Towards a Conceptual Framework for Information Technology Disaster Recovery Plan for Banks: based on Cases from Ethiopia

Nigussie Tariku
School of Information Science
Addis Ababa University
P.O.Box: 1176, Addis Ababa, Ethiopia

Lemma Lessa
School of Information Science
Addis Ababa University
P.O.Box: 150453, Addis Ababa, Ethiopia

ABSTRACT
IT services and solutions in the banking sector should be protected to keep the business continuity in a disastrous scenario. This study aims to develop an Information Technology Disaster Recovery Plan (IT DRP) framework in the case of Ethiopian Banks. Qualitative case study method is employed to investigate current best practices and challenges in Ethiopian banks. The findings indicated that Banks do not have IT DRP in place. Lack of framework, lack of focused group, lack of experience, and lack of standardization are some of the challenges identified. Accordingly, the IT DRP framework is proposed for Banks of Ethiopia. The framework is confirmed and validated by subject experts. The framework can serve banks as a quality tool to evaluate existing IT DRP or develop new ones based on their business needs. Recommendations are also forwarded and related topics are suggested for future research.

Keywords
Business continuity, IT disaster, IT disaster recovery plan, disaster recovery

1. INTRODUCTION
Disaster recovery (DR) is a recovery of critical technology assets in the catastrophic IT failure events. Information technology disaster recovery (ITDRP) is about the recovery of technology-based resources such as applications, data, network connectivity & IT peripheral/hardware ([18], [29]. DRP can be distinguished as more a tactical document that provides a short-term plan to deal with IT-specific disruptions to an organization such as cyber-attack or system failures. DRP concentrates not only on the mitigation of the disaster but also to respond to and recovery of IT systems. Disaster recovery is considered as part of a business continuity (BC) management program [28]. Business Continuity in IT is the uninterrupted availability of IT resources that support key business functions. It is a general term that includes disaster recovery. The interest in BC and DR has increased in the last few years, especially with the increasing corporate dependence on computer systems and the growing levels of devastation associated with recent disasters ([5], [10]).

An IT disaster recovery plan is an IT-focused plan designed to restore the operation of the intended systems, applications, and computed facility infrastructure at an alternate site after a disaster. A mission-critical or essential business process functions of BCP or COOP (Continuity of Operations Plan) can be supported by DRP by recovering such supporting systems at an alternate location. IT DRP also deals with an information system (IS) disruptions that require relocation ([6], [31]).

The causes of disaster recovery are multifold. The incidents such as fire, flood, tornado, hurricanes, etc. have the potential to cause damage to buildings, equipment, and IT systems. The effects can be direct damage to buildings, IT equipment, and IT systems, causing buildings uninhabitable and systems unusable. There is also a utility outage that can cause no direct damage. But the essential supplies such as power, water, and others are interrupted to wider areas for days or so. In most cases, businesses simply can't survive after experiencing such an outage that causes them to cease operations for hours, days, or longer and this is a big loss for businesses like banks [8].

The major benefits of DRP are improved business processes, improved technology, fewer disruptions, higher quality services, and competitive advantage. A DR plan allows an organization for better availability and reliability of services. Businesses can leverage these benefits if and only if disaster recovery plan is in place among other things. In today's environment, most organizations depend on systems and online transaction processing. Hence, system interruption for a few seconds can lead to million-dollar losses to an organization ([2], [18]).

The modern sense of banking service in Ethiopia began towards the end of Emperor Minilik II. And the first bank was opened in 1906 E.C in cooperation with the British owned National Bank of Egypt and it was called the Bank of Abyssinia. Currently, there are 16 private and 2 government-owned banks and one central bank in Ethiopia that transact millions of birr per day ([10], [20]).

Banks are coming up with highly sophisticated technologies to get competitive advantages over their rivalries, but this is not enough for banks to stay in the market for a long time as natural or manmade disasters could disrupt their business process and the whole system for an extended time. So banks need to adopt BCPs and disaster recovery strategies to avoid intentional or unintentional problems that prevent the system from operating its normal business processes ([9], [27]). The purpose of this study is to identify the gap in the Ethiopian banks' disaster recovery planning practice and propose an ITDRP framework that can guide them in their IT Disaster planning endeavor.

The paper is organized as follows. The following section presents the research gap. In section three, a review of related literature is presented followed by the method in section four. Then, results and discussion of the research are presented. Finally, the proposed framework is presented and conclusions are made.

