UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

EVALUATION FRAMEWORK FOR IT SERVICE CONTINUITY AND DISASTER RECOVERY PLANS: THE CASE IN KENYA'S COUNTY GOVERNMENTS.

By

Bernard Kibet Koech

P/56/70379/2007

Supervisor: Dr Evans Miriti

A Research Project Presented in Partial Fulfillment of the Award of Degree in Master of Science Information Systems in the University of Nairobi.

2016

DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university for academic credit.

Signed: _____ Date: _____

Bernard Kibet Koech (P/56/70379/2007)

This project has been presented for examination with my approval as the appointed Supervisor.

Signed: _____ Date: _____

Dr. Evans Miriti.

School of Computing and Informatics

University of Nairobi.

ABSTRACT

Information Technology and Systems are bound to fail due to various reasons at one time or the other. Business and organizations rely more on systems these days than before. If these failures happen it affects objectives of the business negatively.

To alleviate these failures, IT industry addresses them through various technologies, legal and industry regulatory frameworks.

IT industry is evolving at an unprecedented rate. Solutions to past problems are obsolete within short span of time. Therefore there is no way that solutions to past problems are effective today.

There is no single methodology that can ensure 100% full recovery after a business disruption, there is a need for a set of benchmarks or standards to help ensure an adequate level of survivability, resources are used efficiently, and the best criteria for IT service continuity frameworks are adopted.

The objectives of this research was to assess implementation of IT service continuity initiatives in Kenya's County governments and secondly to formulate a framework to evaluate IT service Continuity and Disaster Recovery programmes on Information systems in Kenya's counties. An effective IT service continuity planning framework assures information availability and its survivability.

This study assessed IT service continuity plans or initiatives in the counties and secondly interrogated key Information Systems frameworks in existence which were found to be complex and expensive to be employed by county governments hence the study finally formulated a cost effective and simplistic framework that ensures credible assessment of the plans or any initiative at minimum effort. It also validated the framework by adopting a scoring system to test it based on assigned parameters against collected field data.

ACKNOWLEDGMENT

I give gratitude to the Almighty God for his guidance, mercy and providence in enabling me to work on this research project until the end. It was rigorous and resource consuming.

I would like to express my sincere thanks to my supervisor Dr Evans Miriti for having agreed to supervise this research paper and his patience in reading the drafts many times and guiding without which this research would have not been a reality. May God bless you.

My heartfelt appreciation goes to my family for their understanding and support during the project.

Lastly, I would also like to express my sincere thanks for all those who contributed in one way or the other, the respondents and my colleagues Mr. Charles Katua and Mr. Samwel Langat for their contribution and support. Thank you and God bless you all.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS.

AIMD - Accounting and Information Management Division

BCP - Business Continuity Planning

BIA - Business Impact Analysis

COBIT - Control Objectives of Information and related Technology.

CIC - Commission of Implementation of Constitution.

DRP - Disaster Recovery Plan

GAO - United States General Accounting Office GAO/AIMD, 1999

FFIEC - Federal Financial Institutions Examination Council

ITGI - Information Technology Governance Institute

ITIL - Information Technology Infrastructure Library.

ITSM - Information Technology Service Management.

ITSCM - Information Technology Service Continuity Management.

ISO - International Organization of Standards.

KGI - Key Goal Indicator.

KPI - Key Performance Indicator.

CHAPTER I

INTRODUCTION

1.0. Overview

Chapter one is an introduction to the research and it has seven parts. Part 1.1 is the background of the study. Part 1.2 Introduction about the study area that is the Kenya's devolved county system of governance. Part 1.3 outlines the problem statement of the research. Part 1.4 is the aim of the research, Part 1.5 and Part 1.6 is about the objectives of the study, intends to feature on and Part 1.7 Outlined the significance of the study.

1.1. Background of the Study

Information and the knowledge based on it have increasingly become recognized as information assets, i.e. A business information asset without it the organizations will not achieve its objectives. It is a business enabler, requiring organizations to provide adequate protection for this vital resource.

To realize effectiveness and sustainability in this era of information age with complex and interconnected world, availability of information assets must be addressed at the highest levels of the organization. It should not be regarded as a technical specialty relegated to the IT departments only. Current businesses demands industry specific regulations in most areas of IT including managing information security and associated risks, compliances and Intellectual property. Several tools in terms of frameworks have also been developed to address these challenges.

Kenya National ICT Master Plan 2013/14 - 2017/18 mission statements reads that "To improve the quality of life of Kenyans by ensuring the availability of accessible, universal, affordable, modern and high quality ICT facilities and services within the Country". Ministry of Information Communications and Technology, ICT Master Plan (2014)

The master plan is meant to create e-government policies, legal and regulatory frameworks that are simple and easy to implement and that result in efficiency and effective delivery of ICT services.

The Kenya's Commission of Implementation of Constitution (CIC) in line with its mandate undertook an assessment of the status of implementation of devolution in the counties and came up with a report.

In the report CIC (2014), CIC noted commendable progress that has been realized in the operationalization of devolved systems in particular key institutional structure and systems. However, they noted that there are substantive challenges which have not been addressed and compromises success of devolved government. Part of these challenges are in areas that may influence implementation of ICT policies and regulations and these includes.: Unclear Organizational structure, fear of perceived job insecurity, lack of funding, lack of appropriate legislation to implement functions, lack of capacity and skills , difficult staff retention due to hardship areas, Lack of soft infrastructure Connectivity, Negative attitude of former local counties, long and complicated procurement and associated delays ,Struggle of powers between the Chiefs/Administrators and lack of clear norms and standard and need to harmonize
According to this study, CIC assessment did not go into the details to identify particular policies, plans and regulations. Lack of in-depth analysis indicates attempts to only identifying availability of the documentations rather than applicability and that is only to satisfy the regulatory requirements and not adequate for good governance practice.

As importance of IT grow in enterprise strategy, managing IT also becomes critical. Lack of IT management policies and frameworks etc means organization will be deprived of benefits of the same which are improved business process, service quality, legal or regulatory compliances and other increasingly important strategic corporate goals. Joch (2011) noted that the holistic desire of IT governance become elusive when IT governance becomes complex.

The downside in implementation of most IT management and governance frameworks is that they are more complex in applicability or costly; they tend to be a preserve for only blue chip companies. IT frameworks ought to be simple tool for all types of companies or organizations.

Devolution of governments is a new idea in this country and many other countries in Africa. This scenario of devolving services including Information Technology departments and systems

provides a new unfamiliar scenario with Information systems policy makers in the national government and the implementation team in the counties. Going by the mandate of ICT master plan, what stands out is availability of information systems. In normal circumstances availability is guaranteed by adopting appropriate best IT Service Continuity practices in information systems.

Taking a panoramic view of Kenya's information security landscape there are red flags all over throughout the country especially in the counties. As Kenya Government decentralizes ICT service there are old and emerging threats. Going by recent cases locally and internationally, social and technological threats have been heightened, Kenya is a neighbor to Somali the homeland of Al-shabab, which is a jihadist terrorist group based in Somalia and pledge allegiance to the militant Islamic organization Al-Qaeda. These radicalized groups are fighting Kenya government from all ways and by any all means physically, technologically or otherwise.

In the light of absence of enforced policies and rogue imminent Information in-security looming throughout the counties there is an urgent need to develop structures to protect against any impending disruption.

1.2 Devolved County Governments.

Kenya's Election of year 2013 marked official launch of government decentralization into forty-seven (47) counties with county governments and assemblies. The counties were to form their own institutions.

The constitution also established a state commission called Commission for the Implementation of the Constitution (CIC) to ensure smooth implementation of the 2010 Constitution.

CIC in the assessment report CIC, (2014) concluded that there is a need to establish and review existing policies, legislation in institutions in order to ensure they facilitate improved governance and service delivery. It recommended that both levels of government individually and collectively expedite the development and review of procedures, legislation and polices.

According to Nalo (2007), the role of ICT in Kenya and the reliance on ICT by both government and private sector is increasing rapidly and thus the need to protect the vital information and data held by the various information systems. The government has implemented IFMIS, KRA I-Tax, e-procurement etc. Most of these are already devolved to the county level. The county systems are now connected with national government systems. Implementation of the National Optic Fibre

NOFBI project has eased communication across counties as well as improved government service delivery to the citizens such as issuance of national identity cards and registration of certificates of birth and death. It is expected that by December 2015 all counties will have been connected on NOFBI.

1.3 Problem Statement

Apart from Commission of Implementation of Constitution assessment report CIC, (2014) there exist no other literature on status of IT service continuity or information security of ICT departments in the devolved counties. Secondly, the CIC assessment report was a generalized and not in-depth exercise to establish the actual statuses of ICT policies and regulations and their implementations. If for sure IT is taking centre-stage as business enabler then it ought to be probably managed.

Thirdly, from the study it was deduced that CIC lacked resources in terms of personnel and tools to assess level of IT service continuity and disaster recovery plans in the counties.

In order for the counties to get maximum ROI, ensure security of Information, compliance to regulation, the counties can adopt IT governance and service management tools like best practices, policies and regulations.

Guldentops (2010) asserts that IT Framework in particular helps organizations map the complexities of managing information systems and helps to understand, utilize, implement and direct important information related activities and make more informed decisions through simplified navigation and use.

IT Service Management and IT Governance frameworks in existence include ITIL, COBIT, ISO27000, PRINCE2, COSO etc. but their nature is prescriptive. Zhangx (2013) established that these frameworks do not show how it is done but rather only show what needs or expected out of IT function hence complex and not easy to understand, they lack guidance on implementation that makes them difficult to launch within established IT environments. Further, they are costly and cumbersome to apply in evaluating IT service continuity system in small to medium organization.

1.4 Aim

This research project aims at obtaining a deeper understanding of how Kenya's devolved county governments can ensure IT service continuity from normal and emerging threats without the

dilemma of whether to adopt established internationally recognized frameworks like COBIT and ITIL.

This requires studying of IT service continuity, its significance, role and practice and major existing frameworks.

It attempts to propose a simplified evaluation framework for IT service continuity which addresses technology risks within a county government size of organization.

1.5 Main Objectives.

The main objective is to identify salient IT practices used and establishes an appropriate evaluation framework for ensuring adherence to standard and practices that ensures IT service continuity in the counties.

1.6 Specific Objectives

i. Assess implementation of IT Service Continuity in Kenya's Devolved Counties.

ii. Develop a user friendly and cost effective evaluation framework for IT Service Continuity and Disaster Recovery plan that can be applied to implemented or work-in-progress IT SC/DR processes in Kenya's Devolved Counties and thereby give hints on areas of improvement.

1.7 Significance of the Study.

The study serves to advise interested organization like CIC, ICT-A and County governments on an appropriate evaluation framework for IT Service Continuity and Disaster recovery programmes that can be used to proactively gauge levels of the plans implementation. Secondly, once gauged it can be used to allocate resources where found to be in-adequate.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

The purpose of this literature review is to highlight how critical information security and IT service continuity is as business takes up Information Technology as part of business strategies. It surveys existing IT framework and highlight the disadvantages and how they are impracticable to apply in the County governments. It further brings to fore situational analysis emerging security threats and important factors that need to be addressed at worst case scenario when implementing IT Service continuity strategies in devolved counties in Kenya.

2.1 Information Technology.

Information technology is a type of technology used to produce different applications of computers and computer networked to reducing manual processing hence reducing of errors, increase efficiency, effectiveness and enhances communication speed for the benefit of the mankind.

Some important advantages of information technologies are communications; it is used in developing different types of communicational devices and also enabler of better communications services. Secondly, Globalization; Modern world becomes closer in ways of communication and provides the easy way for faster communication which enhances economy and the profit of different types of businesses and finally creation of new jobs; because of the development of the new technologies it provide opportunity for new generation of people to come in the technical field and generate the technology of the future.

The same information is an asset to the organization. Khan and Wanner (2010) also viewed that organizations are increasingly relying on these Information Technologies to perform various functions in all departments. The factors, when provisioned to satisfactory level, will definitely contribute to achieve organizational goals. However, a most challenging factor encountered in these organizations is the lack of clear and concise enterprise-wide view of organizational IT service continuity.

Layton (2001) agreed that organizations rely on these Information Technologies and System today more than ever before. But unfortunately the same information is being hunted by criminals. Hacktivism and other information related vices are on the rise. There are several motivational

factors that are contributing to their meteorite rise. The development of information superhighways provides fertile grounds for it, increased knowledge is another and there are many more others.

Information security is defined as protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption.

Securing Information technologies and monitoring them for suspicious activity reduces the risk of breaches. Establishing enterprise-wide approach to information security, support by top management, is the best way to protect organizations from information risks.

Bowen et al (2006) argue that addressing these security risks, an organization must implement an information security strategy through the establishment of a framework to enable the development and improvement of an information security program. In particular, information security strategy must support the overall organization's strategic plans with its content clearly traceable to these higher-level sources.

IT and systems risk have always been inherent in any business but information security threats have emerged and persisted and seemed nothing can be done to eradicate. Hossein, (2006).

This therefore calls for some other action plan and for this matter IT continuity and disaster recovery plans that can manage responsibility of increasing resiliency. In turn these strategies can be optimally managed through industry best practices. Included in the IT best practices are various IT frameworks. A pool of the most used IT frameworks and best practices supporting Information systems include: ITIL, Cobit, PMbok, CMMI, ISO 27001, Val IT and eTOM according to Bahshani,Semma2,Semma3(Jan 2015).

2.2 **Overview of Information Security.**

Information Security is something which is a problem of IT department. It involves all main resources and business processes in an organization. Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification in order to provide Confidentiality , Integrity and Availability.(Sewall, 2009) --the common acronym is CIA**.**

Confidentiality is preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is the guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information.

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles.

Brotby, (2008) alluded that information security deals with all aspects of information, whether spoken, written, printed, electronic or relegated to any other medium, and regardless of whether it is being created, viewed, transported, stored or destroyed

Both Information security and IT service continuity are concerned with protecting information technology and systems. Information security focuses partly on the organization's network boundaries, reinforcing it while still permitting approved information to permeate. It guarantees confidentiality, integrity and availability of data through proactive and reactive measures, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS). IT service continuity plans give organizations that rely on IT the ability to remain in business during disasters, economic downturns and bad reputation. IT service continuity plans outlines steps necessary for a company to operate in the wake of a sudden and severe change to market conditions.

A comprehensive IT service continuity plan makes management review of vulnerabilities and threats to their organizations from a remote perspective.

Regardless of the controls in place the organization from physical or logical security threats must have a fallback plan to invoke should a threat materializes. Information Security tries to prevent serious breaches but there must be a continuity plan.

During Business Impact Analysis on IT Service continuity plans, there are security concerns that need to be dealt with for example:

1. Security-dependent applications can be identified in BIA. Then a secure work-around for gaining access to those security-dependent applications has been created; and the work-around has been thoroughly tested.
2. Security concerns of Data drives access should be identified and tested during BIA.

Information security controls is to prevent intrusions , IT Service continuity plan/DRP should be in place and should include technology and systems recovery that will also provide contingency and recovery back to the usual business state, should a breach occur as asserted by (World Insurance Report ISBN: 0306-3445 , 2006).

Ensuring IT service continuity and timely recover of business critical information systems is becoming increasingly important. Since measures to improve continuity of information systems and backup centers often require a huge investment and organizations need to consider cost effectiveness of each measure they plan to take.

2.2.1 Information Security Policies.

The main reasons why an organization implement IS policies is primarily to meet legal compliance and reduce the frequency, duration and cost of information security incidences. (Stahl and Pease ,2011).

