankan commercial banks, the DR site should be at a distance of more than 15 kilometers from the primary site. Primary sites of all banks are located within Colombo city limits, close to the sea. Therefore, it is important to choose the secondary location more to the interior of the country rather than selecting a location in a coastal area. Since the distance clearly affects the RTO, convenience of transportation should also be taken into consideration and banks should be mindful of not building the disaster recovery sites in congested areas and areas with high traffic by road.

3.1.3 Design of Disaster Recovery Facility

As per the study, it is recommended that the banks should have a hot site as the disaster recovery site. All critical systems should be readily available at the DR site and the infrastructure should provide support for a low recovery point objective (RPO). Important considerations while designing the disaster recovery site are:

Mission-critical systems should be readily available at the DR site and the databases should be replicated real-time or with a very high frequency. It is recommended to have the same infrastructure as the primary site in order to cater the same level of business volume in a contingency situation.

Other key applications for the business should also have an infrastructure similar to that of the primary site. However, replication to the DR site can be decided depending on the criticality of the information and the frequency use.

Important applications that are not identified as critical or key systems can be set up in the DR facility by virtualizing several application servers on similar hardware. Yet, replication should be decided on the criticality and necessity of the application, which is identified during the phase of business impact analysis.

Furthermore, according to banking practices, banks make backups on physical media such as sequential tape drives as a tertiary option. It is recommended to continue with the practice of making backups to physical tape media (two copies) and store these in both the primary and the secondary site.

For file backups, banks can implement NAS/SAN storage or any other feasible storage mechanism or cloud computing or thin clients depending on a need basis, which can be replicated to the DR site as specified in the available technology section above.

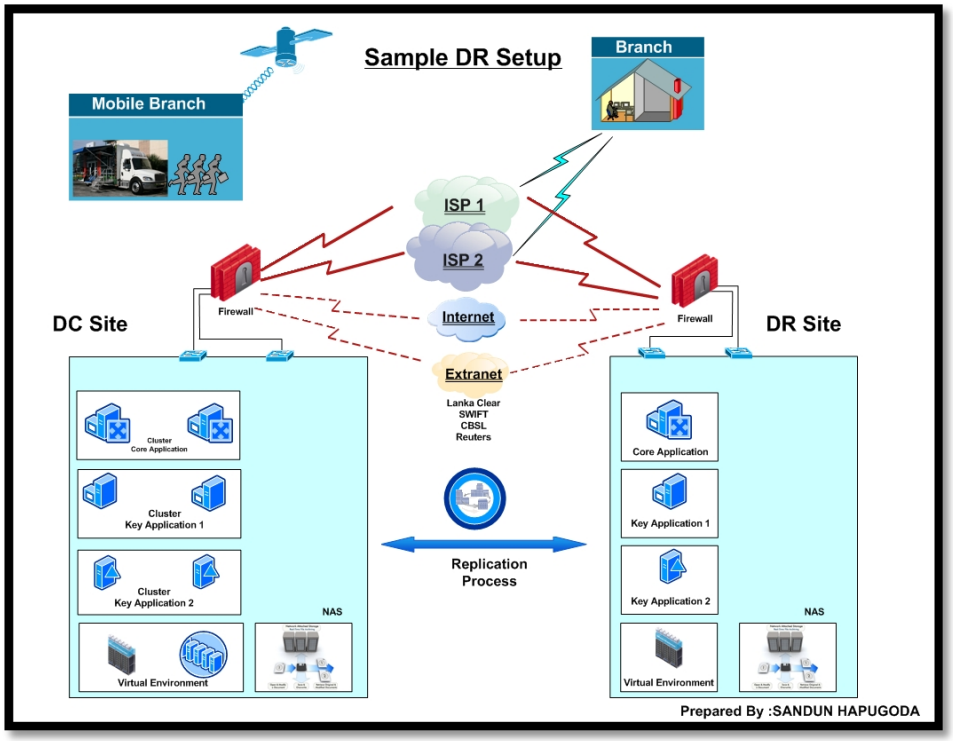

Figure 1 Proposed disaster recovery framework.