2. RESEARCH GAP

Business continuity is vital for any organization to survive in a competitive environment. It is too critical for organizations dealing with financial services and online data processing, where a fraction of a minute may worth several millions of dollars. In today's environment, most organizations depend on systems and online transaction processing. Hence, a disaster for a few seconds can lead to million-dollar losses to an organization ([7], [26]). An incident that drew attention of the international community towards disaster recovery was 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 on the significance of disaster recovery strategies to their key organizations [28]. The International Federation of Red Cross and Red Crescent Societies (IFRC) identified 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 dollars of economic damages, millions of casualties while billions of people were affected ([25], [37]).

Kadlec and Shropshire [13] found out that 60% of United States companies don't have IT disaster recovery plans in place. The IT disaster recovery planning guides developed were also inconsistent or complicated and the resources were not complete. It was also reported that on the IT DR planning practices of 154 banks in the United States, those organizations with adequate IT disaster recovery plans do not have IT budget and the size of their IT department was small.

IT disaster recovery plan has been one of the main concerns for IT management ([14], [38]). An effective IT disaster recovery plan is essential for organizations to protect them from data loss [9]. According a study by [14], 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).In a study by [35] in banking and the financial sector, it was found that 59.7% of the functions were 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. It was also 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 [3]. Another study indicated 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 due to lack of decision-makers and influencers [3]. These figures prove the fact that a DR plan cannot be implemented exactly by using a template or guideline, rather they will be helpful when creating a customized disaster recovery plan to cater to the business requirements. This also implies that international standards should be customized to fit into Ethiopian bank's context and culture.

Ethiopian Banks introduced various new products and services on the local market to gain a competitive advantage over 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. Consequently, the operational risks in the banks are exposed due to large dependency on automated systems and centralized databases have become critical. Ethiopia is amongst the developing countries that are most vulnerable to natural and man-made disasters ([16], [17], [23]). A study by [21] showed that 54.8 % of the companies faced a disaster in their computer systems, and infrastructure threats found to be the largest cause, and the software was the most affected part. Same study revealed that 76.3% of the companies had the plan, but did not follow all the necessary procedures and components of the plan. Nigussie [24] on his study assessed IT disaster recovery practices in the commercial bank of Ethiopia and found that there was an ITDRP framework gap. According to [10], 42.1% of the banks in Ethiopia have implemented ITDRP; whereas 57.9% of the banks didn't put into work so far. Whereas 42.1% of banks that have the plan in place are still believe that their plans need major improvements to meet its intended purpose. Hence, the researchers concluded that ITDRP was not exercised well at Ethiopian banks and that is why it is receiving attention from researchers and practitioners. The previous local studies revealed that there is no IT DRP Framework developed for Banks in Ethiopia. Thus, motivated by the problem on the ground and as suggested by scholars in recent related works, the researchers aimed at developing an IT DRP framework for Banks in Ethiopia.

3. REVIEW OF RELATED WORKS

There are few pieces of related works in Ethiopia on DRP investigation and assessment. Haylay [10] investigated the current ITDRP status in Ethiopian Banks using mixed methodology. The study found that 58% of the banks have no ITDRP in place. According to this study, there is a lack of ITDR framework and standardization, the problem of ITDRP adoption, lack of top management involvement, the problem of risk identification, and management perception. Furthermore, there was no ITDRP update, maintenance, and test performed for those that already have ITDRP in place. Besides, the study did not include other financial sectors.

Nigussie [26] made an assessment of ITDRP on commercial banks of Ethiopia using the qualitative method. 51% of the respondent agreed there was no risk control mechanism and 25% confirmed risks and its impacts on the bank had not been analyzed. 40% responded there was no IT DRP in place and the banks had not considered any international standards at all. Besides, IT DRP human aspect, updating, maintaining, and testing were the components that had been overlooked by those branches that implemented it. The study recommended the ITDRP framework as a future study. The study did not consider the private banking sector.

The following list of themes were identified from extant literature on IT DRP.

- **Project Initiation:** Businesses must establish the need for disaster planning and define a project plan to guide development efforts. The major tasks included in the initiation stage are: securing management support, organizing the planning project team, establishing the project management process, obtaining the required resources, and developing initial project objectives ([18], [22], [33]).
- **IT Business and Service Analysis:** A series of assessments to identify the core IT business scenarios, IT business impacts, potential IT threats and risks, inventory of all IT systems and associated services, and resources

deployed to support them. It consists of **IT Inventory**, **IT Risk assessment** and **IT impact analysis** ([6], [12]).