How to implement IS Security Policy:

1. Identify organizational issues that impact IS Policy. - IS Policy need to accurately reflect the organization it serves.
2. Identify various classes of Policy Users.- Define roles and responsibilities
3. Organize IS policies into meaningful categories.
4. Review draft policies and Standards with Management, users and legal counsel.
5. Train all Personnel in the organizations IS policies and Standards.
6. Enforce IS Policies and Standards.
7. Review and modify IS policies, Standards at least once annually.

On point 4 above there are several standards that IT groups typically adhere to when developing response strategies. Some of the most common security best practices include NIST, ISO 27001, ISO 15408, and RFC 2196.

2.2.2 Situational Analysis of Information Security in Kenya.

Cybercrime is on the rise locally. This is a criminal activity done using computer and internet and includes anything from stealing money from banks to pirating of software. It also includes offences like creating viruses and distributing pornographic materials.

According to a media report (How Anonymous and other hacktivists are waging war on Kenya 2014), hackers penetrated sites operated by Kenya‘s state secret agents and sensitive security and financial institutions were accessed. The sites include Central Bank of Kenya, Department of Immigration, Kenya government IFMIS, Attorney general’s Office and Kenya Police. While the damage was not much, it illustrates weaknesses in the systems. Internet professionals blamed the government for underestimating the risk and under resourced to deal with it as noted by Souter and Kerretts, (2012).

Cases recently reported involved banks and money transfer services but prediction is that Kenya is yet to witness escalated cases that extend into other sectors like Energy, Transport, regulatory establishments.
In December 2012, Standard Chartered (Kenya) customers were hit by series of attacks where bank accounts were wiped out; forcing the bank to inform customers to reset passwords for their ATM machines (Wanjiku, 2013).

It further wrote that the Real Time Gross Settlement System (RTGS) and other EFT modes intended to deal with fraud, are the most vulnerable.

From the little literature available it can be deduced that the bank did not have a fallback mechanism for this kind of threat. The idea of asking clients to reset password for ATM is a remote control. It implies that there has never been a communication to Customers on the procedure to follow in case this kind of attack happens. The procedure could have appeared in the IT Service Continuity or Business continuity/Disaster recovery plan and communicated clearly to clients. Therefore it indicates that Disaster recovery and Information security are operating independently or non-existent in most organizations.

Kamau (2012), an independent security consultant specializing in penetration tests alluded online banking and mobile banking in Kenya vulnerability to inside fraud activities and said it is because employees are least suspected.

Information security is a moving target. It is high time controls at all levels of government institutions are enforced. Government institutions are more vulnerable and easy target especially now ICT systems are interlinked between counties and central government. This can be made

worse if internal controls are absent. The scenario in counties will be assessed by this study and will be able to establish a likely scenario throughout the country.
The central government owing to established institutions like ICT-A and Cybercrime units the situation could be better.

2.3 **IT Service Continuity Management.**

IT service continuity management (ITSCM) defines the processes that enable IT to work closely with Business Continuity Management to ensure plans and other services are in place. Business continuity management is needed in the event of a significant business disruption according to TeamQuest Corporation, (2015)

ITSCM supports ensures that the required IT technical and service facilities can be resumed within agreed and required business timescales whenever an interruption occurs according to a scholar Sarnovský, M. (2005).

ITSCM is concerned with managing an organization's ability to continue providing a pre-determined and agreed level of IT services to support the minimum business requirements following an interruption to the business.
ITSCM supports the specific IT technical and service requirements.

Differentiating Business Continuity and IT Service Continuity.

IT service continuity is the IT aspect of business continuity. Currently, economics and business processes increasingly rely on ICT Systems and Networks. ICT systems are crucial components of the processes and their safe and timely restoration is very important. If such systems are disrupted, an organization's operations can come to a halt. If the interruption is too serious the business will cease to exist.
Therefore, ITSCM implementation can only be realized with commitment from the senior management. Ongoing maintenance of the recovery capability can be achieved through the following processes;

1. Configuration and Change Management and review process.
2. Education and awareness for the whole organization.

3. Utilizing the latest technology and software supporting tools.
4. Personnel training involved in the process.
5. Regular drill and tests.

IT service continuity and disaster recovery plans provide detailed strategies on how the business will continue after severe business interruptions and disasters.

Scope of ITSCM.
The scope considerations of ITSCM are listed below (Schlichtherle, 2011):

1. Technology dependency.
2. Organization geographical location
3. Critical business processes and the level of integration between them
4. Services that need to be provided to the business to support those critical business processes
5. Any limitations in the provision of ITSCM mechanisms (e.g. Cost of downtime)
6. Organization Risk Management view.

ITSCM Risk Management.
When a Risk Analysis is undertaken it is possible to determine appropriate countermeasures or risk reduction measures. Listed below are some risks and threats that can be considered in the context of ITSCM.

Table 1 - Risk / Threats
Source:

Risk	**Threat**
Loss of internal IT systems/networks, PABXs, ACDs, etc.	Fire Power failure Arson and vandalism Flood Aircraft impact Weather damage, e.g., hurricane Environmental disaster Terrorist attack Sabotage Catastrophic failure Electrical damage, e.g. lighting Accidental damage Poor quality software
Loss of external IT systems/networks, e.g., e-commerce servers, cryptographic systems, etc.	All of the above Excessive demand for services Denial of service attack, e.g. against an Internet firewall Technical failure, e.g. cryptographic systems
Loss of data	Technical failure Human error Viruses, malicious software, e.g. attack applets

Loss of network services	Damage or denial of access to network Service providers' premises Loss of service provider's IT systems/networks Loss of service provider's data Failure of the service providers
Unavailability of key technical and support staff	Industrial action Denial of access to premises Resignation Sickness/Injury Transport difficulties
Failure of service providers, e.g. outsourced IT	Commercial failure, e.g. insolvency Denial of access to premises Unavailability of service provider's staff Failure to meet contractual service levels

IT Service Continuity Management in Kenya Devolved Counties.

KPMG (2012) survey conducted in year 2012 concluded that IT and Infrastructure disruptions, Corruption, Cyber attacks and Fire are African business leaders' main concerns in Africa. Terrorism is the lowest with 2.3/4.0 index, the former is leading at 3.48/4.0.

IT and infrastructure continuity in organizations is achieved through deployment of business continuity plans, Processes, Controls, Technology, Data and Business resumption planning.

CIC (7, 2014) report identified various policies, plans and regulations mentioned in various counties. A total of 53 policies, 8 plans and 11 regulations were reported to have been in various stages of development. But the detailed of specific documents or even the specific counties where those documents are located were not indicated.

Table 2 - Plans, Policies and Standards count in Counties
Source - CIC Assessment Report (7, 2004)

Documents	Completed	WIP	Total
Policies	8	45	53
Plans	4	4	8
Regulations	5	6	11

The literature review could not establish which of the documents belong to ICT departments in the visited counties.

2.3.1 Benefits of IT Service Continuity.

2.3.1.1. Minimizing disruption in IT services following a major interruption or disaster

2.3.1.2. Minimizing costs associated with recovery plans through proper proactive planning and testing.

Properly prioritizing the recovery of IT services by working closely with BCM and service level management (SLM).

Lapkiewicz (2002) noted that the overall goals of a business continuity plans are to maintain confidence in the business by all external constituents including clients, partners and regulatory bodies. Others are listed as

1. Provides competitive advantage in terms of reliability.
2. Ensures supply chain security and order fulfillment
3. Enhance resiliency.
4. Potential life saving.
5. Provide compliance benefits like cheap insurance.

2.3.2 **Evolution of IT Service Continuity.**

Trying to look back on evolution of IT service continuity, the 1980s saw the recovery sites being initiated by profit making entities to offer shared services. Later in 1990s due to advancement in IT it changed gradually from Disaster Recovery plan (DRP) to Business continuity planning (BCP). Gallagher (2003) noted. Despite the development this study is narrowing in on ITSCM as a component of BCM.

Before 9/11, capability of an organization to recover from a disaster was related to the disaster recovery plan but after that it became profound for organizations to implement disaster recovery plans.

<u>Significance of Disaster Recovery protection</u>

1. Data backup and recovery.
2. Enabled fast recovery of files and email to resume business as quickly as possible.
3. Virtualization of failed servers reduces downtime from days to hours.
4. Remote offsite storage ensures data security and compliance.
5. Built-in archiving is more cost-effective and reliable than tape.
6. 24/7 monitoring and management ensures data integrity.

2.3.3 **Components of IT Service Continuity.**

There are four major components of IT SC that stand out. A successful IT Service Continuity program should be:

1. Sponsored – Requires support, involvement and funding—from the executive management team.
2. Accountable - Organizations with successful programs hold managers accountable
3. Prioritized - Continuity planning is impact driven. Successful programs have standards that focus more attention on those areas of the organization that pose the greater risk.
4. Continuous - The continuity program is a continuous process requiring regular review, planning, and updating commensurate with the degree of change within a facility.

IT SC /DR program goal is that unless a program achieves the fundamentals of being sponsored, accountable, prioritized and continuous, its ultimate purpose to keep the services running is more difficult to achieve.

2.4 **Developing IT Service Continuity/DR Plan.**

Key steps in developing the Plan

When developing an IT continuity strategy there are standards that are used. Some of the common information security practices like NIST and ISO 27001 may be inadequate in making organization determine impacts and appropriate decisions. Therefore, the input of experts is paramount in developing plan specific to an industry or organization.

NIST SP 800-34 defines various types of IT contingency plans that includes BCPs and DRPs. It also outlines a six step planning process for creating contingency plans to be:

1. Develop the Contingency Planning Policy Statement
2. Conduct the Business Impact Analysis (BIA)
3. Identify Preventative Controls
4. Create Contingency Strategies
5. Plan Testing, Training and Exercises
6. Plan Maintenance.

While developing Continuity plan, AT&T Knowledge ventures (2006) underscore three key useful measurements that fall on the critical path.

(1) Recovery Time Objective (RTO) – It is the amount of time the business will be out of order.

(2) Recovery Point Objective (RPO) – It is a measure of how much data is at risk incase a disaster materializes.

(3) Level of Service (LOS) – It is a combination of throughput and functionality, and is an indicator of what services are essential.

2.5 IT Service Continuity Best Practices.

Best practices and procedures are established to create value and minimize risk. It is achieved through implementation of IT control frameworks.

A framework is a real or conceptual structure that guides expansion of a structure into a more useful form whatis.techtarget.com (2015).

In Information Technology a framework is layered structure showing what kind of programmes that can be built and how they interrelate. It may be a set of functions within other systems.

According to Microsoft Tech Centre, 2015 the following are best practices in a Microsoft Exchange environment. They seem to reflect as standard best practices for other systems.

1 Carry out Business Impact Analysis.

2 Carry out Risk Analysis. Identify the threats and vulnerabilities and develop appropriate mitigation strategies.

3 Work closely with IT and the business to agree upon the contents of the plan, and ensure that risks and recovery times are understood and accepted.

4 Define and document procedures for the invocation of a disaster recovery plan.

5 Work closely with the service monitoring and control (SMC), service desk and incident management teams to define interfaces and hand-offs between processes.

6 Define and document procedures for "return to base," following the invocation of a disaster recovery plan.

7 Define, document, and implement a process by which the service continuity plans are reviewed as a result of changes to the services, such as if critical components change.

8 Define, document, and implement a backup strategy for critical data.

9 Develop a testing schedule. Conduct tests at least every six months and after the implementation of major changes.

10 Define, document, and implement a process by which service continuity tests are reviewed
11 Work closely with the technical support teams in the organization to ensure that sufficient technical documentation exists to recover critical components in the event of a disaster

Kirva (2004) argue that Business continuity programmes are many and the reason for this high number is the fact that recognition of the value of business continuity is brought up by more countries establishing their own standards and practices.

He said that many standards are prescriptive on the fact that the standards only describe what should be done rather than describe how each activity is to be implemented and this is usually at the discretion of the organization.

Each of the standards and frameworks addresses a BCP issues, but a few of them provide any real instructions as to how to plan and implement a BC program. To gain more inside we narrow down into our specific area of IT frameworks next.

2.6 **IT Service Management Frameworks.**

Every department in organizations these days are being forced to consider new areas of optimization, and IT is no exception (IT-Software.com, 2012)

According to Kozina (2009) COBIT and ITIL are specific frameworks that are widely used in managing IT in business. Others include COSO, ISO 2000 and PRINCE2. In this study we will look at two of them, ITIL and COBIT because of they are popular in applicability. But ITIL is the one that is particularly used as IT service management whereas COBIT is an IT governance framework.

Usage of existing IT Frameworks.

IT Governance Institute's status report of 2011 on the frameworks indicates that ITIL and ISO 2000 are ahead of the rest in usage. Refer to performance indicator in percentages since year 2006 in Figure 2.

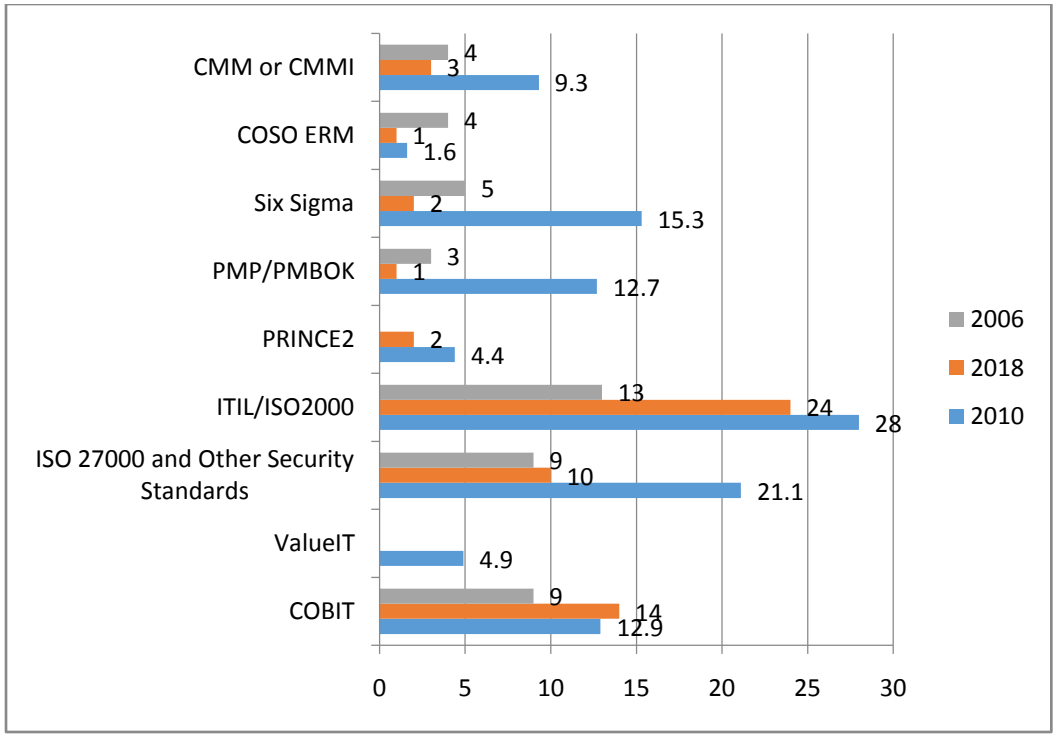


Figure 2.6-1 Trends in Usage of IT Frameworks
Source: ITGI: Global Status Report on the Governance of Enterprise IT (GEIT)-2011

ITIL is leading and its growth is progressive whereas adoption of COBIT is declining. Use of ISO 2700 is also progressive; this can be attributed to ever rising threats in Information Security.