On the basis of the discussions, it was found that director-level attention for business continuity and disaster recovery was very low and rarely discussed at board meetings. In most of the banks, this aspect was discussed in a risk committee. Still, most of the times more attention was given to the financial risk (credit risk) and market risk than to BCP and DR. In all the discussions in the risk committees and corporate management meetings, the aspects of disaster recovery or business continuity were discussed only up to the point of regulatory compliance and not really on a strategic level in order to cater for an

actual contingency situation. Therefore, key-responsibility stakeholders believe that the corporate directors and management should pay more attention and provide a better level of support for planning for the actual possibility of contingency situations.

Knowledge of the general staff of the bank
It was observed that the knowledge of the general staff regarding BCP/DR was not up to the expected level. According to the conversations with the key personnel, it was found that most of the general staff who are not much involved in BCP/DR planning do not really know the difference between disaster recovery procedures and business recovery procedures.

Defining RPO and RTO
It was noted that with all banks, the definition of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) was not done in a calculated, scientific manner. All banks have defined RPO and RTO through expert judgments from the relevant IT staff members. The values were guessed by the relevant experts, without calculating real values. Re-valuations of RPO and RTO were done on the basis of the expert estimations without taking measurements.

Selection of the DR site location
All banks have chosen the disaster recovery site (secondary site) considering convenience. According to the standards, the secondary site has to be in a separate geographical location at a considerable distance from the primary location. However, considering the convenience factor and the cost of maintenance all banks have chosen the location within Colombo city limits or very close to Colombo. Due to this, any mass destruction may possibly bring down both the primary and the secondary facilities.

Requirement of the BCP/DR practices
On the basis of data gathered across all banks, it was observed that they built up their BCP/DR framework mainly because of the regulatory aspects and to comply with the regulatory guidelines. Therefore, the real business needs and the actual scenarios were given less attention when developing the disaster recovery plan and the test scenarios.

Policies, Procedures and Standards
All banks have a documented BCP/DR plan, at least for the sake of regulatory requirements. However, except for the foreign banks, all banks have mainly taken the CBSL guideline issued in the year 2006 as the main reference to build their documentation and the framework for contingency planning. However, it

was observed that two private local banks had obtained external expert knowledge for building their frameworks.

Regulatory Support
It was the general impression of all bankers that the regulator should revise the guideline. The local regulator, the Central Bank of Sri Lanka, is conducting audits for the BCP/DR once in two years. However, these audits are based on much higher standards than those from the guidelines.

4 Testing of Proposed Framework

It is evident that the international disaster recovery practices cannot be applied in the Sri Lankan banking sector as it is as specified above due to the specialized payment systems and unique practices used by commercial banks in Sri Lanka. Therefore, the purpose of this research was to understand the existing disaster recovery practices and compare them with each other, with international standards, regulatory guidelines, and other important aspects in order to develop a best-aligned disaster recovery framework for Sri Lankan commercial banks.

Since Sri Lanka has only 24 licensed commercial banks [2], the sample size was small enough to perform a proper scientific quantitative analysis and most of the available data are exploratory in nature, therefore a case-study approach was chosen as the most suitable approach for performing the research [35]. This is further prompted by the fact that the data for this research was gathered by interviewing domain area experts of each bank and the information would be relative according to the level of knowledge, experience and way of thinking. Therefore, the data would be explanatory of the practices used by each bank. Azevedo states that the case-study approach would be the best method to conduct a research when the boundaries are not clear and when there is no control over behavioral events. Therefore, the information analysis in this research was qualitative in nature and the case-study approach was adopted as the research methodology [36].

In this research, interviews with the domain area experts in each bank of the selected sample were the approach for the data gathering. Interviews were conducted on a one-to-one basis and data were gathered according to the responses of each individual. Yin summarizes the description of the further methodology as analyzing the collected data, which includes the arrangement of information in various different arrays, placing evidence in separate categories, presentation of data by using different graphical methods, and using the data for examination and complexity analysis. The same method was adopted for this research, in a manner where the data gathered from each bank were tabulated

under each research question area. Qualitative and relative answers were arranged in a manner that they fitted into a common framework in order to make the evaluation and compression process much easier [35].