- **Develop IT Recovery Strategies:** Define and specify the approaches, policies, procedures, and processes to implement the needed resilience to achieve the principles of incident prevention, detection, response, recovery, and restoration. It includes Human aspect and responsibilities, IT DR action plan strategies and IT DRP testing, and evaluating strategies ([6], [30]).
- **Develop an ITDRP Plan:** Based on the information and steps listed above, identify and prepare an ITDRP documentation of specific policies and procedures to be used in the event of a disaster ([4], [6]).
- **Conduct Test, Exercise, awareness, and training:** Give bi-annual awareness and training once the plan has been developed. Overall testing should also be conducted per annum or quarterly as needed by the bank. Exercising after the new training and awareness is mandatory and recommended by pieces of literature ([1], [6], [24])
- **Conduct Disaster Recovery Plan maintenance and Audit:** Changes are inevitable, IT DRP requires continuous support and maintenance to fit the current requirements. Auditing the IT DRP documents, the technology, and human aspects are crucial to fit changes and preparedness ([6], [19], [34]).

4. METHOD

The research approach used for this study was qualitative and the strategy selected was a case study. Case study research involves an intensive study of a single unit to understand a larger class of (similar) units observed at a single point in time or over some delimited period of time. As such, case studies provide an opportunity for the researcher to gain a deep holistic view of the research problem and may facilitate describing, understanding, and explaining a research problem or situation [15]. Purposive sampling was employed to select the participants from both government and private banks. A face to face and telephone interview was conducted to collect the data from the banks. The interview questions were prepared based the themes identified from extant literature. Thematic analysis is used to analyze the interview data. The validity and reliability of the framework were done by domain experts. The participants for this study were IT Audit directors, IT Security Directors, risk managers, IT Data Center managers, CIOs, IT security Managers, BC and ITDRP managers, IT infrastructure and services managers, and incident teams and managers who are located at Addis Ababa city head offices of the two banks.

5. ANALYSIS

The interview involved asking questions, listening to, taking notes and recording answers from an individual and group in a structured and semi-structured format in an in-depth manner. The interview question was written in English and the conversation with the interviewees was in Amharic[1]. A translation of language and transcription of the recording was made to present the data.

The concepts are drawn from the conceptual framework. It has three phases: (i) Pre-plan phase includes project initiation and IT business analysis. The IT business analysis consists of IT inventory, IT risk assessment and IT business impact analysis such as RTO and RPO. (ii) Plan phase includes the recovery strategies and developing the actual IT DRP document. (iii) Post-plan phase includes the testing, training, awareness and exercise as well as the maintenance and ITDRP audit. Then, interview was made with interviewees per each area as a process that has been included in the framework. A briefing was made to the interviewees about each process or steps that need to be followed in the course of developing the ITDRP document.

A. Project Initiation

In relation to the initiation of an IT disaster recovery practice in bank A, the business continuity and IT DRP manager explained:

"Our IT DRP department is newly established and under development. The IT security directorate used to manage it. Due attention was not given and IT DRP was overseen by the bank. But recently the bank noticed its importance and established a business continuity and disaster recovery section that initiated the IT DRP project. Such project can be initiated in two ways. The first one is using a consultant agency from an external organ and the second is by the Bank's internal staff. In our case the project was initiated by internal staff. A gap analysis was made using the ISO/IEC 22301 by Bank's internal teams".

The IT audit director added "we are forcing the section to develop a standardized IT DRP plan and the report is submitted to the board of directors. The regulatory body (i.e. the national bank of Ethiopia) also strongly demands it and is putting pressure on banks to put it in place. So our management is also involved in the initiation of the IT DRP".

Bank B's Infrastructure and service management division head said: "The IT DRP plan was initiated by the bank's business team which includes IT teams and regulatory bodies. After approval of the project, it followed a project lifecycle as usual. IT DRP is incident driven and it was overlooked by management. The business continuity and disaster recovery section was not established yet. But the development is under initiation and we did not decide which standard to follow". The Data center supervisor of Bank B explained "The role of management is high as there is enforcement from internal business units and external regulatory bodies like the national bank of Ethiopia".

B. IT Inventory

The IT audit director and IT infrastructure manager of Bank A both said: "We are doing IT inventory as part of asset management".

The Business continuity and disaster recovery manager of Bank A described "ITIL process is implemented to facilitate the process and the IT asset management is automated. So, asset management software is used to control the IT inventory system of the bank". He added "confidential items, equipment, applications, software, tools, systems, etc. are well identified as part of IT inventory in particular and IT DRP in general". The information security manager of Bank A highlighted "sensitive and expensive security devices, equipment and systems are identified and managed as part of IT inventory".

The Infrastructure service management division head and data center manager of Bank B said "application, system, hardware, software, equipment, tools and services of data center and other inventory is done using excel spreadsheet. We have no specialized database to manage and control inventory. We recently established a service management unit and delivery team to identify services, critical systems, etc.

[1] Amharic is a local language widely spoken and used as official working language of the federal government

and prioritize them according to our criticality as high, medium or low".