2.6.1 **COBIT**

COBIT is published by ITGI and it provides a maturity model that includes the following component.

1. Framework
2. Control Objectives
3. Management guidelines
4. Maturity Models.

COBIT Framework.

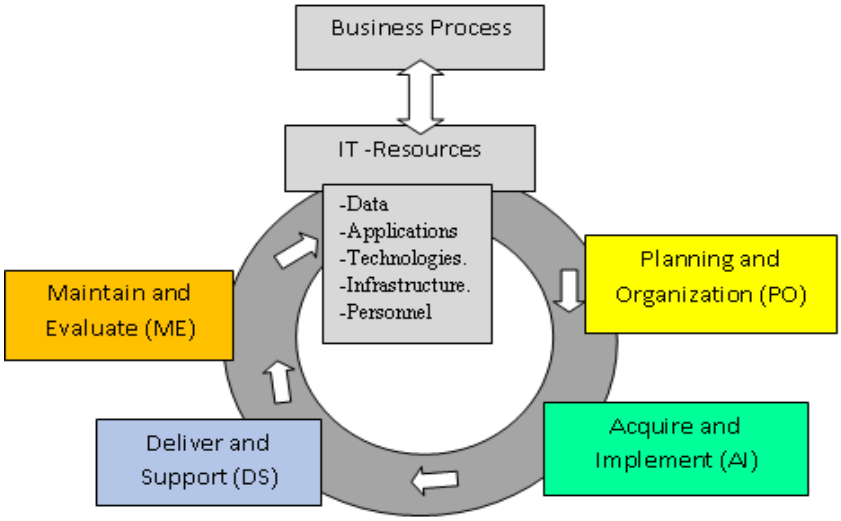


Figure 0-3 - COBIT Core Concepts.
Source: ITGI, www.itgi.org

COBIT helps management in managing ICT investments throughout lifecycle and provides a process to assess whether IT services and related activities achieve business objectives and are to deliver the intended goals. However there are also disadvantages in applicability to some organizations.

Disadvantages of COBIT as noted by Simonsson, Johnson and Wijkström (2007)

(a) It has a lot of criteria and it requires experts to implement it effectively.

(b) There are 34 IT processes with 222 control objectives and more than 300 KPIs and KGIs hence satisfying all these can be a challenge.

(c) It requires a great deal of knowledge to understand from both sides business and IT.

(d) There are no details about how processes should be implemented to support internal controls.

(e) ITGI and ISACA claim many advantages but there are neither industrial nor academic statistics nor studies supporting it.

2.6.2 ITIL

ITIL is a standard published by UK government and consist of best practices for managing IT services in organizations. Its main components are;

1. Service Strategy
2. Service Design
3. Service Transition.
4. Service Operation
5. Continual Improvement

ITIL Model.

It is outlined in IT Service Continuity Management (ITSCM) and consists of the following processes.

(a) Requirements and Strategy:
   a. Business Impact Assessment
   b. Risk Assessment

(b) Business Continuity Implementation:
   a. Develop Interim Operational Plan
   b. Develop Recovery Plans.
   c. Develop procedures

(c) Management:
   a. Education and awareness
   b. Review and audit
   c. Testing
   d. Training
   e. Assurance.

Disadvantages of ITIL.

1. Processes are many and it tends to take long time on implementation and require significant effort and costs.
   SS- 13, SD-21, ST-14, SO-19, CSI – 20 == (Total = 87 Processes).

In addition to an introduction volume describing rationale for lifecycles and key principles in each life cycle stage.

2. Continuous improvement of service and cost reduction is insufficiently visible.
3. For it to be successful the implementation would require involvement of all levels of organization.

With respect to implementing Information Systems continuity, at the county level, ICT departments have not matured enough to the level of using COBIT and ITIL. Implementation for these internationally recognized frameworks is a complex process for Kenya County governments. It would require a lot of resources in terms of training personnel and budget to procure necessary resources.

ITIL and COBIT processes aligned together are tabulated in table 2. Here we focused only on processed the deals with Information Systems Continuity. Because of similarities of processes there are some which overlap. Therefore implementing the overlapping processes in unison and adding the unique one will worsen and make it even more expensive and would not be practicable for small/medium IT setup. It becomes a preserve of big companies with financial muscle. Zhang (2013) noted that these two ITIL and COBIT can be implemented separately or can be combined. Mingay and Bittinger(June 2002) agree that combining ITIL and COBIT will create a stronger IT governance environment.

Table 3 - Mapping of ITIL and COBIT
Source: ISACA

COBIT		ITIL
Control Objective	**Name**	**Processes**
DS4	Ensure Continuous Service	SO 4.6.8 IT Service Continuity management.
DS4.1	IT continuity framework	SD 4.5 IT service continuity management
		SD 4.5.5.1 Stage 1 – Initiation
		CSI 5.6.3 IT service continuity management
DS4.2	IT continuity Plans	SD 4.5.5.2 Stage 2 - Requirements and Strategy
		SD 4.5.5.3 Stage 3 – Implementation
DS4.3	Critical IT resources	SD 4.4.5.2 The proactive activities of availability management
		SD 4.5.5.4 Stage 4 - On going operation.
DS4.4	Maintenance of the IT continuity plan	SD 4.5.5.1 Stage 4 - on going operation

DS4.5	Testing of the IT continuity plan	SD 4.5.5.3 Stage 3 – Implementation
		SD 4.5.5.4 Stage 4 - On going operation.
DS4.6	IT continuity plan Training	SD 4.5.5.3 Stage 3 – Implementation
		SD 4.5.5.4 Stage 4 - On going operation.
DS4.7	Distribution of IT continuity plan	SD 4.5.5.3 Stage 3 – Implementation
		SD 4.5.5.4 Stage 4 - On going operation.
DS4.8	IT service recovery and resumption	SD 4.4.5.2 The proactive activities of availability management
		SD 4.5.5.4 Stage 4 - On going operation.
DS4.9	Offsite backup Storage	SD 4.5.5.2 Stage 2 - Requirements and Strategy
		SO 5.2.3 Backup and restore
DS4.10	Post-Resumption review	SD 4.5.5.3 Stage 3 – Implementation
		SD 4.5.5.4 Stage 4 - On going operation.

Table 4 - COBIT and ITIL Processes Abbreviation

Source: Author (2015)

COBIT Domains	ITIL processes
PO-Plan and Organize AI- Acquire and Implement DS – Deliver and Support M-Monitor	SS-Service Strategy SD-Service Design ST-Service Transition. SO-Service Operation CSI - Continual Improvement

2.7 **Proposed Evaluation Framework for IT Service Continuity/DR plan in Kenya's County government.**

According to Gartner and Holub (2015) in developing IT excellence, organizations pursue IT operation optimization through implementation of established frameworks in five principles listed as follows

1. Strategize and Plan - Draw Charters to synchronize with vision and align with business goals.
2. Develop Governance - Establish decision making channels and agree on flow.
3. Drive change management - Get buy-in from stakeholders.
4. Execute - Optimally operate in accordance with business objectives.
5. Measure and Improve - measure outcome, seek feedback and drive improvement processes.

To be able to develop an appropriate framework befitting Kenya's county governments, the above five principles serve to guide the selection of features into Demining cycle model of Plan, Do, Act and Check and leverage on the disadvantages of internationally recognized frameworks like COBIT and ITIL.

The Deming Cycle is a systematic series of steps for gaining valuable learning and knowledge in Quality Control in a production environment. Sometimes referred to as Deming Wheel, or PDCA Cycle, the concept and application is the brain child of Walter Shewahart but Dr Deming popularized it. Both were at Bell Laboratories in New York.(Moen and Norman,2010)

According to Wing S. Chow, Wai On Ha, (2009) the determinants of the critical success factor for disaster recovery planning for information systems are as listed below.

1 DRP policy and goals.
2 DRP documentations.
3 DRP steering committee.
4 DRP testing,
5 DRP training.
6 DRP maintenance and staff involvement.
7 DRP minimum IS processing requirements.
8 Top management commitment to DRP.
9 Prioritization IS functions/services.
10 External, off-site back-up system, and internal
11 On-site back-up system.

This study define evaluation framework based on Critical Success Factors (CSFs) of Continuity and Disaster recovery plans identified by Barbara (2006) and this study fitted them into different phases of the Deming cycle. The overall evaluation framework is depicted in figure 0-3.

Critical success factor (CSF) are elements that are necessary for an organization or project to achieve its mission Gates, Linder (2010).

Based on the Deming lifecycle aspects the identified CSF followed the evaluations criteria step by step from Plan, DO, ACT and Check.

According to PWC, (2012) report, IT and Infrastructure disruptions is leading as a major threat to businesses. This shows that much effort is needed to look into solutions to address this disruption factor.

Table 5 - CSF for Continuity Plans and Disaster Recovery
Source - Barbara (2006)

SNo.	CSF	PDCA Stage
1	Top Management Committed.	PLAN
2	Adequate Financial support.	PLAN
3	Alignment of Disaster Recovery Planning Objectives.	PLAN
4	Adoption of Projects Management Techniques	PLAN
5	Presence of Formal Recovery Planning Committee.	PLAN
6	Participate of Respective from each Department	PLAN
7	Engagement of External Consultant	DO
8	Risk Assessment and Impact Analysis.	DO
9	Determination of Maximum Allowable Downtime.	DO
10	Prioritization of IS Applications.	DO
11	Off-site Storage of Backup.	DO
12	Presence of Emergency Response Procedures.	DO
13	Training of Recovery Personnel.	DO
14	Appropriate Backup Site.	DO
15	Periodical Testing of (Business Continuity/Disaster Recovery) Plan.	CHECK
16	Maintenance of (Business Continuity/Disaster Recovery) Plan.	ACT
17	Insurance Coverage for IS Loss.	PLAN
18	Effective Communication.	DO
19	Service level Agreement.	CHECK
20	BC/DR Implementation Plan & Templates.	CHECK

Almen and Rosqvist (2008) agree that the way to minimize risk in an organization is to concentrate on the worst case scenario hence in order to keep it simple the proposed IT SC/DR framework selected worst case scenario factors within the CSFs. The factors selected are as follows:

PLAN

An Enterprise-wide key success word is access to the decision-makers, budgetary allocation funding, resource allocation and technological capabilities (Dato, 2002).

1. Top Management Support
2. Budget Allocation
3. Team Planning and Composition

DO.

1. Emergency Responses.
2. Team Co-ordination
3. Metrics

CHECK

1. Frequency of Conducting IT continuity planning and Disaster Recovery planning.
2. Tests for Worst case scenario.

ACT

IT Service continuity planning should be periodically updated to reflect and respond to changes in the institution.

1. Lessons Learned.
2. Plan review procedures.

The proposed framework is designed to achieve simplistic approach while achieving the objective of evaluating credibly IT service continuity initiative in the county governments ICT departments.

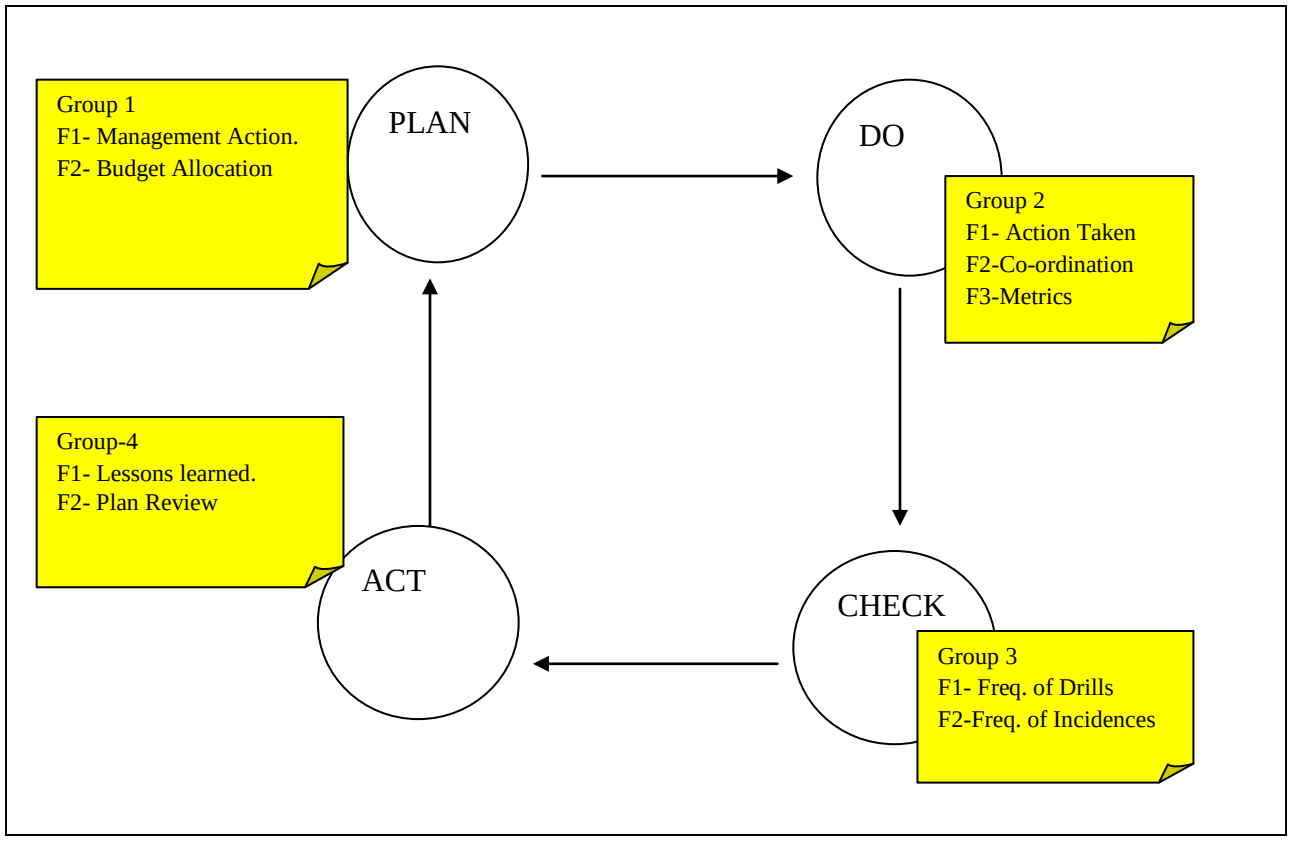


Figure 2.7-1 - Proposed Evaluation Framework

Businesses or organizations that do not adhere to these CSFs when implementing Continuity plans are likely to end–up not implementing them in totality. Recent reports published by Heather (2011) indicate that as many as half of SMBs lack a business continuity or disaster recovery plan. Those that formulated plans often discover they lack critical information or coverage when a disaster strikes therefore this implies that they lack understanding of CSFs.

Key Issues, Challenges and Resolutions of Implementing Continuity Plans.

The key issues and challenges in implementing Continuity Plans projects revolve around four major areas:

1. Senior management commitment and involvement
2. Lack of thorough understanding of the data dynamics and dependencies involved in data Recovery by Continuity practitioners.
3. Inappropriate approach in executing continuity processes
4. Incorrect and/or inappropriate assumptions in formulating IT SC/DR.

CHAPTER III

RESEARCH METHODOLOGY.

3.0 Overview

This chapter discusses the methodology of the research and identification of research aspects. Therefore the chapter is divided into 6 sections. (3.1.0) Research Design, (3.1.1) Population (3.1.2) Sample (3.1.3) Data Collection (3.1.4) Data Analysis (3.1.5) Structure of the interview.