The observations stated below represent information in each section under the statistical findings. Each area was critically evaluated with the help of represented output of the information for each section. Furthermore, a separate section was dedicated to a descriptive explanation of the general observations gathered while having discussions with the various domain experts of each bank, which could not be compiled in a tabulated manner in order to conduct a statistical analysis. At the final stage, the individual cases were taken and a cross-case approach and a pattern-matching approach were applied in order to derive the best practice for each aspect. Each case was critically evaluated and analyzed for this purpose. The artifact, a streamlined DR strategy framework for commercial banks in Sri Lanka, was developed as a guideline/reference for best practices under each aspect in disaster recovery planning and execution [35].

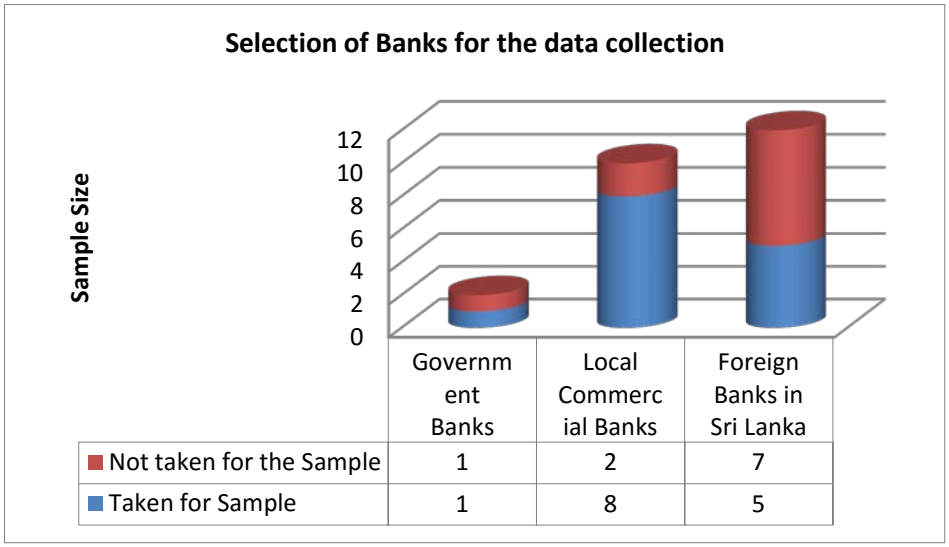

Figure 2 Selection of banks for data collection.

Sri Lanka has a total of 24 commercial banks. Out of these 24 banks, only two are state-owned banks, while the rest are owned by private entities or foreign stakeholders. Of the 24 commercial banks, there are 12 foreign banks and 12 local banks. In spite of the mix of private versus government banks, they are fairly well distributed in terms of financial book size, branch network and economic impact [2]. Considering the market, 14 banks were taken as a sample in order to understand the existing disaster recovery practices and gather data.

Out of the sample, 9 were local banks and 5 were foreign banks. One government bank was also taken into the consideration in order to understand the existing disaster recovery practices as shown in Figure 2. The strategy was to identify the existing disaster recovery practices of these banks and also to understand the strategic initiatives they have taken, not only to be compliant with the regulatory requirements but also to face any actual contingency situation [11].

Table 1 Testing Factors and Criteria

Area and Sub-Area	Sum of Average Response
Research Methodology & Data Analysis	34.58 (Avg: 3.84)
Analysis of available technology – Databases	3.83
Analysis of available technology – Storage	3.92
Analysis of regulatory requirements and guidelines	4.00
General observations and qualitative explanation	3.83
Interpretation and observations on statistical findings	3.83
Presentation of statistical findings and analysis	3.92
Research approach and qualitative analysis	3.42
Statistical findings and analysis	4.00
Survey strategy and sample selection criteria	3.83
Developed Framework – Streamlined DR strategy for commercial banks in Sri Lanka	37.50 (Avg: 3.75)
Business Impact Analysis	3.83
Defining DR scenarios	3.75
Disaster recovery documentation	4.00
Monitoring and auditing	3.50
Project Initiation and management (Responsibility)	3.92
Risk evaluation & control	3.67
Selecting the correct technology	3.83
Setting up of the secondary (DR) site	3.33
Setup of the specialized systems	3.75
Testing and DR drills	3.92
Overall adoptability of the framework	3.83
Adoptability of the framework	3.83
Grand Total	75.92 (Avg: 3.80)

Interviews were conducted to gather the information. Some details were obtained from the relevant authorities of the each bank in phone discussions. However, for both modes of data gathering, standard sets of questions were taken as a baseline. Data gathering was done mainly on three areas. The general area covered the availability of a DR facility, mode of operation, distance, documentation, and other information on readiness for a contingency situation. Some of the other details, like IT infrastructure, existing technology and information related to business awareness, management support, and customer impact, were also gathered.