They also explained the asset management is under development and not yet matured.

C. IT Risk Assessment

Bank B's CIO and Infrastructure service management division head said: "Any risk is assessed by the combination of Bank's IT audit team, risk and compliance management team, security team, risk identification and assessment team. Enterprise level risk management is not in place. Establishment of a unified risk assessment team is underway. There is a capability gap towards the establishment of enterprise level unified risk management. But the IT risk identification and assessment is working 24/7. After a risk is identified, it is reported to management and board directors and a mitigation action is taken to resolve the incident. A formal risk analysis is done in each section of the bank separately".

The IT security manager of Bank A said "We are conducting a formal IT risk assessment and analysis per the regulatory body and internal audit advises and bank's international standards". Bank A's IT audit director and Infrastructure manager on his part said "We work with the risk and compliance section of the bank and ensure risk assessment lifecycle is followed and in line with the business strategy as well as regulatory body and risk governance". The IT audit director added: "We also follow two approaches to identify risks. Those are risk based audits which allow us to identify risks with high, medium and low impact and report to management and board directors. The second approach is to follow a risk assessment lifecycle. The risk analysis is done per a standard and we advise the bank to follow standards whenever we assess IT related risks".

D. IT Business Impact Analysis

The Infrastructure service management division head and Data center supervisor of Bank B underlined "Because of the limitation of telecom infrastructure, the business impact analysis was not done according to the standards. But we provide support and maintenance services and have premium agreements for the critical system. Recovery point objective and recovery time objective are not set in our bank". The business continuity and disaster recovery manager of Bank A on his part stated "We have not made business impact assessment. We believe we are in the project initiation phase and on the IT inventory stage. We will follow the step and assess outage toleration, resource identification and mapping, dependencies of systems and others will be identified per ISO standards".

E. Recovery Strategies

The business continuity and disaster recovery manager of Bank A explained "Our recovery strategies are not well organized. There are separate general policies and procedures for tape based traditional backup and recovery strategies. However, this is not practiced as per the standard. Service plan has also taken longer time. The hot site is in place but the full documentation, policies and strategies are not in place". The data center manager said "we are taking tape backups. We are taking full back up once and use incremental backup afterwards. We were able to restore from technical and software crashes and it was one part of a test that the bank can restore from a crash in this scenario. But in case of catastrophic scenarios where restoration from relocation is necessary, it will be difficult".

The Infrastructure service management division head and Data center supervisor of Bank B explained "There are generic policies and procedures developed by the infrastructure team since there is no separate disaster recovery team established. The damage assessment is made by the same team. There is no specific document about strategies. There is no regular test needed as there is no hot or warm site. But basic facilities and human elements are in place on the cold site. We also have a power surge, cooling system, redundant infrastructure and cable systems on the site".

F. Disaster Recovery Plan

The Infrastructure service management division head and Data center supervisor of Bank B said, "There is no IT disaster recovery plan document in place. The information technology disaster recovery plan is under development by selected IT teams. It is in the initiation stage. We are trying to follow the international standards like ISO, COBIT, ITIL and NIST but unable to confirm which standard fits our bank. So we were urged to train the IT staff. Four of the IT staff have been selected to take the train. Lack of BC and DR division or lack of a focused team affected the Bank to lag behind in developing disaster recovery plans".

The business continuity and disaster recovery of Bank A's manager said: "There is no IT disaster recovery plan in place. The newly established BC and DR section is in its emerging stage to develop the document. We are following the ISO/IEC 22301. No one is trained on this standard and it is difficult to understand and implement per our bank's context. So, we are seeking for professional certified implementation company to train our staff".

G. Awareness, Train and Test

Business continuity and disaster recovery division manager of Bank A said: "Awareness, training and exercising the IT disaster recovery cannot be dreamed without developing the document. The previous steps should be followed consciously and carefully, the strategies should be developed, specific backup and recovery policies should be developed and tested first. The recovery test approach will be followed after we are able to develop the disaster recovery document".

Bank B's Infrastructure service management division head and Data center supervisor believe that "The document should be developed primarily, at least warm or hot sites should be in place and awareness, training and exercise will follow".

H. Maintenance and Audit

The Infrastructure service management division head and Data center supervisor of Bank B suggested: "The only maintenance we have in place is application and hardware based support and maintenance service by external vendors. We also have 24/7 premium maintenance and support service for critical services and systems. There is no maintenance or update done on IT DRP as there is no document in its full form. We have been advised by internal IT audit and regulatory bodies like the national bank of Ethiopia to develop an IT DRP plan and it is in progress".