3.1 Research Methodology.

A research process is a set defined as connected multi-steps procedures required to complete a research project.

3.1.0 Research Design

From the previous discussion and based on the available literature of IT service continuity which enabled the researcher to define the research variables and having the research objectives this research was conducted as survey of qualitative and quantitative nature.

The main reason that led to selection of this method is actually one of the objectives of this research and that was to assess IT Continuity Plans. The research was to select a sample from a population. Selecting a few counties from a population of 47 counties. Secondly, it needed to ensure validity and thirdly it needed analysis of results and finally in continuity processes surveys help to identify expectations and determines specific areas for improvement.

In survey method research, participants answer questions administered through interviews or questionnaires. After participants answer the questions, researchers describe the responses given according to Jackson (2009).The researcher used questionnaires as data collection instruments. In this study data was collected and analyzed to provide information which in turn used to describe and interpret current events. In addition, it was useful in studying the relationship between variables already mentioned in the evaluation framework.

3.1.1 Population Selection

A population is a group of things that shares similar traits or characteristics whereas a sample is a subset of the population. In this study the population was forty seven (47) County governments. The selected sample was based on geographic distribution of the regions and accessibility

consideration. The regions being the former provincial administration regions namely: Central, Coast, Western, North Eastern, Eastern, Western, Nyanza and Rift Valley.

Table 6 - Population Selection

Region	No of Counties
Nairobi	1
Coast	6
North Eastern	3
Eastern	8
Central	5
Rift Valley	14
Western	4
Nyanza	6
Total	**47**

3.1.2 Sample Selection

A social sciences research involves determining the "population" and "sample". A population is a group that has characteristics and the sample is the subset of that population from where the evidence is collected from.

Purposive research is form of non-probability sampling in which decisions concerning the individuals to be included in the sample are taken by the researcher (Jupp, 2006) and depend on a number of characteristics include the subject matter and willingness of that individual to participate in the research.

In picking the sample interviewee and the counties the researcher used purposive sampling and random sampling methods with consideration of security and logistical reasons

The questionnaire was filled by ICT personnel in the station. This selection is because it is their responsibility to manage IT Service Continuity plans.

In selecting the Counties, regions like North Eastern has zero sample selected because of in-security experienced at the time of the research and also accessibility in terms of road infrastructure. Secondly, many samples were selected in Rift valley because of expansiveness of the region with 14 counties and also to compensate for the North Eastern. The researcher target was to get feedback from at least 10% of the entire population. 10% of 47 is 5 Counties but a sample of ten (10) Counties was selected purposively this being a purposive selection based on the stated logistical concerns mentioned above.

Table 7 - Sample Design

Region	No of Population	Target No. of Sample	% of Sample
Nairobi	1	1	10
Coast	6	1	10
North Eastern	3	0	0
Eastern	8	2	20
Central	5	1	10
Rift Valley	14	3	30
Western	4	1	10
Nyanza	6	1	10
Total	47	10	100

3.1.3 Data Collection

According to Wikipedia Data (2015) data is a set of values of qualitative or quantitative variables. It is measured, collected, reported, analyzed and can be visualized using graphs and images.

Primary data are those that are collected a fresh and for the first time and happen to be original in nature (Kothari, 2004). Secondary data is that has been collected previously by other scholars.

Data can be obtained from primary sources or secondary sources. Each of these sources has got pros and cons. Saunders et al, (2000) too agrees that use of both is recommended. Therefore based on this and to gain the advantage of both primary and secondary methods will be employed in this research.

For the purpose of this research primary data was collected because that is what shows as is situation i.e. things currently in existence and therefore more accurate. Secondary data could not be obtained because of sensitivity of information. They declined to provide reports and periodicals.

The primary data was obtained from ICT personnel in the county; Chief ICT officers (IT Managers), Systems Administrator, Business Analyst, etc in various counties in the selected sample space. Where there was no Chief IT Officer/ICT Director, an officer in charge was the respondent. The response of the ICT Director/Chief ICT (Manager) is most important because of the overall responsibility.

The question's group in terms of PDCA was not made known to the respondents. They were asked discretely to give precise answers and other comments were given where necessary.

3.1.4 Data Analysis and Procedures

Analysis of all the collected data generated information that was desirable. This involves summarization of data that in turn resulted in fewer data, patterns and involves applications of statistical techniques. The analyses employed tools like Statistical Package for Social Scientist (SPSS), Microsoft excel, Microsoft Visio and graphs.

Quantitative studies rely on quantitative data including numbers and figures that can be obtained using administered questionnaires.

Qualitative researches rely on the subjectivity of the matter and judgmental knowledge of the researcher.

The questionnaire as study tool was standardized using 10 respondents regions and found to be 42 suitable for the study. In the 10 regions the structured questionnaires where interviewer administered to motivate respondents to complete the entire questionnaire and provide relevant data, according to (Ihab Hanna, 2012).

SECTION A: Respondent Profile.

The study seeks to find out respondents' profile in terms of designation, level of education and years of experience.

The response will highlight whether the county has right personnel responsible for IT Service Continuity/DR Plans.

SECTION B: Assessment of Implementation of IT Service Continuity/DR Plans in the County.

This section interrogates various aspect of IT Service Continuity planning randomly.

It test existence of IT Service Continuity plans, existence of disruptions, existence of threats, interrogates if risk assessment is done and intend to establish of awareness of any of the IT framework used.

SECTION C: IT Service Continuity and DR Plan CSF for Proposed Framework.

This section seeks to test the proposed framework. The questionnaire has been categories into Plan, Do, Check and Act as per the framework but will not be revealed in the interviewee on the questionnaire. The factors under consideration are Critical Success Factors (CSF) for implementation of IT Service Continuity Plan in Small to medium size IT department the size of County government IT office.

CHAPTER IV

DATA ANALYSIS, FINDINGS AND INTERPRETATION.

4.0 Introduction

This chapter presents analysis and findings of the study. This study finding is presented on IT Service Continuity and Disaster recovery in Devolved counties in Kenya.

The data was collected through questionnaire designed to meet the objectives of the study.

This section interrogates various aspect of IT Service Continuity planning and DR plan.

It test existence of IT Service Continuity plans, existence of disruptions, existence of threats, interrogates risk assessment and intend to develop evaluation framework and test with existing processes.

4.0.0 Response Rate

The study targeted 10 Counties out of 47 in the whole country.

There were 42 structured questionnaires were administered to the county staff according to their responsibility. The distribution of respondents is depicted in Figure 4.0. The questionnaire was filled in and returned by 9 out of 10 respondents, resulting in a response rate of 90%.

4.0.1 Data Analysis

4.0.1.0 Structure of the Interview

Quantitative research involves numerical analysis of data and enables the use of statistical Procedures to answer research questions about relationships and differences between measured variables (Ghauri and Gronhaug, 2005). Quantitative studies rely on quantitative data including numbers and figures that can be obtained using administered questionnaires. Qualitative researches rely on the subjectivity of the matter and judgmental knowledge of the researcher. The questionnaire as study tool was standardized using 10 respondents regions and found to be 42 suitable for the study. In the 10 regions the structured questionnaires where interviewer administered to motivate respondents to complete the entire questionnaire and provide relevant data, according to (Ihab Hanna, 2012).

4.0.1.1 Results

Results obtained from each question are analyzed to see if the counties responses are similar to internals standards. Responses on the PCDCA clusters/groupings are analyzed to see how counties performed under the group.

Summarized results with the responses count and the response percentages are detailed in the next Chapter.

4.0.1.2 Respondent's Profile

The study established the respondents' profile in terms of gender, age, education level, duration in Service and job designations, all the respondents were male between 21 to 44 years of age. Majority being age 33-38 (43%), 21-26 years were 29% and 39-44 years were 29%.

Academically most respondents were of graduate level at 60%, postgraduate were second at 30% and Diploma holder were 10%.

On Job designation most of the respondents were CIO/IT In-Charge (37%), followed by Systems Administrator (36%), Software Support Staff (18%) and the rest were Hardware Support staff (9%) and there were none of Systems Analyst or Business Continuity Administrator.

The distribution of the respondent's job description is as shown in Figure 4

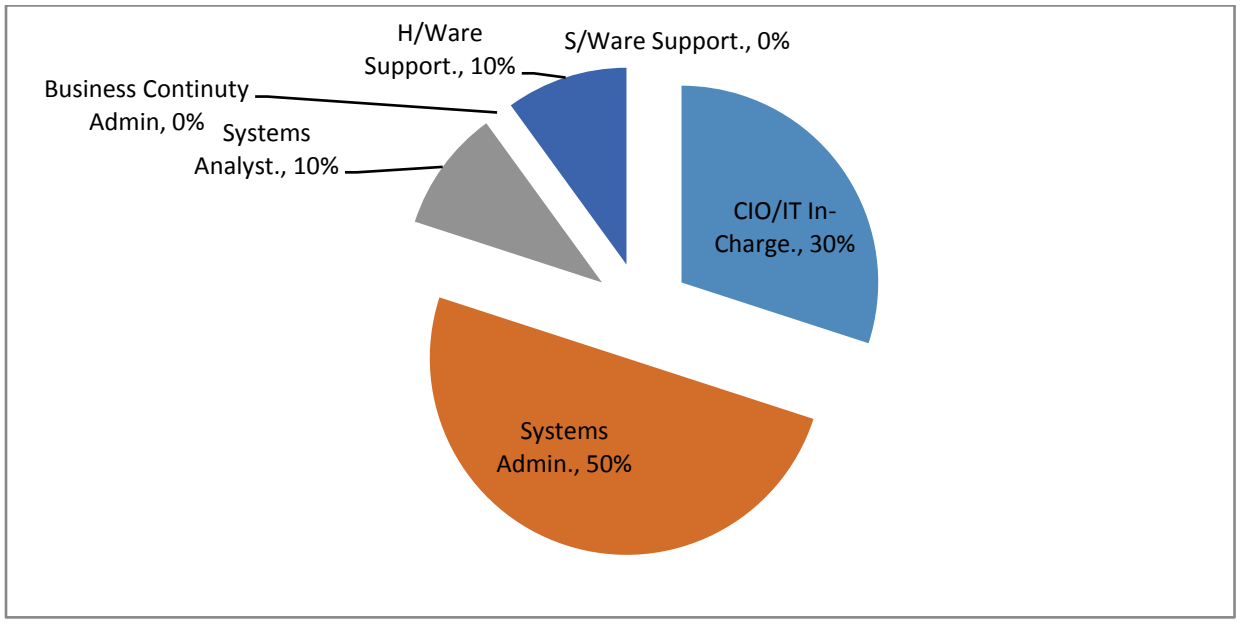


Figure 4.0.1.2-1 - Respondents' Designation

The percentage informed decisions on respondents profile and also objective response on roles and responsibility in understanding and implementation of IT Service Continuity. The CIO/In Charge are responsible for these plans and Systems Administrators are normally the implementers.

Evaluating how long the respondents has worked at the County is also important, the study found that 40% of the respondents has been in the county for a duration of 3-5 years ,those who have worked for 0- 2 years followed with 30% and 6-9 years and 10+ year were 10% and 20% respectively. This is important because the study need to establish some facts on past experiences on IT disruption. And also to validate the fact that the formation of the County governments is only about four (4) years ago. This is depicted in Table 4.1 and Figure 5.

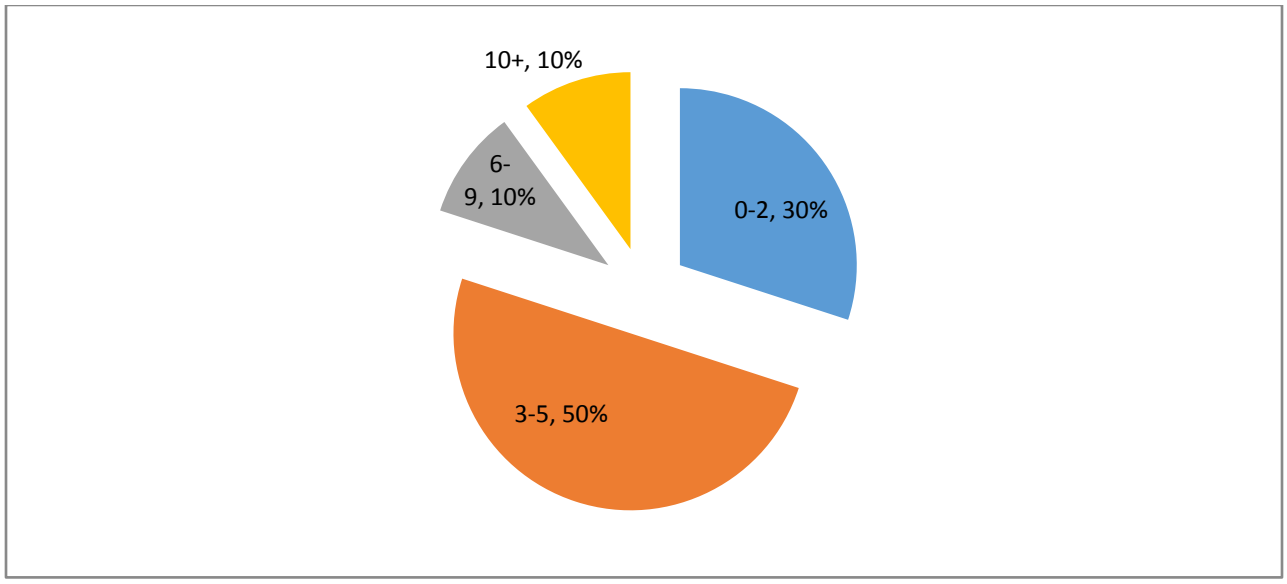


Figure 4.0.1.2-2 - Respondents' Years in Service

Table 4.1- Period the respondents have worked in the County.

Duration in Service	Count	Percentage
0-2	3	30%
3-5	4	40%
6-9	1	10%

10+	2	20%
		100 %

4.1 Assessment of IT Service Continuity/DR Plan in the Counties,

Existence of ITSC / DR Plan and Coverage

To establish the existence of ITSC/DR plan in the counties, the respondents were asked to either tick 'yes' or "no" or "partially" on whether they are aware of existence of the plan(s) . It was found that half of the respondents (50%, n = 5) agreed that there exist ITSC/DR plan in their respective counties. A third (30%, n=3) of them answered partially and 20%, n= 2 said the plan do not exist in their counties.

This indicates that half of the counties are responsible; they take seriously IT continuity services.