The proposed disaster recovery framework was tested and analyzed in fourteen (14) different public and private banks in Sri Lanka. The results generated after testing the framework are shown in Table 1. The developed framework was distributed among 12 domain area experts including representatives from the central bank of Sri Lanka in a standard questionnaire format. All questions were scaled from 1 to 5, where 1 represents the areas that need improvement and 5 represents excellent work. According to the results, the methodology, analysis, and artifact were accepted and the framework was considered adoptable by the commercial banks in Sri Lanka.

4.1 Domain Area Experts Comments

Comments received from local banks:
"This is a very good reference book for a new bank when setting up their DR site. Even for existing banks that are still in the process of enhancing disaster recovery procedures this piece of work will be very useful. Almost all the areas related to DR are fully covered in the proposed framework and it's a complete reference if databases, backups and restoration features are improved a bit more." Another manager from a bank commented that the author refers to two main databases, Oracle, and SQL. However, if the sample is increased with two other database applications, such as DB2, MySQL or Sybase, it would be more beneficial for the readers since some of the giants in the Sri Lankan banking sector use these database applications. Other features, like Log Shipping and Replication in SQL Server and Data Guard, GoldenGate and Clusterware in Oracle, need more explanation and clarification. Another recommendation given by a manager highlighted that more emphasis needs to be put on the DR review process, with periodic updates of reference data to be processed and periodic drills/tests to be done in order to be ready for any disaster situation.

Comments received from foreign banks:
"I believe this is a well-timed research since most banks are currently in a need of enhancing their DR facilities. As a foreign bank, we do have a good policy framework and standard DR guidelines. However, there is still room for

changes and additions to the previous DR framework according to the banking setup in Sri Lanka and it can be further improved by applying the proposed framework and other outcomes of this research. Specialized payment systems and the architecture are considerably different compared to the country's, which houses our head office. Therefore, this type of baseline standard is a requirement for us to customize the DR setup representing the banks in Sri Lanka. Further, the framework should be evaluated for disaster recovery practices in the Asia Pacific Region, which for sure needs a lot of improvement; especially standards and procedures can be much improved in order to align with the best practices in the world."

Comments received from Central Bank of Sri Lanka:
"This research proposes a framework for streamlining DR practices in Sri Lankan banks. It is really considered critical in the present context where business continuity is considered a main aspect of the banking industry. Along with the increase in volume and complexity of banking activities, the banking institutions have depicted a large dependency on electronically processed data and online transactions. As such, it is eminent to have a robust disaster recovery (DR) plan in place to ensure continuous customer service and long-term stability. The researcher has conducted a comprehensive analysis on the existing DR strategies of Sri Lankan commercial banks, current regulatory frameworks, and respective international standards in order to produce an effective research outcome.

The research carries a thorough evaluation of the existing regulatory guidelines laid down by the Central Bank of Sri Lanka (CBSL) on DR practices, including the requirements of the Basel II Capital Accord. As is clearly highlighted through the research findings, the current regulatory guidelines do not provide a step-by-step approach to implement best practices of disaster recovery other than a basic general framework. Furthermore, the current regulations do not specifically address certain areas examined by the CBSL supervisors during the statutory examination of licensed banks. Therefore, a revision of the present regulatory framework on DR planning for licensed banks seems to be essential. The action plan proposed by the researcher for DR planning is possible to be applied in such a revision under proper consultation with the CBSL officials.

The researcher has not considered the Call Tree application, which is an important element of DR planning in formulating the proposed strategy. 'Call tree' refers to a communication technique used during disaster situations to activate recovery teams, share real-time updates between teams and to communicate to stakeholders about the recovery status of the bank on a continuous basis. An updated database which contains contact details of the

entire staff of the DR team should be available in order to deploy such technique."