The IT audit director of Bank A also explained: "We recognized the necessity of developing IT DRP plan document per the regulatory advice and enforcement. But there were no focused group to work on this plan. Recently, the BC and DR section is established to do the job. We will continue the follow up and report the progress to the management and board director as part of our responsibility".

6. DISCUSSION

The literature revealed that without conducting an effective project initiation, an IT DRP strategy will be incomplete and potentially unsuccessful when activated. For example, an IT professional who attempts to develop a DR plan without engaging other subject matter experts and managers will not be able to accurately assess the time-critical systems or the needs of each relevant stakeholder [18]. Both Bank A and Bank B tried to prepare a disaster recovery document without project initiation and were not successful. The infrastructure service management division head of Bank B stated that they had a pseudo-IT disaster recovery document that they used to show the regulatory bodies. Later they found that it was incomplete and decided to initiate an IT DRP project from scratch.

In the IT DRP project initiation phase, system requirements are identified and matched to their related operational processes, and initial contingency requirements may become apparent. Very high system availability requirements may indicate that redundant, real-time mirroring at an alternate site and fail-over capabilities should be built into the system design. Similarly, if the system is intended to operate in unusual conditions, such as in a mobile application or an inaccessible location, the design may need to include additional features, such as remote diagnostic or self-healing capabilities. During this phase, the IT system also should be evaluated against all other existing and planned IT systems to determine its appropriate recovery priority. This priority will be used for developing the sequence for recovering multiple IT systems [11]. The business continuity and disaster recovery manager of Bank-A confirmed, they are on the project initiation phase and have identified all critical systems but have not ranked them accordingly as they need to do BIA first.

A Business Impact Analysis (BIA) aims to determine which resources warrant the expense and effort of distinct inclusion in a disaster recovery plan. A BIA further specifies the priority by which each time-critical system is recovered after a disaster. The close examination of technology and business processes necessitated by a BIA can also identify potential changes that will reduce system interruptions or improve service quality. An assessment of current literature indicates that a BIA is a best practice that should play a central role in DR planning activities. A recent survey of business continuity managers reveals that 20 percent of businesses with continuity plans do not have a current BIA on file, and one-third of those companies with a BIA have failed to keep it up to date [8]. Accordingly, the business continuity and disaster recovery manager of Bank A and Infrastructure service management division head of Bank B stated that they have not developed BIA such as recovery point objective and recovery time objective reasoning telecommunication infrastructure limitation as a challenge.

The literature and international standards proved that the first step in the prioritization process is to define a maximum tolerable downtime (MTD) for each time-critical IT system that specifies how long the business can function after the system fails. The business should also calculate a recovery time objective (RTO) that declares how quickly the system should be restored. The RTO must be less than the MTD to account for delays in the resumption of work after a system outage. The final step in the prioritization process is to create a recovery point objective (RPO) that identifies the amount of information that a business can afford to lose permanently from each system during a disaster. The RPO will determine how frequently electronic data must be backed up to an offsite location from which it can subsequently be restored after a disaster has taken place ([8], [36]).

Per the conversation with Bank A and Bank B's CIO and business continuity and DR manager respectively, customer and business requirements are identified, external dependencies (i.e., government, industry, and legal) are identified, a business risk assessment is underway, management support is obtained and project planning are initiated. They explained they will follow the standards like ISO (Bank A) to prioritize the process.

DR planners should also meet with key members of the company, such as those responsible for facility management, to analyze the potential risks with which the company is faced. Such risks could include concerns ranging from a fire or flood in an IT server room to a major earthquake that destroys entire facilities. Secondary effects of disasters such as utility and communication outages should also be considered as potential risks. A formal approach that organizations can follow to identify and prioritize the risks that could lead to a disaster includes: (1) identify each potential disaster that could affect time-critical IT systems; (2) assign a value between 1 and 10,000 that represents the likelihood of each disaster, with 1 being the least likely to occur; (3) for each disaster identified, rate the potential impact on the time-critical IT systems, again using a scale of 1 to 10,000; (4) multiply the likelihood values by those estimated for the impact; and (5) sort the results to list the risks with the highest calculated numbers, representing the most significant risk, first. The broad range of values allows companies to distinguish clear priorities between many potential risks ([32], [8]). The IT Audit director of Bank A confirmed that they follow formal risk assessment and audit based risk assessment approach in assessing the risk in the Bank. This complies with what the literature stated above.

Recovery activities can be conducted in three approaches. The first one is to move operations to the Disaster Recovery Backup Site and the Emergency Operations Center. This activity begins with the activation of the Disaster Recovery Plan. The second one is to recover critical business functions, restoration of the critical applications, and critical network connectivity. The goal here is to recover the systems and network so that the customers can continue the business. The third one is to return data processing activities to the primary facilities or another computer facility [18]. In Bank A and Bank B only vendor based recovery activities and strategies are in place.