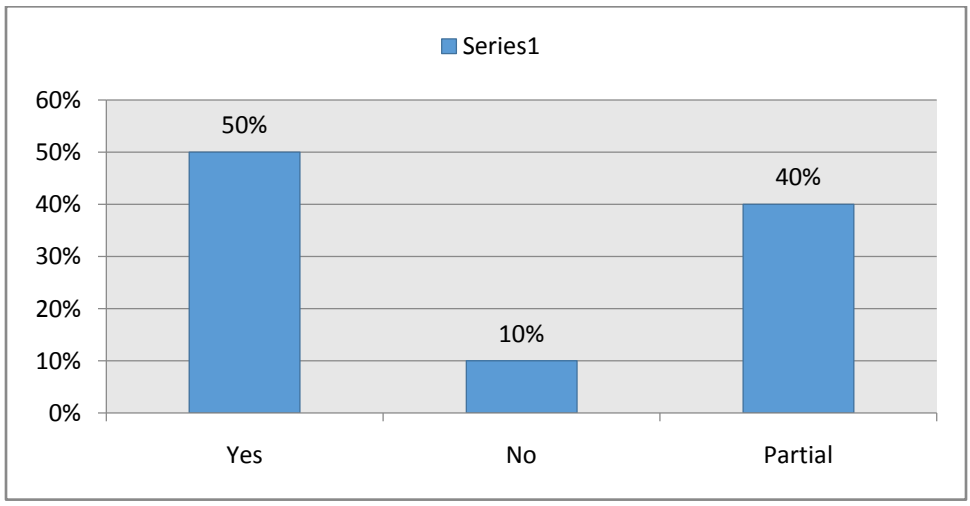


Figure 4.1-1 - Existence of ITSC/DR Plan

On scope on coverage of ITSC / DR Plan, most respondents have indicated their plans covers Fire (19%), Loss of Site (19%), Loss of IT Capacity (15%), Loss of people and Loss of communication each is at (12%), Loss of Skills and Environmental liability at (8%) each, Terrorism damage and Negative publicity each at (4%), whereas due to Protest Group is (0 %) (none). This indicates that Fire and loss of site are highly regarded as the cause of loss to IT Services. This also informs the

fact that decision makers need to put more emphasis on Fire preventative measures and availability of Site at all levels including strategic planning and budget allocation. See representation on Figure 6 below.

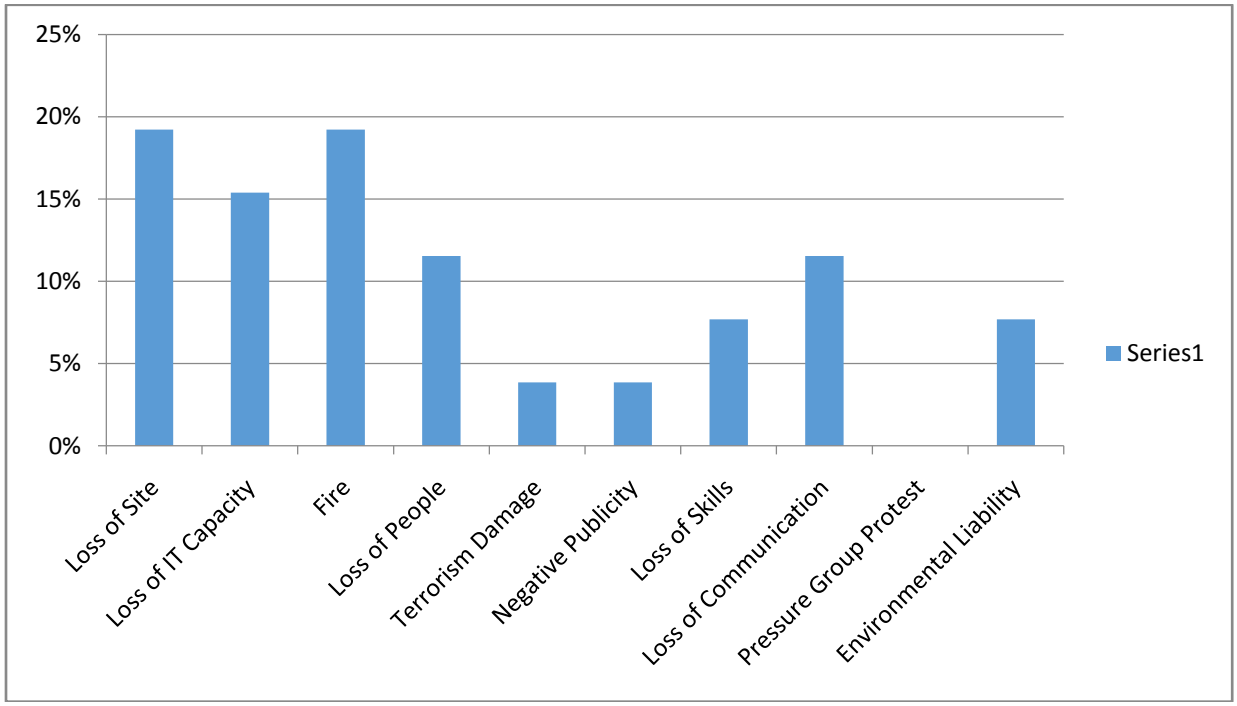


Figure 4.1-2 - ITSC/DR Plan Coverage

Past Experience of threats and Extent of disruption

Asked which threats have they experienced in the recent past. Unplanned IT and Telecomm outage and Interruption of Utility supply responses were the highest with 27% each. Data breaches, new laws and regulations and Loss of IT skills were 8%, Fire incidents, Security incident and Loss of Site each at 4%.

This shows that unplanned IT and Telecomm outage and Supply of utility are most rampant and have caused losses to IT departments in the counties and need to be given more attention. This would mean deploy redundancy equipment and Networks to mitigate the outages. Whenever third parties are involve proper contracts and Service levels agreement need to be in place and enforced.

Extend of disruption 88% consider human error as modest, 13% said it is non-existence, and neither as severe nor serious. Act of Terrorism, 63% of respondents said it is non-existence, 25% said it is severe and 13% as said it is modest, Power fluctuation/Failures 38% said it is serious , another 38% said it is non-existence and 25% indicated it is modest .

Computer viruses, 56% indicated it is modest, 33 % said serious, and 11 % showed it is severe.

This outcome indicates that Computer viruses have caused more damage than any other threat followed by Power Outages and Act of Terrorism in places that have occurred. More resources need to be allocated to Data security i.e. deploy good antivirus protections and employ qualified personnel. Also Power redundancies need to be implemented. There is need to ensure clean and continuous power supply to IT equipment.

Table 8 - Recently Experienced Threats

Threats Experienced Recently	Respondents Count	Percentage
Unplanned IT and Telecom Outage	7	27%
Cyber Attack	0	0%
Data Breach	3	12%
Adverse Whether	2	8%
Interruption to utility Supply	7	27%
Fire	1	4%
Security Incident	1	4%
Health and Safety Incident	0	0%
Act of Terrorism	0	0%
New laws or Regulations	2	8%
Loss of site	1	4%
Loss of IT Capacity	0	0%

Loss of Skills	2	8%
Military Strike	0	0%
Pressure group Protest	0	0%
Others	0	0%
Total	26	100%

Table 9 - Extent of Disruption caused by Threats

Threats	Count	Percentage
Computer Viruses		
Severe	1	11%
Serious	3	33%
Modest	5	56%
Non-existence	0	0%
Don't Know	0	0%
	9	**100%**
Power Fluctuation/Failures		
Severe	0	0%
Serious	3	38%
Modest	2	25%
Non-existence	3	38%
Don't Know	0	0%
	8	**100%**
Act of Terrorism		
Severe	2	25%
Serious	0	0%
Modest	1	13%
Non-existence	5	63%

Don’t Know	0	0%
	8	**100%**
Human Error		
Severe	0	0%
Serious	0	0%
Modest	7	88%
Non-existence	1	13%
Don’t Know	0	0%
	8	**100%**

Importance to the Senior Management.

This measure was taken to indicate how it ought to be placed in the strategic plan in the County government i.e. how important it is in the overall picture. The respondents were required to indicate the level of importance of ITSC/DR plans to the Senior Management since it is either the management are aware or support or they own the process. Results indicate that those who regard it to be “Very Important” were 60%, “Important” were 40%. See data depicted in Table 9 below.

This shows it is a strategic element and need to be placed high in the County Strategic Plan.

Table 10 - IT SC/DR Plan - Importance to Senior Management

Level	Count	Percentage
Very Important	6	60%
Important	4	40%
Neutral	0	0%
Not-Important	0	0%
	10	**100%**

External Request for Plans

The devolution system of government that Kenya adopted is per se not fully-devolved. The Central government is still a parent to all the counties politically and economically. Most functions in the counties are regulated by the Central government.

The central government has roles to play in the devolved counties through its various arms. The particular ones that touch on ICT in the counties are ICT-Authority, KRA, Transition Authority, and Commission of Implementation of Constitutions (CIC). There are also other interested bodies like insurers and other regulators who come into picture.

This study sought to establish whether those arms of governments and other players have had an interest in IT Service continuity in the counties. The study found that external requests have been made and leading is ICT-Authority with 62%, followed by Transition Authority of Kenya 12%, Insurers 12 % and CIC, KRA, Auditors and others have not requested for these plans. See responses in percentages in Table 10 below.

This indicates that these plans are very important for statutory and regulatory obligations. For those in existence updated documentation need to be available both in hard and soft copies.

For the counties who do not have or working on it they need to implement them as soon as possible.

Table 11 - External requests for ITSC/DR Plan

External Bodies	No. of responses	Percentage
ICT-Authority	5	63
Transition Authority of Kenya	1	13
CIC	0	0
KRA	0	0
Auditors	0	0
Insurers	1	13

No External Requests	1	13
Other	0	0
Total	8	100

ITSC/DR Plan Maintenance.

The study also sought to establish how ITSC/DR plans are maintained in terms of reviewing.

A large number of respondents are reviewing their plans every 2 Qs per year, 25 % are reviewing once per year, 13% do the review once a quarter per year. Those who do not review are a quarter (25%) of the sampled population.

An outdated plan is a risk to IT Service Continuity /DR plan. Figure 4.2 depicted the distribution of review as per the sample.

When a plan is not reviewed it gets outdated especially in IT field where changes happen very fast. Failure to review or prolonged review period could be due to inadequate skills or personnel in the IT departments or there is general laxity in maintaining the Plan. An upto date Plan implies that the department is fully functional and processes are on course.

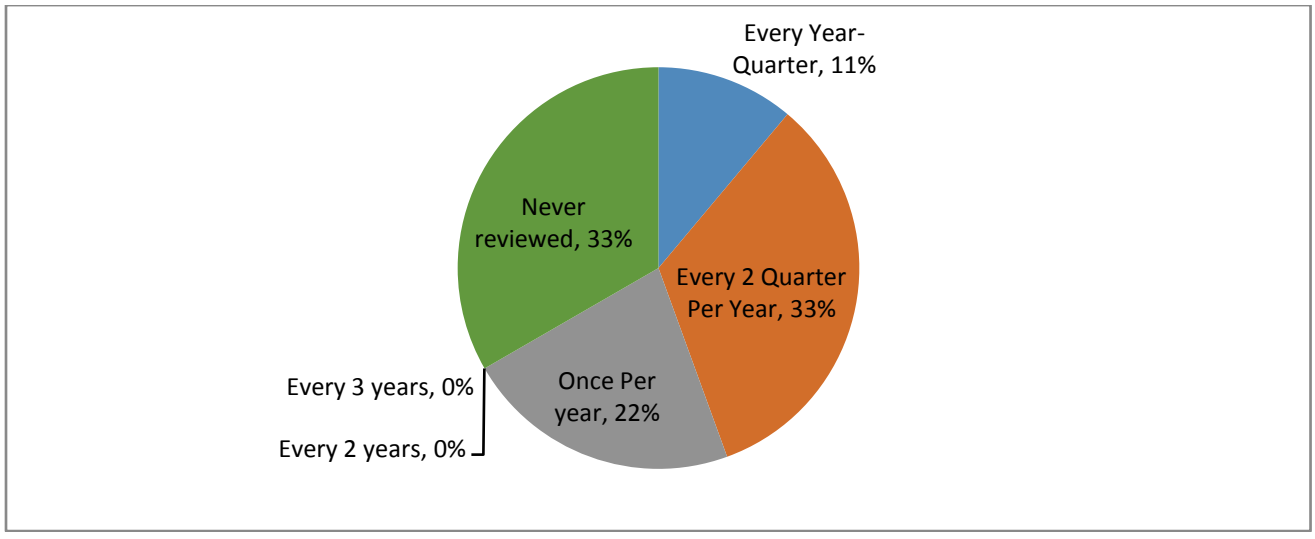


Figure 4.1-3 - Frequency of ITSC/DR Plan Review

Familiarity with IT Frameworks

Establishment of evaluation framework was part of the objective of this study. Here, the study sought to establish whether the respondents are aware of some of the popular IT frameworks in the field.

It found out that CoBIT is popular at 40% of the respondents citing familiarity, followed by ISO 2900 at 33%, ITIL is thirdly popular at 20% and the least popular is COSO , none is aware about it. These are depicted in Figure 8 - Familiarity with IT Frameworks below.

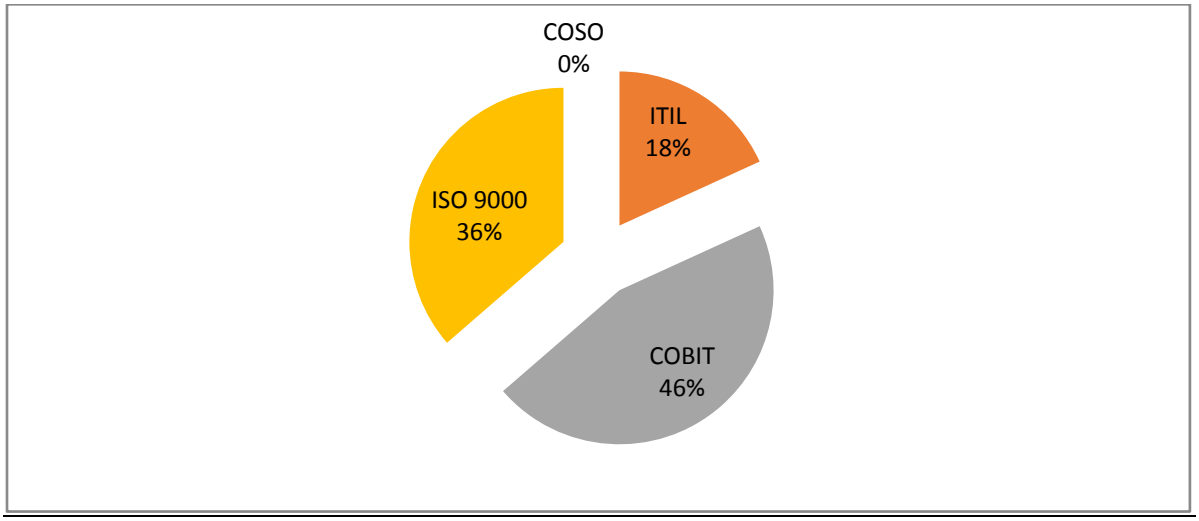


Figure 4.1-4 - Familiarity with IT Frameworks

4.2 Proposed Evaluation Framework for ITSC/DR Plan.

After situational analysis of the ITSC /DR plan in the counties. The study found that implementation of ITSC/DR plans is not consistent between counties. They implement them independently and therefore not standardized throughout the country.

Determining the level of statuses of these plans it requires a universal evaluation tool that is applied to all counties at the same time. This study also found out that external requests have been made for these plans but did not establish the purposes of the requests.

There are industry recognized evaluation tools but they are quite expensive on cost and implementation processes.

This study therefore came up with Evaluation framework with critical success factors (CSF) or salient features that have been selected and categorized according to adopted and modified Demming cycle model.

Using the same instrument of questionnaire (Section C). Responses from PDCA clusters were collected and evaluated to establish if they conform to international standards.

PLAN Section:

Table 12 - Results for Salient features for PLAN Section

PLAN	1	**Are there IT Service Continuity and Disaster recovery policy with senior management**	**Total**	%
		Yes	3	30%
		No	2	20%
		Partially	5	50%
	2	**Is there Budget Allocation for IT Service Continuity Plans**	**Total**	%
		Yes	4	40%
		No	3	30%
		Partially	3	30%

Management support and budget allocations are critical factors for existence and success of IT Service continuity plan.

Senior Management Support.