5 Conclusion

The research reported in this paper motivates to understand the best-existing disaster recovery practices and compares them to existing disaster recovery practices with international standards and the regulatory guidelines. The main purpose is to develop a standard framework that can be used by the banks as a standard guideline. The research was mainly carried out as a qualitative data analysis and data were collected by conducting structured interviews with the domain area experts from selected commercial banks. 14 banks were selected from a total of 24 registered banks in Sri Lanka. Additional data were gathered referring the circulars, guidelines and discussions with officials in the Central Bank of Sri Lanka.

From the preliminary data analysis, it was understood that the commercial banks in Sri Lanka are not following any standard disaster recovery framework but they are merely using the CBSL guidelines issued in 2006. These banks certainly need a proper framework to build their disaster recovery policies and procedures. The "Streamlined DR strategy for commercial banks in Sri Lanka" , the artifact of this research, was proposed keeping in view the requirements of commercial banks in Sri Lanka. The proposed framework helps top level management to devise step-by-step procedures to develop and set up the disaster recovery practices for their respective banks.

The proposed framework was tested for its validity and correctness by experts from various foreign and local banks in Sri Lanka and also representatives from the Central Bank of Sri Lanka tested its acceptance level. From the findings of experts, the framework was considered a major breakthrough for the commercial banking industry in Sri Lanka as they were clearly lacking in following a DR framework for streamlining their data services and IT infrastructure. Further research can be carried out to enhance the findings and include licensed specialized banks and the non-banking financial institutions to understand their disaster recovery practices and to build a more comprehensive framework that will help the whole Sri Lankan economy.

References

[1] IFRC, *World Disasters Reports: Focus on Urban Risk*, 2010, Retrieved from http://www.ifrc.org/en/publications-and-reports/world-disasters-report/wdr2010/ (last accessed 15th April 2013).

[2] CBSL, *Central Bank of Sri Lanka: Annual Report*, Central Bank, Colombo, Sri Lanka, 2011.
[3] CSBL, CSBL Payments Bulletin, **9**(1), Central bank of Sri Lanka Colombo, 2009. Retrieved from http://www.cbsl.gov.lk/pics_n_docs/10_pub/_docs/statistics/monthly_bulletin/Monthly_Bulletin_2009/Bulletin_jan09e.pdf (last accessed 20th May 2013).
[4] FSSRC, *Financial Systems Stability Review*, Financial Systems Stability Review Committee, Central Bank, Sri Lanka, 2011.
[5] Doughty, K., *Auditing the Disaster Recovery Plan*, EDPACS, **21**(3), pp. 1-12, 2004.
[6] Botha, J. & Solms, V.R., *A Cyclic Approach to Business Continuity Planning*, Information Management & Computer Security, **12**(4), pp. 328-337, 2004.
[7] Chandler, R.C. & Wallace, J.D., *Business Continuity Planning after September 11*, Disaster Recovery Journal, **17**(3), 2004.
[8] Witty R. J., *BCM/DR Survey Results From Gartner, DRJ*, Disaster Recovery, **19**(4), pp. 26-32, 2005.
[9] Morwood, G., *Business Continuity: Awareness and Training Programs*, Information Management & Computer Security, **6**(1), pp. 28-32, 1998.
[10] British Standards Institution, Business Continuity - BSI Shop Homepage, Available: http://shop.bsigroup.com/en/Browse-by-Subject/Business-Continuity/, 1998 (Last accessed 18 January 2010).
[11] Cox, L.A., *Game Theory and Risk Analysis*. Risk Analysis, **29**(8), pp. 1062-1068, 2009.
[12] Balaouras, S., *The State of Business Continuity Preparedness*, http://www.drj.com/index.php?option=com_content&task=view&id=2407&Itemid=419&ed=49, 2009 (last accessed 18 January 2010).
[13] Cegiela, R., *Selecting Technology for Disaster Recovery*, IEEE International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX'06), pp. 160-167, 2006.
[14] Paradine, T.J., *Business Interruption Insurance: A Vital Ingredient in Your Disaster Recovery Plan*, Information Management & Computer Security, **3**(1), pp. 9-17, 1995.
[15] Yiu, K. & Tse, Y.Y., *A Model for Disaster Recovery Planning*, IS Audit & Control Journal, **5**, pp. 45-51, 1995.
[16] Rosenthal, P.H. & Sheiniuk, G., *Business Resumption Planning Exercising the Disaster Management Team*, Journal of Systems Management, **44**, pp. 12-16, 1993.
[17] Salkowe, R.S. & Chakraborty, J., *Federal Disaster Relief in the US: The Role of Political Partisanship and Preference in Presidential Disaster Declarations and Turndowns*, Journal of Homeland Security and Emergency Management, **6**(1), pp. 1-23, 2009.