To adequately respond to a disaster, a business must have a "well-thought-out, documented" DR plan in place. IT DR planning best practices indicates that it is during the IT DRP development stage that organizations specify (a) how to react to disaster scenarios, (b) when to activate a DR plan, (c) how each critical IT system should be recovered, and (d) who should perform needed recovery tasks. The key elements identified within this section can guide DR planners as they develop and document IT recovery strategies based on the information identified through the BIA process [29]. It was well justified by both bank's IT managers that they do not have an IT DRP document in place.

Although no specific law states that a business must have a DRP, there is a body of legal precedent that has been used to hold companies and even individuals responsible for the recovery of data after a disaster [11]. According to the

business continuity and disaster recovery manager of Bank A, the regulatory bodies like the national bank of Ethiopia necessitates the development of the IT DRP plan. It was also confirmed by the CIO of Bank B that the regulatory body and the internal IT auditors urge the bank to have IT DRP in place.

According to [17], the purpose of computer security awareness, training, and education is to enhance security by improving awareness of the need to protect system resources; developing skills and knowledge so computer users can perform their jobs more securely; and building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. Awareness stimulates and motivates those being trained to care about security and reminds them of important security practices such as IT disaster recovery. Explaining what will happen to an organization, its mission, its customers, and its employees when security fails or disaster occurs often motivates people to take security more seriously. The success of a disaster recovery effort depends on the effectiveness of the response team. For this reason, all individuals who are assigned a position in an IT DR plan should be included as regular participants in DR testing. It is also important to involve the response team in the testing of DR plan to let those individuals get experience to enable a "cool and competent" response to a disaster. In addition to training through involvement in recovery testing, other sources such as conference room training and seminar-based instruction should be utilized. If employees are not properly trained to implement a DR plan, the planning efforts will have effectively been "wasted" ([31], [33]).

Bank A and Bank B IT managers and CIO confirmed that they have no IT DRP plan to maintain. Bank A and Bank B have not conducted post-implementation training, awareness, and testing since they have no IT DRP in place. But they have conducted some IT DRP awareness for the IT DRP development team who recently initiated the project. Due to the continuously changing nature of risks that face time-critical IT systems, businesses must ensure that DR plans are updated regularly to reflect the current environment. Depending on the frequency and complexity of changes, maintaining a DR plan may end up being the biggest challenge of the DR planning process for some businesses. However, developing an explicit strategy to address DR plan maintenance can reduce the complexity of the task ([9], [20]).

7. PROPOSED FRAMEWORK

ITDRP framework process or steps should be evaluated through well-executed method to prove the quality and efficiency of developed framework. The variable and measurement criteria used to evaluate the IT DRP framework are functionality, completeness, reliability, usability, and fit to the Bank environment. Those validation criteria are some of the relevant quality attributes prior to use it to the intended purpose. In this study, expert validation method is used to evaluate the proposed framework. Accordingly, focus group was used to gain expert validation. The experts in the focus group from both banks confirmed that this will greatly help them in the process of IT DRP framework development underway. They commented each area should be included and have no point to drop. The expert validation was chosen to gain different views of the business continuity and IT DRP, security directors, security managers, risk managers, and other experts who work in both Bank A and Bank B in various IT positions. Knowledge of IT DRP will help to gain valuable inputs and proper investigation of the proposed IT DRP framework. Besides, the experience of the knowledge area experts in the Banks in different positions also adds value to the holistic view of the proposed Information Technology disaster recovery plan framework.

A. Validation Comments from experts in Bank A

The Business continuity and disaster recovery division manager of Bank A commented that: "We are on the process of developing the IT DRP plan. Management acceptance is secured and we initiated the plan recently. This is nice and helpful as it consists of all the areas that we actually go through in the process of developing the plan. The areas included in the framework fits to our bank and the steps are valid. We used the IT inventory as part of auditing the general IT software and hardware. But we learned from the proposed framework that IT inventory as part of ITDRP document is useful and fits to our plan document. The inclusiveness of the recovery strategies to consider each and every process is an essential part that the bank will consider. In general, all the areas the bank need to include in the plan are included and complete. I do not find a point to drop in this plan. But I want to comment if implementation is considered".

The Data Center Manager of Bank A Said "MTD, RPO and RTO included under the business impact analysis are essential parts that over looked by the bank for many years. They are important metrics to be considered as we have only premium service level agreements for our critical applications. The testing, training, awareness, exercise and maintenance process in the framework are crucial usable steps and fits to our plan". The IT audit director of Bank A also commented that "This is what we used to recommend our bank. I like the inclusion of IT Audit as part of the process to help us follow up each and every step to be implemented as per the plan. Our regulatory bodies always force the bank to have IT DRP in place but did not give us the detail or framework to go through. The proposed framework is a good reference/guidance for both our bank and other banks in our country. I found all areas are useful to consider".