This is a very important factor. The senior management has to be in agreement that the plans are necessary and subtle to existence of business. Business processes are nowadays entirely dependent on IT platforms. Ensuring its continuity is also ensuring business continuity.

From the collected data, results show that 30% of respondents agree that Management is aware and supporting the Plan, 20% are not supporting and 50% say they partially support.

A partial commitment is no guaranteed that those counties will have an effective IT service Continuity plan. The commitment of the senior management will affect every other factor of having the plans in place.

Budget Allocation:

Budget allocated to IT service continuity will help to run effective IT service continuity activities ; planning , personnel training, purchase of redundant equipment and any other necessary activity. The results from research indicate that 40% of the counties have budget allocated, 30% do not have whereas 30% have it partially allocated. This implies that the budget are not enough or available. This can affect effective IT Service Continuity.

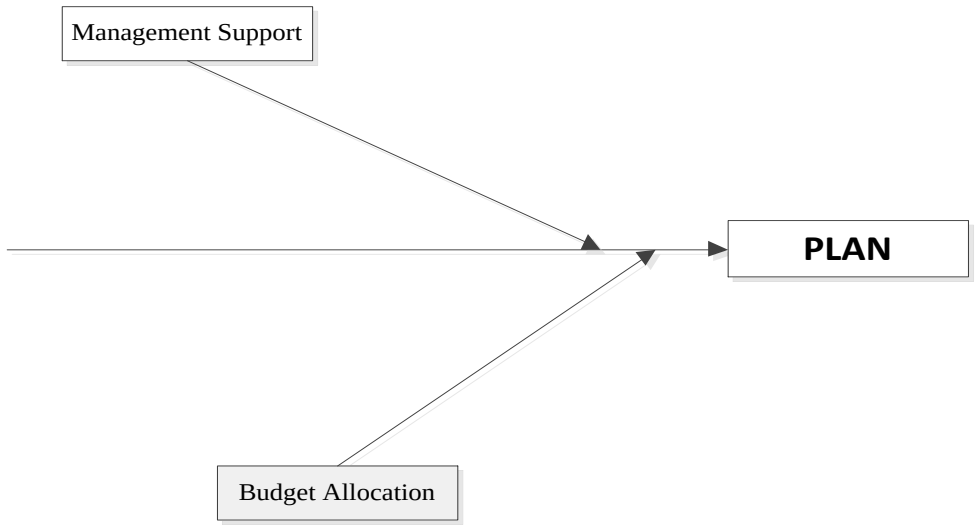


Figure 4.2-1 - Salient features derived from PLAN Section

DO Section:

On this section the study sought to tests actual activity that the county needs to undertake to ensure effective IT Service Continuity.

Table 13 - Results for Salient features for DO Section

1	Through a review of the backup procedures with staff within each division, is it evident that they are aware of their responsibilities, especially with respect to protection of data and software?	Count	%
	Yes	5	50%

	No	1	10%
	Partially	4	40%
		10	100%
2	Are there internal responders to develop plans for helping the County during emergency?		
	Yes	6	60%
	No	3	30%
	Partially	1	10%
		10	100%
3	Has Continuity Team done IT Business Impact Analyst and Risk Assessment?		
	Yes	5	56%
	No	4	44%
	Partially	0	0%
		9	100%
4	Do IT Service Continuity/DR Plans include People, Premises, Technology and Information		
	Yes	5	50%
	No	3	30%
	Partially	2	20%
		10	100%
5	Is ICT-A or TA aware of ITSC/DRP	Total	%
	Yes	6	60%
	No	3	30%
	Partially	1	10%
		10	100%
6	Are Backup systems and files stored off-site?		
	Yes	5	56%

	No	2	22%
	Partially	2	22%
		9	100%
7	Does transfer of data occurs immediately after backup?		
	Yes	6	67%
	No	3	33%
	Partially	0	0%
		9	100%
8	Does the documentation of the service providers also review of copies of their backup plans?		
	Yes	6	67%
	No	2	22%
	Partially	1	11%
		9	100%
11	Have the service providers' backup plans been tested with respect to backup of the County's services?		
	Yes	5	56%
	No	3	33%
	Partially	1	11%
		9	100%
12	Maximum Tolerable Outage(MTO) for Power		
	0-6hrs	6	60%
	6-24hrs	2	20%
	1-3days	0	0%
	3-7days	1	10%
	>7 days	1	10%
		10	100%
13	_Maximum Tolerable Outage(MTO) for Internet		
	0-6hrs	8	80%

	6-24hrs	1	10%
	1-3days	0	0%
	3-7days	1	10%
	>7 days	0	0%
		10	100%

Users Responsibilities for Protection of Data and Software:

Assigning responsibilities is vital for effective accountability. This will ensure coverage of functions in when implementing IT Service Continuity and during systems recovery. 50% of the responders indicate the division users are aware of their responsibilities on data protection and 10% said no and 40% of respondents are partial. This implies general weakness in awareness throughout the counties on users being aware of their responsibilities on Protection of Data and software.

Internal responders developing plans:

The success of IT Service Continuity plan will depend also on participation of local user/workers e.g. fire department, electrical. Internal responders have knowledge and expertise in their areas and collaborating in terms of ensuring IT Service Continuity will help when there is downtime. 50 % of the counties have involved internal responders, 40% have partially involved and 10% have not involved. This implies that the counties need to involve more internal responders. They may engage them through signing of Service Level Agreements of some kind of contracts

IT Business Impact Analysis or Risk Assessment

BIA and Risk assessment are some of the most important activity in IT SC. Without them there is no ITSC. These help to focus on the Systems impacts and risks that can affect IT systems directly including human beings and other resources. 56 % of the respondents have had BIA and or RA undertaken in the counties. 44% have not undertaken either of the two.

Composition of IT SC Plans in terms of People, Premises, Technology and Information.

This is about the scope of the plans. What it covers and who is included. A result of 50% say it cover all, 30% respondents indicated that their plans does not cover and 20% said it partially covers. This means counties need to extend inclusion to cover most of the subtle areas.

Central government role (ICT-A, TA etc)

Being part of the central government, the counties are answerable to the central government in some areas. Through ICT-A and/or TA the government need to be in full control of their responsibilities in the counties. Results from awareness by ICT-A or TA indicate that 60% of counties ICT-A or TA are aware of this ITSC plans. 30% ICT-A and/or TA are not aware and 10% respondents say they are partially aware.

Backup files and Systems Stored Offsite?.

IT Systems with no files and data backup is too risky to rely on. Systems data and files need to be kept offsite incase the primary site is not accessible. Results obtained indicate that 56% of counties have files kept offsite, 22% do not know and 22% have files partially kept offsite.

This means that Systems are still dangerously run in the counties. In case of disruption on the primary site, losses are imminent.

Transfer of Data occurring immediately after backup.

Data when backed up need to be transferred immediate to avoid chances of losses. Results obtained show that 67% of the counties have data transferred immediately, 33% said no. This is fairer but regulating Authorities need enforce 100% transfer immediately.

Documentation of Service Providers includes copies of their Backup plans.

Where IT service depends on Service providers the client need to ensure those Service providers do also have Continuity plans for the services rendered to the client. 67% of the responders said Service Providers have provided copies of their service backup plans.22% indicated “no” while 11% said partially.

Testing of Service Providers Backup Plans.

The client to ensure none interruption of services provided by external party need to test Service provider backup. Results obtained indicate that 56% do test the plans, 33% have not tested whereas as 11% have done it partially.

This implies that a few counties have tested Service Providers continuity plans. This level is not adequate and puts services in the counties at risk.

Maximum Tolerable Outage (MTO) for Power

Power available is vital to IT service since most systems are electronics. Prolonged outage will affect negatively effectiveness of IT Service and hence business at large. Results obtained shows that 60% of counties can tolerate 0-6 hrs only, 20% can tolerate 6-24 hrs, 10% can tolerate 3-7 days and 10% can tolerate > 7 days. This implies more counties are reliant on IT Services and less tolerable hours. A few those who tolerate > 7 days are not dependent on IT and show a unique setup. To improve reliability of Power counties may seek alternative source of power to run parallel with the main source.

Maximum Tolerable Outage (MTO) for Internet

Internet is currently being relied for many application hosted in remote sites. Cloud architecture has become popular and much organization runs critical applications on the cloud. Others runs Systems and files backup on the cloud hence availability of Internet is becoming very critical.

The study found that 80% of the counties can tolerate 0-6 hrs, 10% can tolerate 6-24 hrs and 10% can tolerate 3-7 days. The outcome implies that internet is critical and counties cannot tolerate prolonged downtime.

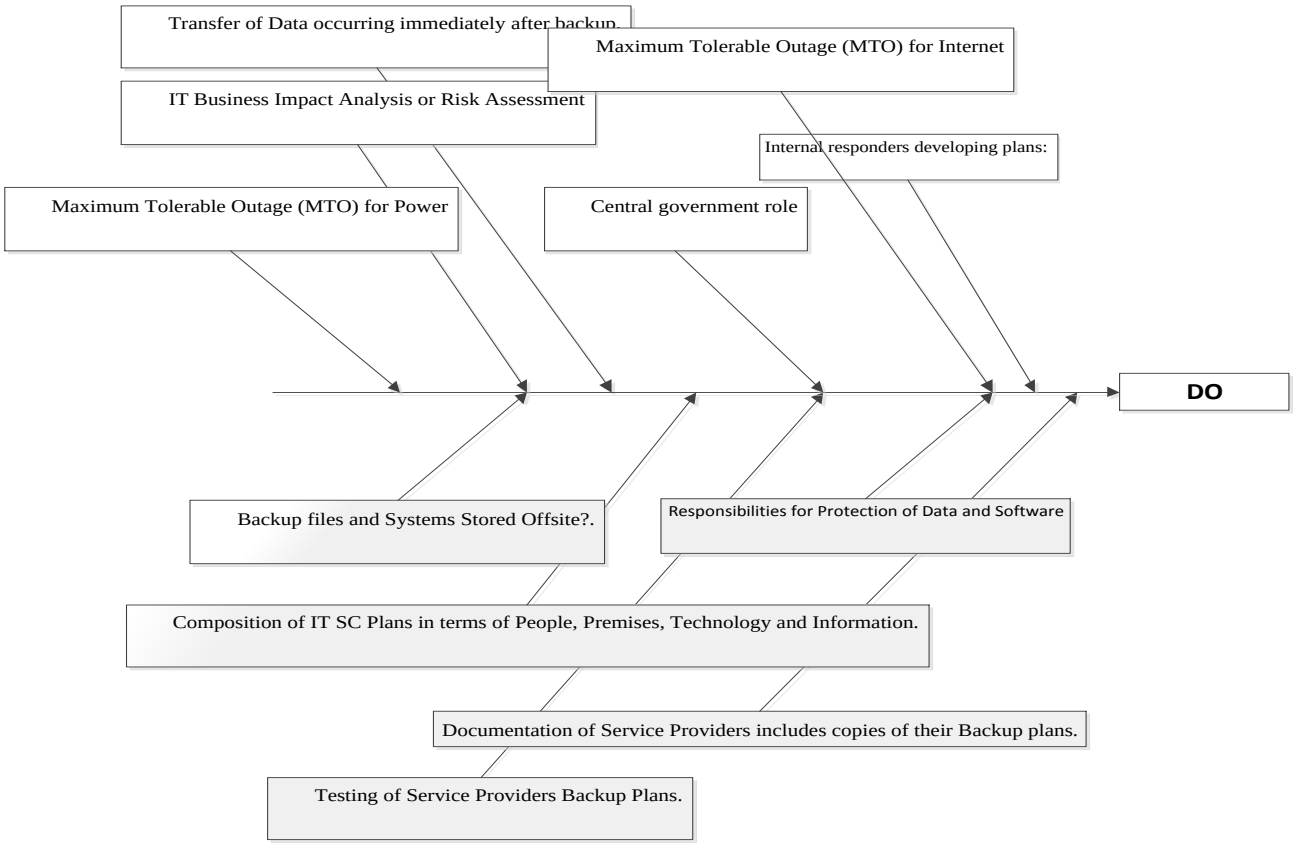


Figure 4.2-2 - Salient Features from the DO Section

The counties need to improve on the infrastructure to ensure more availability of the internet.

CHECK Section

Table 14 - Results for Salient features for Check Section.

1	**Frequency of Conducting Tests/Drills**	Total	%
	Every Quarter	1	13%
	Every half Year	2	25%
	1-2 Years	4	50%
	3-5 Years	1	13%
		8	100%
2	**Plans Test for Worst Case Scenario**	Total	%

	Yes	2	25%
	No	5	63%
	Partially	1	13%
		8	100%
3	**Do testing provide details to indicate that..**		
	a. The test was evaluated?		
	Yes	5	63%
	No	3	38%
	Partially	0	0%
		8	100%
	b. Any cited deficiencies were documented?		
	Yes	4	50%
	No	3	38%
	Partially	1	13%
		8	100%
	c. Deficiencies were corrected?		
	Yes	6	75%
	No	2	25%
	Partially	0	0%
		8	100%
	d. Deficiencies were retested?		
	Yes	4	50%
	No	3	38%
	Partially	1	13%
		8	100%
4	**Were the following areas, at a minimum, tested?**		
	a. Data files?		
	Yes	6	75%
	No	0	0%
	Partially	2	25%
		8	100%
	b. Equipment?		
	Yes	6	75%
	No	0	0%
	Partially	2	25%

		8	100%
	c. Backup equipment?		
	Yes	6	75%
	No	0	0%
	Partially	2	25%
		8	100%

Tests and Drills

Tests and Drills are meant to check effectiveness of plans. Results obtained show that 20% of the counties carry out test/drills every quarter, 30% do it every half year, 40% every 1-2 years and 10 % indicate they test 3-5 years. This shows that most counties do not carry test/drills in shorter period. Prolonged period of test/drills are not good for effective plans.

A test for worst case scenario.

A way to minimize risk in an organization is to concentrate on the worst case scenario hence in order to keep it simple the framework selected worst case scenario factors within the CSFs

The study sought to establish whether worst case scenario has been carried out in the counties. The study obtained show that 22% of counties have tested for worst case scenario, 67% have not and 11% have partially tested. This implies counties generally have performed poorly in testing of worst case scenario and risks are not minimized.

Deficiency Tested.

The results obtained from respondents indicated that 63% said the test was evaluated, 38% have not tested. And deficiencies cited documented was 50%, 38% show deficiencies not documented 13% indicate partially.

The respondents indicated that 75% of the counties have had deficiencies corrected, 25% have not corrected .And whether deficiencies were retested showed 50% show the test have been retested, 38% have not retested and 13% partially retested.

Testing of Data files, Equipment and backup equipment

Data files, Equipment and backup equipment were subjected to the questionnaire, results obtained show 75% of counties have their data, equipment and backup equipment files tested, 25%

partially. This means that the backups fairly test the data files, equipment and backup equipment. But improvement to fully comply.