[18] Hoffer, J., *Backing up Business-industry Trend or Event*, Health Management Technology, **22**(1), 2001.
[19] Menkus, B., *The New Importance of 'Business Continuity' in Data Processing Disaster Recovery Planning*, Computers & Security, **13**(2), pp. 115-118, 1994.
[20] Wiboonrat, M., *An Empirical IT Contingency Planning Model for Disaster Recovery Strategy Selection*, School of Information Technology, Assumption University, Bangkok, Thailand, 2008.
[21] Hutt, A.E., Bosworth, S. & Hoyt, D.B., *Computer Security Handbook, 2nd ed*., Macmillan Pub. Co., New York, NY, P. 399, 1988.
[22] Baker, C., The Top 10 IT Disasters of All Time - at ZDNet_co_uk, http://resources.zdnet.co.uk/articles/0,1000001991,39290976,00.htm 2009, (last accessed 19 January 2010).
[23] Bajgoric, N., *Information Technologies for Business Continuity: An Implementation Framework*, Information Management & Computer Security, **14**(5), pp. 450-466, 2006.
[24] Vijayan, J., *Data Security Risks Missing from Disaster Recovery Plans*, Computer World, **39**(41), pp. 16-18, 2005.
[25] Hong, Y., & Apostolakis, G., *Conditional Influence Diagrams in Risk Management*, Risk Analysis, **13**(6), pp. 625-636, 1993.
[26] Sheth, S., McHugh J. & Jones, F., *A Dashboard for Measuring Capability when Designing, Implementing and Validating Business Continuity and Disaster Recovery Projects*, Journal of Business Continuity & Emergency Planning, **2**(3), pp. 221-239, 2008.
[27] ISO, *ISO/IEC 24762:2008, Information Technology, Security Techniques, Guidelines for Information and Communications Technology Disaster Recovery Services*, http://www.iso.org/iso/catalogue_detail.htm?csnumber=41532, 2009 (last accessed 25 November 2009).
[28] Bank for International Settlement, *High-level Principles for Business Continuity*, Consultative Paper, http://www.bis.org/publ/joint14.htm,2009 (last accessed 19 January 2009).
[29] Varghese, M., Disaster Recovery Planning, [Online], Premier Press of Course Technology, Ohio, http://site.ebrary.com/lib/staffordshire/docDetail.action?docID=10066758&p00=disaster%20recovery, 2002 (last accessed 19 January 2009).
[30] BSD, *Directions, Circulars and Guidelines issued to Licensed Commercial Banks, Bank Supervision Department*, Central Bank, Colombo, Sri Lanka, 2011.
[31] CBSL, *Guideline on Business Continuity Planning*, Colombo: Central Bank of Sri Lanka, (BCP Guideline No: 01/2006), 2006.
[32] Schmidt, K., *High Availability and Disaster Recovery: Concept, Design, Implementation*, Berlin: Springer-Verlag Berlin Heidelberg, 2006.

[33] Steinarcher, S., *Is Your Organization at Risk?* System iNews, **47**(6), pp. 11, 2008.
[34] NIST, *Contingency Planning Guide for Information Technology Systems*, edited by U.S.D. o. Commerce. Washington, US Government Printing Office, 2002.
[35] Yin, R.K., *Case Study Research: Design and Methods*. Sage Publications Inc., Newbury Park, CA. 2003.
[36] Azevedo, S.G., Carvalho H. & Machado C., *The Influence of Green Practices on Supply Chain Performance: A Case Study Approac*h, NECE Research Unit, Department of Management and Economics, University of Beira, Portugal, 2011.