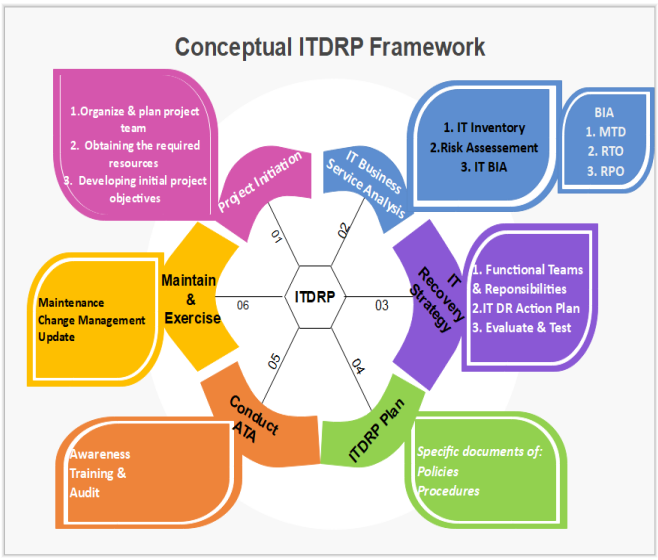

Figure 1: The proposed ITDRP framework

B. Validation Comments from experts in Bank B

When the proposed framework is presented to the Infrastructure service management division head and Data center supervisor of Bank B, he commented: "The established focused group development teams are in the way of developing the plan. We found the proposed framework is

inclusive and complete. Our current technology is in line with the areas depicted in the framework diagram. We are following the ISO standards to develop the framework but ISO lacks coverage area and details. We found this framework usable in our development of the plan document and no area to drop from the proposed framework. But in the future if we update our technology, we may need to maintain our plan and document".

8. CONCLUSION

The objective of the study was to propose an ITDRP framework for Ethiopian Banks that can be used as a base for developing their respective disaster recovery plans. Accordingly, an assessment of current practice was made and challenges were identified from one government-owned and other private-owned banks in Ethiopia. Per the study, the strength of Bank A related to the study is the establishment of the IT business continuity and disaster recovery department which deals with any IT disruption scenarios. Also Bank A has well established IT security directorate and IT audit directorate with subsections to deal with IT security issues and IT audit and evaluation activities. An added strength of Bank A is the implementation of automated asset management software to deal with the IT inventory system which is one component of the IT DRP plan document. The follow up of the IT audit to necessitate the development of IT DRP is the strength of both Banks and regulatory bodies like the national bank of Ethiopia. Overall, the IT DRP practice is at an infant stage in Ethiopian Banks. According to the participants, lack of strong backbone network between the data center and recovery site provided by the service provider in the country is also a challenge to both banks.

The proposed framework is aimed at ensuring consistency of disaster recovery planning practice among Ethiopian Banks. It will increase the efficiency and effectiveness of the services provided by the banks. It can also be extended to other financial sectors with minimum modification and used as a major input to develop IT DRP framework for other organizations in Ethiopia as it is developed in the context of Ethiopian Bank's culture, technology, understanding, knowledge gap and human elements factor.

The study is limited by the current level of understanding of the IT DRP plan document development, implementation, training, testing, and updating in the country in general and in the Banks in particular. Some of the topics except the pre-planning phase such as project initiation and risk analysis are difficult to gather sufficient data about. The planning and post-planning phases are not implemented in both cases. The study is limited to one tool that is interview. In most cases, the respondents were willing to share information regarding the topic. However, in some cases, they were not willing to admit weaknesses in security measures and do not want to share information due to fear of exposing vulnerabilities concerning IT risk analysis and assessment.

To cope up with the current advance in cyber-attacks, threats, and risks of IT-related disasters the following issues are worth researching in the future: Business continuity and disaster recovery framework for financial and other sectors; and mechanisms to address the acute scarcity of BC and DR professionals in the financial and other sectors in the country.

9. REFERENCES

[1] Adedayo, O. 2014. Disaster Recovery Strategy and Maintenance Plan.

[2] Ashebir E. 2017. Assessment of Information Systems continuity Management at CBE.

[3] Balaouras, S. 2009. The State of Business Continuity Preparedness.

[4] Baškarada, S. 2014. Qualitative case study guidelines. The qualitative report, 19(40).