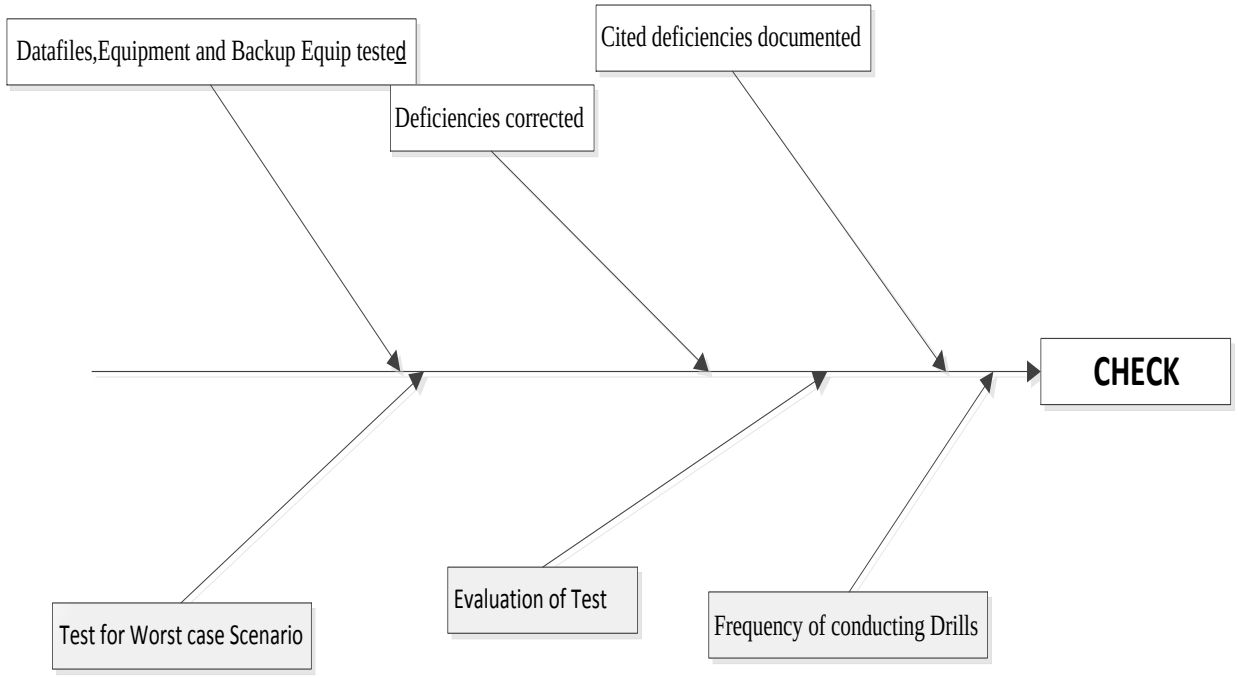


Figure 4.2-3 - Salient features derived from CHECK Section

ACT Section

Table 15 - Results for Salient features for ACT Section

	Are there arrangement that include Incident Management Process, Notification, Recovery and Estimated Time?	Total	%
1	Yes	7	88%
	No	0	0%
	Partially	1	13%
		8	100%
2	Is the previous Outcome lessons learned been used for improvement of ITSC/DRP?		
	Yes	6	75%

	No	1	13%
	Partially	1	13%
		8	100%

Arrangement that include Management Process, Notification, Recovery and Estimated time

Queried on existence of arrangement that include management process, notification, recovery and estimated time.88% of the respondents said there exists, 13% said partially. This shows there is generally inclusion of those processes in the overall ITSC/DR plan.

Previous outcome lesson learned used for improvement of ITSC/DR Plan.

This framework is circular in nature, learned lesson are used to correct or improve the plan. Results indicated that 75% have had previous lesson been used to improve ITSC/DR plan, 13% indicated "no" whereas 13% showed partial.

This implies that there is remarkable improvement of ITSC/Dr plan from lessons learned from previous incidences or drills. There is still substantial no of counties whose lesson learned have not been used to improve the plans.

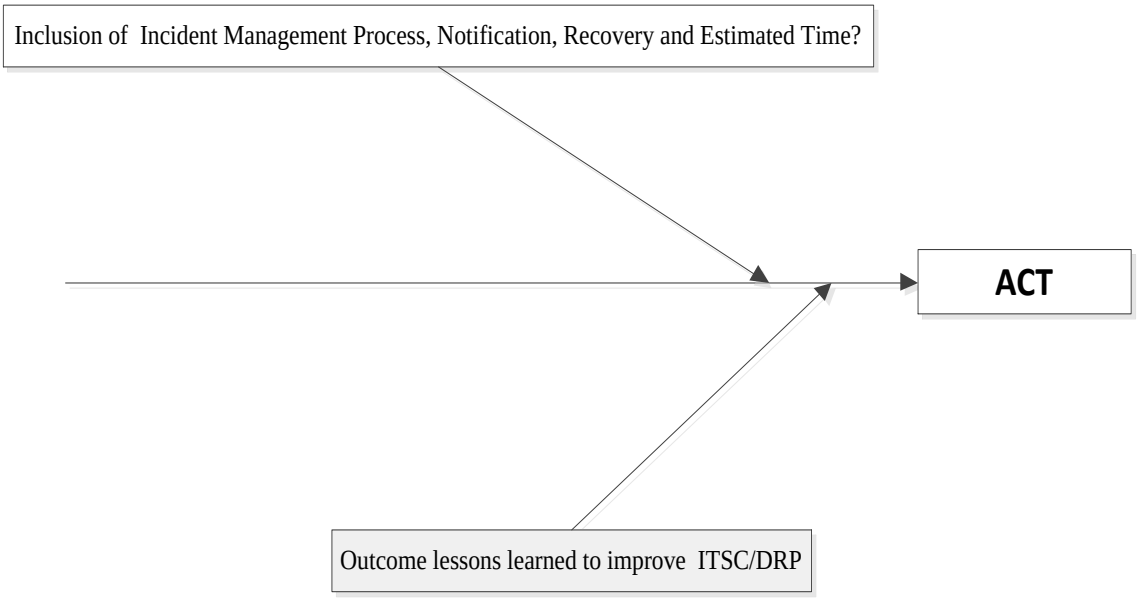
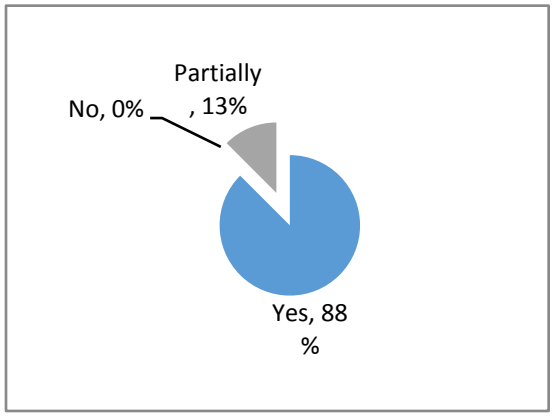
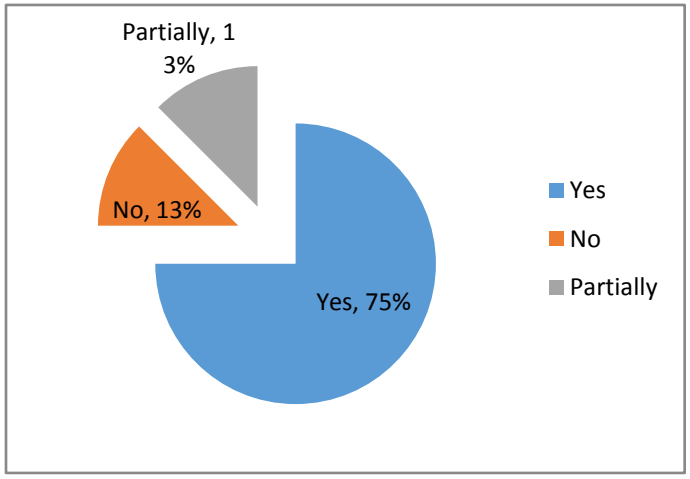


Figure 4.2-4 – Salient features derived from ACT Section

Inclusion of incident Process, Notification, Recovery and Estimated Time.



Previous outcome lessons learned used to improve ITSC/DR plan.



4.3 Application of the Framework in an Organization setup.

The IT Service continuity evaluation framework is to be used at site level. It may be used at the group level as well.

The framework can be filled in less than an hour. To get credible results it is better to ask the questions people in the organizations under investigation.

The answers are translated into **1 for Yes, -1 for No and 0 for partially**. All answers are summed in each group of the stages and a grand total is obtained. The questions that have wordings as response are ignored.

Evaluation Framework as applied to Sample 1 County and Sample 2 County Consecutively.

Table 16 – Results of Evaluation of Sample 1 and Sample 2 Counties

			SAMPLE 1 COUNTY		SAMPLE 2 COUNTY	
PLAN	1	**Are there IT Service Continuity and Disaster recovery policy with senior management**				
		Yes			√	1
		No				
		Partially	√	0		
	2	**Is there Budget Allocation for IT Service Continuity Plans**				
		Yes			√	1
		No	√	-1		
		Partially				
		Sub -Total		-1		2
DO	3	**Through a review of the backup procedures with staff within each division, is it evident that they are aware of their responsibilities, especially with respect to protection of data and software?**				
		Yes			√	1
		No				
		Partially	√	0		
	4	**Are there internal Responders to develop plans for helping the County during emergency?**				
		Yes				
		No	√	-1	√	-1
		Partially				
	5	**Has Continuity Team done IT Business Impact Analysis and Risk Assessment?.**				
		Yes			√	1
		No	√	-1		

		Partially				
	6	**Do IT Service Continuity/DR Plans include People, Premises, Technology and Information**				
		Yes			√	1
		No	√	-1		
		Partially				
	7	**Is ICT-A or TA aware of ITSC/DRP**				
		Yes			√	1
		No	√	-1		
		Partially				
	8	**Are Backup systems and files stored off-site?**				
		Yes			√	1
		No	√	-1		
		Partially				
	9	**Does transfer of data occurs immediately after backup?**				
		Yes	√	1	√	1
		No				
		Partially				
	10	**Does the documentation of the service providers also review of copies of their backup plans?**				
		Yes			√	1
		No	√	-1		
		Partially				
	11	**Have the service providers' backup plans been tested with respect to backup of the County's services?**				
		Yes			√	1
		No	√	-1		
		Partially				

	12	**Maximum Tolerable Outage(MTO) for Power**				
		0-6hrs	√	1		
		6-24hrs				
		1-3days				
		3-7days			√	0.2
		>7 days				
	13	**Maximum Tolerable Outage(MTO) for Internet**				
		0-6hrs	√	1		
		6-24hrs				
		1-3days				
		3-7days			√	0.2
		>7 days				
		Sub-Total		-4		7.4
	14	**Frequency of Conducting Tests/Drills**				
		Every Quarter	√	1		
		Every half Year				
		1-2 Years			√	0.2
		3-5 Years				
	15	**Plans Test for Worst Case Scenario**				
		Yes			√	1
CHECK		No	√	-1		
		Partially				
	16	**Do testing provide details to indicate that.**				
		a. The test was evaluated?				
		Yes			√	1
		No	√	-1		
		Partially				
		b. Any cited deficiencies were documented?				

		Yes				
		No	√	-1		
		Partially			√	0
		c. Deficiencies were corrected?				
		Yes			√	1
		No	√	-1		
		Partially				
		d. Deficiencies were retested?				
		Yes				
		No	√	-1		
		Partially			√	0
	17	**Were the following areas, at a minimum, tested?.**				
		a. Data files?				
		Yes	√	1	√	1
		No				
		Partially				
		b. Equipment?				
		Yes	√	1	√	1
		No				
		Partially				
		c. Backup equipment?				
		Yes	√	1	√	1
		No				
		Partially				
		Sub-Total		-1		7
ACT		**Are there arrangement that include Incident Management Process, Notification, Recovery and Estimated Time?**				
		Yes	√	1	√	1
		No				
		Partially				

		Is the previous Outcome lessons learned been used for improvement of ITSC/DRP?				
		Yes	√	1	√	1
		No				
		Partially				
		Sub-Total		2		2
				Grand Total.	-4	18.4

Summarized Scores

Table 17 - Summary Scores for Sample 1 and Sample 2 Counties

	Sample 1 County Scores	Sample 2 County Scores	Min	Max
Plan	-1	2	-2	2
Do	-4	7.4	-11	11
Check	-1	7	-9	9
Act	2	2	-2	2
	-4	18.4	-24	24

Scoring 24/24 according to this research means the level of IT service continuity is most efficient. It does not mean it has been improved to near perfection. But mathematically scoring 10/24 is not better than scoring 20/24. It also depends on the cost of arriving at those levels. This implies that when analyzing results cost-benefit analysis is also paramount.

Benefits.

The benefits will be realized if applied as is without any biased answers. It requires honesty from the respondent and from a real existing organization.

Procedures for Implementation:

To achieve optimum results the following has to be used:

1. The right respondent has to fill in the questionnaire.
2. The responded has to find the actual responses as is on the ground.
3. Summarize the results for each stage.

The Model's four stages of PDCA makes it clear to for organization or the evaluator to see which stage requires improvements.

Fulfilling the Purpose.

The purpose was to provide a simplified evaluation framework for IT service continuity which addresses technology risks within a county government size of organization

The evaluation framework is a methodology to learn more on what changes should be made within the organization for a more efficient IT service continuity. This will reduce negative impact from IT service downtime Based on this the researcher believe the purpose has been fulfilled.

CHAPTER V

SUMMARY OF THE FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction.

This chapter summarizes findings, provides conclusion and recommendation that is based on the objectives of the study. Objectives of the study was to Assess implementation of IT Service Continuity in Kenya's Devolved Counties and to develop evaluation framework for IT Service Continuity and Disaster Recovery plan that can be applied to implemented IT SC/DR processes in Kenya's Devolved Counties. Two areas were evaluated: Establishment of status of IT service continuity and Disaster recovery level and a developed evaluation framework was tested.

A questionnaire was developed and data collected with it from County governments' ICT department throughout the country using a size sample of ten (10) counties.

5.1 Summary of Findings.

In the context of the county governments, the study found that half the counties have ITSC/DR plan in place, 10% do not have and 40% partially have. From those who have and those who partially have 19% covers Fire, 19% covers loss of site, 15% covers loss of capacity, loss of communication and loss of people each covered 12%, Loss of skills and Environmental liability each is 8% covered and none covers pressure group protest. This moderate implementation of ITSC/DR plan could be attributed to the fact that wrong prioritization of projects in the county government. Most decision makers are not IT literate; hence projects funds only go those that are physical in nature like roads and buildings. Other factors include the regulatory compliance; the regulator in the Central government is under performing. These are ICT-A, TA and CIC they do not have capacity in terms of adequate human resources and tools to enforce practice of implementing ITSC/DR plan in the counties.

The study found that these plans are very important, 60% of the respondent said they are "very Important" and 40% of the respondent said they are "Important" and none was neutral or said not important.

On past incidences at least all have experienced interruption at one level or the other, 27% of the respondent said they have experienced Unplanned IT and Telecom outage and 23% have had experienced of utility supply. Request by auditors is 0% this indicates that no audit has been

carried throughout the country to audit IT Service Continuity plans. Insurers have requested from only 10% from the respondents. There is general laxity in enforcing implementation of these plans in the counties.

Among those who have implemented the Plans reviews take long time and hence not good for IT Service Continuity plan since IT evolves faster than other industries. 33% of the respondents review Plans every two (2) quarter per year while 11% review every year quarter. The recommended is monthly or every quarter.

On awareness of IT frameworks most of the respondents are aware of COBIT, followed by ISO 9000 and ITIL subsequently, none is aware of COSO. This therefore implies that conformance to IT frameworks is at minimum.

The designed evaluation framework categorized the processes into four stages by adopting PDCA demning circle. This model is adequate because evaluation of these plans is a continuous and circular in nature. Evaluation process is arranged such that each Critical success factor falls under a category within the circle.

Among the counties most ITSC/DR plans covers other functions in the organization and the most covered is Finance this could be because of its sensitive of money matters.

The biggest challenges in implementation of ITSC are lack of or minimum support from senior management (indicated by 20% of the respondents) this would be expected countrywide. The evaluation framework standardizes Critical success factors for effective IT SC evaluation.

5.2 Conclusion.

In conclusion, a few counties have implemented IT Service Continuity/DR plans but the overall picture is that implementation is low (50%). It is evident that there is senior management support but there is little on the ground to warrant the support and high importance regard of these plans.

Allocation of budget is also very low. 40% of the counties have budgeted for it.

The study also concludes that BIA/Risk management is fairly undertaken (54%) and the biggest threats are Unplanned IT and Telecom Outage and interruption of utility supply. Familiarity to framework is fair; the respondents are aware of other IT frameworks like CoBIT, ITIL and ISO. However, the study established that COBIT and ITIL are expensive and cumbersome to implement. Only big companies would afford to implement but the level of counties may not have the capacity in terms of finances and human capital. As part of the objective this study come up

with an evaluation framework and test it with data collected from the counties. This framework can be adopted by anyone interested in evaluating ITSC/DR in Kenya's devolved counties and any other organization of similar nature with few modifications.

In Summary, the proposed IT Service continuity and DR plan framework show that there are a lot of weaknesses and vulnerabilities on IT Service Continuity in the counties.

5.3 Recommendation.

The findings of the study show that implementation of ITSC/DR plans is regarded as important but the implementation is low. The counties that have implemented have not done it upto the required standard , this was noted by other factors like review period, relaxed MTO, low tests and drills circles, test of worst case scenario etc.

This study recommends awareness creation at all levels from County Governors to the juniors levels, responsible regulatory Authorities like TA and ICT-A and sound implementation approach that covers all systems in the counties.

It also recommends adoption of simplified evaluation framework based on PDCA demming circle principle of continues improvement.

The central government should also take it up through relevant arms to ensure compliance to standards. The government should have regulation and guidelines in place since they are excellent approaches to ensuring completeness and compliance.

The county government should take it up and up skill their employees by training them in matters that's affect IT Service Continuity. There are many on-job skills opportunities which employees can attend to as while at working.

5.4 Recommendation for Further Research.

The study was based on IT Service Continuity and DR plans in the counties. It established statuses of the plans implementation. It also developed a simplified evaluation framework that can be adopted to evaluate the plans.

To further develop results from this study, it is recommended that further research be done on the following areas;

Research on factors that affects implementation in other organizations be it other government bodies or private sectors with more emphasis on factors affecting their implementations.

To develop a more simplified method to identify other critical factors in the framework that would lead to better results.

It is also recommended that further research be done on more specific approaches rather than a more general. Most organization maybe unique in their ways of doing business e.g. Military or other Government secret installations. It may be cost effective and also a good complement to identifying a more specific part or section of the processes where improvement is required.

Table 18 - Research Project Schedule

SNo	Task	04-15	05-15	06-15	07-15	08-15	09-15	10-15	11-15	12-15
1	Problem Definition	√								
2	Literature study	√	√	√						
4	Submit Proposal				√					
5	Interview Questionnaire					√	√	√		
6	Analyze and Re-define Problem(s)							√		
7	Finalizing Report								√	√
9	Bind Report									√
10	Handing in Final Report									√

REFERENCES

1. Almen, J & Rosqvist, A (2008), Evaluate your business continuity management: A step towards a more resilient company.
2. Barbara, Michael, (2006), Determining the Critical Success Factors of an Effective Business Continuity /Disaster Recovery Program in a Post 9/11 World: a Multi-Method Approach.
3. Bahshani, Semma & Sellma(Jan 2015) Towards a New Approach For Combining The IT Frameworks.
4. Brotby, Krag(2008), Information Security Management Metrics
5. Data, 2015. Available from: https://en.wikipedia.org/wiki/Data, 02 August 2015.
6. Darcy, Heather (2011), http://searchsmbstorage.techtarget.com/quiz/Disaster-recovery-basics-for-SMBs-A-quiz-on-DR-planning-strategies as at 09/09/2015.
7. Dolinsky Bob, (2015) Key success factors for business continuity planning: http://www.iltanet.org/MainMenuCategory/Archives/PeertoPeerArchives/February2006/KeySuccessFactorsforBusinessContinuityPlannin.txt,as at 20/07/20015
8. Ghauri.P, Gronhaug Research Methods in Business Studies (4th Edition) , 2005
9. Guldentops, E. (2004). Key Success Factors for Implementing IT Governance: Let's Not Wait for Regulators to Tell Us What to Do. Information Systems Control Journal.
10. Holub,E (2015), IT Operations Optimization via ITSM, ITIL and DevOps Key Initiative Overview.
11. Souter, Makau(2012). Internet governance in Kenya – an assessment for the Internet Society.
12. ITGI. (2011). Global Status Report on the Governance of Enterprise IT (GEIT)—2011. IT Governance Institute, www.itgi.org.
13. ITGI, OGC. (2015). Aligning CoBiT , ITIL and ISO 1779 for Business Benefits: Management"Summary.http://www.isaca.org/Knowledgecenter/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf
14. Juup, V, (2006).The SAGE Dictionary of Social Research Methods,
15. Jackson, S.L. (2009). Research Methods and Statistics: A Critical Thinking Approach 3rd edition. Belmont, CA: Wadsworth.

16. Linder, G (2010). Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework
17. Khan,R & Wanner, R (2010) Practical Approaches to Organizational Information Security.
18. Kozina, Melita (2009). COBIT - ITIL mapping for Business Process Continuity Management. Proceedings of the 20th Central European Conference on Information and Intelligent Systems.
19. Layton, Timothy P, (2006), Information Security: Design, Implementation, Measurement, and Compliance.
20. Mingay, Bittinger (June 2002)., Combine CobiT and ITIL for Powerful IT Governance Management GIAC (G7799), Gold Certification. (2010), the SANS Institute pp 7- 10.
21. Sewall B, (2009), Information Security Handbook.
22. Wanjiku,R(2013) http://www.itworld.com/article/2705832/it-management/kenyan-banks-face-challenges-with-secure-online-transactions.html on 02, August 2015.
23. Wechuli , Muketha & Matoke (2014) International Journal of Technology in Computer Science & Engineering, Volume 1(3), pp 100- 113
24. Zorz, Mirko, (2013), Information risks in the enterprise.

APPENDICES

APPENDIX I – INTERVIEW COVER LETTER

Dear Respondent

REQUEST FOR PERMISSION TO CONDUCT RESEARCH

I am a Master's student in the Department of ICS-School of Computing and Informatics at the University of Nairobi. My supervisor is Dr. Evans Miriti.

The proposed topic of my research is: Evaluation Framework for IT Service Continuity and Disaster Recovery Plans in Devolved County Government: The Case in Kenya.
The objectives of the study are:

i. Assess implementation of IT Service Continuity/Disaster Recovery Plan in Kenya's Devolved Counties.
ii. Develop evaluation framework for IT Service Continuity/DR Plan Kenya's Devolved Counties.

I hereby seek your consent to collect the required information per the questionnaire herewith attached

You have been selected as part of a relatively small sample, so your participation and feedback will be highly appreciated and useful in trying to understand the contribution of these factors. The questionnaire should take about fifteen to twenty minutes to complete

Note: Your response will remain completely confidential.

I appreciate for taking your time to complete the questionnaire,

Sincerely,

Bernard Koech

APPENDIX II - QUESTIONNAIRE

SECTION A: Respondent Profile

Please provide information by ticking the appropriate boxes [ ]

1. What is your gender Male [ ] Female[ ]

2. What is your age?

   Below 20 yrs [ ] 27-32 yrs [ ] 39-44 yrs [ ] over 50yrs [ ]

   21-26 yrs [ ] 33-38 yrs [ ] 45-50 yrs [ ]

3. What is your education level (Graduated)?

   Secondary [ ] College Dip. [ ] Graduate Degree [ ]

   Post Graduate degree [ ] Other……

4. How long have you worked in this County?

   0-2 years [ ]

   3-5 years [ ]

   6-9 years [ ]

   10+ years [ ]

5. What is your designation in the County ICT department?

   Chief Information Officer/IT In-Charge [ ]

   Systems Administrator [ ]

   System Analyst [ ]

   Business Continuity Administrator [ ]

   Hardware Support Staff [ ]

   Software Support [ ]

SECTION B: Assessment of Implementation of IT Service Continuity Plan/DRP in the County.

1. Does the County have IT Service Continuity Plan/DRP?

Yes	[ ]
No	[ ]
Partial	[ ]

2. Which of the following does your IT Service Continuity Plan/DRP Cover?

Loss of site	[ ]
Loss of IT Capacity	[ ]
Loss of People	[ ]
Fire	[ ]
Terrorism damage	[ ]
Negative publicity	[ ]
Loss of Skills	[ ]
Military Strike	[ ]
Loss of Communication	[ ]
Pressure group Protest	[ ]
Environmental liability.	[ ]

3. How do you classify the extent of disruption caused to your county by any of the following events? [*Kindly tick one box as appropriate*].

	Severe	Serious	Modest	non-existent	don't Know
Computer viruses:	[ ]	[ ]	[ ]	[ ]	[ ]
Power fluctuations/Failure	[ ]	[ ]	[ ]	[ ]	[ ]
Act of Terrorism	[ ]	[ ]	[ ]	[ ]	[ ]
Human error	[ ]	[ ]	[ ]	[ ]	[ ]

4. Which if any of the below threats has your county experienced in the past months/years

Unplanned IT and telecom outages	[ ]
Cyber attack	[ ]
Data breach	[ ]
Adverse weather	[ ]
Interruption to utility supply	[ ]
Fire	[ ]
Security incident	[ ]
Health & Safety incident	[ ]
Act of terrorism	[ ]
New laws or regulations	[ ]
Loss of site	[ ]
Loss of IT Capacity	[ ]
Loss of Skills	[ ]
Military Strike	[ ]
Pressure group Protest	[ ]

Other ……

5. How important is ITSC /DR plans to county Senior Management?

Very Important	[ ]
Important	[ ]
Neutral	[ ]
Not Important	[ ]

6. Has the County been requested to provide evidence of Business Continuity plan by any of the following groups or bodies?

ICT-Authority	[ ]
Transition Authority Kenya	[ ]
Commission of Implementation of Constitution	[ ]
KRA	[ ]
Auditors Not Important	[ ]
Insurers	[ ]
No External Requests	[ ]

Other …….

7. In the following list which losses or threats does your IT Service Continuity Plan/DRP cover?

Unplanned IT and telecom outages	[ ]
Cyber attack	[ ]
Data breach	[ ]
Adverse weather	[ ]
Interruption to utility supply	[ ]
Fire	[ ]
Security incident	[ ]
Health & Safety incident	[ ]
Act of terrorism	[ ]
New laws or regulations	[ ]
Loss of site	[ ]
Loss of IT Capacity	[ ]
Loss of Skills	[ ]
Military Strike	[ ]
Pressure group Protest	[ ]

Other ……

8. How frequently is the county's business continuity plan reviewed?

Every Yearly Quarter	[ ]
Every 2 yearly quarters	[ ]
Once per Year	[ ]
Every 2 years	[ ]
Every 3 years	[ ]
Never reviewed	[ ]

9. Has IT Service Continuity Plan/DRP exercised reveled any weakness in its effectiveness and have these bee reviewed and rectified?

Yes, but not yet been rectified	[ ]
Yes, have been rectified	[ ]
No.	[ ]
Not aware	[ ]

10. At what level is your IT Service Continuity Plan/DRP exercised?

IT recovery only	[ ]
Workplace and Site recovery	[ ]

11. Within the County who is?
    a) Responsible for IT Service Continuity Plan/DRP?
    b) Involved in creating IT Service Continuity Plan/DRP?
    c) Not aware [ ]

12. Are you familiar with any IT Frameworks?
    {Tick where appropriate}

COSO	[ ]
ITIL	[ ]
Cobit	[ ]
ISO 29000	[ ]

13. Which other functions in the County included in your IT Service Continuity Plan/DRP?
    {Tick where appropriate}

Finance	[ ]
Supplies and Purchasing	[ ]
IT	[ ]
Security	[ ]
Environment & Natural Resources	[ ]
HR	[ ]
Public Relations	[ ]
Other ……	

SECTION C: IT Service Continuity Plan/DRP salient features. *{Tick where appropriate}*

1. Are there IT Service Continuity and Disaster recovery policy with senior management

   Yes [ ] No [ ] Partially [ ]

2. Does the county have a budget allocated for IT Service Continuity Plan and disaster recovery?

   Yes [ ] No [ ] Partially [ ]

3. Through a review of the backup procedures with staff within each division, is it evident that they are aware of their responsibilities, especially with respect to protection of data and software?

   Yes [ ] No [ ] Partially [ ]

4. Are there internal emergency responders to develop plans for helping the County during emergency?

   Yes [ ] No [ ] Partially [ ]

5. Has the IT Service Continuity Plan/DRP Team undertaken Risk Assessment or Business Impact Analysis and implemented necessary safety measures to protect ICT assets in the county? (Logical and Physical security).

   Yes [ ] No [ ] Partially [ ]

6. Do IT Service Continuity /DR include people, premises, technology and information?

   Yes [ ] No [ ] Partially [ ]

7. Is ICT-A and or Transition Authority or any central government body aware of a IT Service Continuity /DR Plans procedure and aware of what to do in case of a disaster event?

   Yes [ ] No [ ] Partially [ ]

8. Are Backup systems and files stored off-site?

   Yes [ ] No [ ] Partially [ ]

9. Does transfer of data occurs immediately after backup?

   Yes [ ] No [ ] Partially [ ]

10. Does the documentation of the service providers also review of copies of their backup plans?.

    Yes [ ] No [ ] Partially [ ]

11. Have the service providers' backup plans been tested with respect to backup of the County's services?

    Yes [ ] No [ ] Partially [ ]

12. What is the maximum tolerable outage (MTO) for a power disruption the County can tolerate?

    0-6hrs [ ] 6-24 hrs [ ] 1-3days [ ] 3-7 days [ ] > 7days [ ]

13. What is the maximum tolerable outage (MTO) for internet connectivity the institution can accommodate?

    0-6hrs [ ] 6-24 hrs [ ] 1-3days [ ] 3-7 days [ ] > 7days [ ]

14. What is the frequency of Conducting IT Service Continuity Plan/DRP and Disaster Recovery test in the County?

    Every Quarter [ ] Every half yr [ ] 1 – 2 yrs [ ] 3-5 yrs [ ]

15. Have the plans been tested for a worst case scenario?

    Yes [ ] No [ ] Partially [ ]

16. Do testing provide details to indicate that.

a. The test was evaluated?	Yes [ ]	No [ ]	Partially
b. Any cited deficiencies were documented?	Yes [ ]	No [ ]	Partially
c. Deficiencies were corrected?	Yes [ ]	No [ ]	Partially
d. Deficiencies were retested?	Yes [ ]	No [ ]	Partially

17. From previous tests lesson learned used in improving IT Service Continuity Plan/DRP?

    Yes [ ] No [ ] Partially [ ]

18. Is there updated IT Service Continuity Plan/DRP arrangement that include your incident management process, notification procedures, recovery procedures and the estimated recovery time?

    Yes [ ] No [ ] Partially [ ]

19. Were the following areas, at a minimum, tested?

a. Data files?	Yes [ ]	No [ ]	Partially [ ]
b. Equipment?	Yes [ ]	No [ ]	Partially [ ]
c. Backup equipment?	Yes [ ]	No [ ]	Partially [ ]