[5] Benjamin, O. 2014. ITDR and Business Continuity at UN in Kenya.

[6] Choudhary, R. and Bhattacharya, D. 2016. Business Continuity Planning: A Study of Frameworks, Standards and Guidelines for Banks IT Services. International Journal of Emerging Research in Management &Technology, 5(8), 33-40.

[7] Creswell, W. 2003. Research design: Qualitative, quantitative, and mixed methods design. Sage, London.

[8] Gregory, P. 2013. IT Disaster Recovery Planning For Dummies. (PP. 10-14).

[9] Hawkins, S., Yen, D. and Chou, D. 2009. Disaster recovery planning: a strategy for data security. Information Management & Computer Security, 8(5), 222-230.

[10] Haylay G. 2018. An investigation of current status of IT Disaster recovery Plan in Ethiopian Banking Sector.

[11] Jones, V. A. 2011. How to Avoid Disaster: RIM's Crucial Role in Business Continuity Planning. Information Management Journal, 45(6), 36-40.

[12] Joseph, J. 2016. IT-DRP for Business Continuity: Case Study in a Business Sector.

[13] Kadlec, C. and Shropshire, J. 2010. Best Practices in IT Disaster Recovery Planning, Among US Banks. Journal of Internet Banking and Commerce, 15(1), 1-11.

[14] Kappelman, L., McLean, E., Johnson, V. and Gerhart, N. .2014. The 2014 SIM IT Key Issues and Trends Study. MIS Quarterly Executive*:* 13(4).

[15] Kothari, C.R. 2004. Research Methodology: Methods & Techniques. Second edition. New Delhi: New Age International.

[16] Kozina, M. 2009. COBIT - ITIL mapping for Business Process Continuity Management, in Central European Conference, Vara˘zdin.

[17] Lanter, A. 2011. Are You Ready? Getting Back to Business after a Disaster. Information Management Journal, 45(6), 4.

[18] Luckey, T. 2009. Key Stages of Disaster Recovery Planning for Time-critical Business Information Technology Systems.

[19] Mackey, A & Gass, S.M. 2005. Second language Research: Method and Design. London Lawrence Erlbaun, Associate Publishers, Mahwah.

[20] Maitra, S. Shanker, M. and Mudholkar, K. 2013. Business Continuity and Disaster Recovery Experience in Indian Banks. International Journal of Latest Trends in Engineering and Technology (IJLTET), 2(4), 526-534.

[21] Martin, B. 2002. Disaster Recovery Plan Strategies and Processes.

[22] Menkus, B. 1994. The New Importance of 'Business Continuity' in Data Processing Disaster Recovery Planning. Computers & Security, 13(2), 115-118.

[23] Mohammed, E. 2009. Evaluating Business continuity and Disaster recovery planning in information technology departments in Palestinian listed companies.

[24] Mohamed, R. 2014. A Proposed Model for IT Disaster Recovery Plan. I.J. Modern Education and Computer Science, 4, 57-67.

[25] NBE.2012. History of Ethiopian Banking. Insurance, Banking and Negotiable Instrument Law, Addis Ababa.

[26] Nigussie B. 2017. Assessment of IT Disaster Recovery Practices in Ethiopian Commercial Banks.

[27] Nijaz, B. and Moon, Y. 2009. Enhancing systems integration by incorporating business continuity drivers.

[28] Partio, A. 2014. Data center Disaster Recovery & Major Incident Management.

[29] Prazeres, S. and Lopes, E. 2013. Disaster Recovery: A project planning case study in Portugal.

[30] Protiviti. 2017. Guide to Business Continuity management (3rd ed).

[31] Randeree, K., Mahal, A. and Narwani, A. 2012. A business continuity management maturity model for the UAE banking sector. Business Process Mgmt Journal, 18(3), 472-492.

[32] Sheth, S., McHugh J. & Jones, F. 2008. A Dashboard for Measuring Capability when Designing, Implementing and Validating Business Continuity and Disaster Recovery Projects. Journal of Business Continuity & Emergency Planning, 2(3), 221-239.

[33] Sudhish, R. 2013. Optimization of Disaster Recovery Leveraging Enterprise Architecture Ontology.

[34] Swanson, M. 2010. Contingency Planning Guide for Federal Information Systems. NIST Special Publication.

[35] Uddin, M., Hapugoda, S. and Chand Hindu, R (2015). Disaster Recovery Framework for Commercial Banks in Sri Lanka. J. ICT Res, 9(3), 263-287.

[36] Verhofstad, J. (2000). Recovery Techniques for Database Systems.

[37] World Disaster Report. 2010. The Global Risk Report.

[38] World Economic Forum. 2019. The Global Risk Report.