

## DECLARATION

I Godfrey Chege Karugu, declare that this research project is entirely my own work and where there is work or contribution of others it has been acknowledged. To the best of my knowledge, this research work has not been presented to any other education institution of similar purpose or forum.

Signature  \_\_\_\_\_

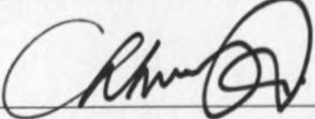
Date 24/04/2012

Godfrey Chege Karugu

Reg. No: P56/72444/2008

---

This research has been submitted for examination with my approval as the university supervisor.

Signature  \_\_\_\_\_

Date 26 April 2012

Christopher A. Moturi

Deputy Director

School of Computing and Informatics

University of Nairobi

## **DEDICATION**

**To my wife**

**Winnie**

**And**

**Our children**

**James and Shiprah**

## **ACKNOWLEDGEMENT**

My sincere gratitude goes to my Supervisor Christopher A. Moturi for his endless support and guidance in this journey. The MSc Project Assessment Panel of Dr Peter Waiganjo, Dr Agnes Wausi, Mr Daniel Orwa and Mr Joseph Ogutu who thoroughly scrutinized my work and gave their valuable contribution.

I would also like to appreciate the kind support from the Director ICTC and permission to carry out my research at ICTC. The entire staff at the ICTC also deserves mention for their assistance and response to the questionnaires.

I am grateful to my family for the love and support during this journey. Your being there for me gave me the impetus to continue even when the going seemed tough.

Finally and most important to the Almighty God, who gave me strength, courage, grace and all that I needed to accomplish this work.

## **ABSTRACT**

Information systems are vulnerable to a variety of attacks such as power shortages, disk failure, equipment destruction, fire and terrorist attack. It is therefore important to undertake IS contingency planning to safeguard against loss caused by such attacks. The study was to develop a model information systems contingency plan for universities. A cases study of the University of Nairobi was taken.

The study was conducted through a cross sectional descriptive case study. A questionnaire was used to collect primary data from the selected population. One questionnaire was administered to end users of information systems at the University of Nairobi. A different questionnaire was administered to the technical staff. The population of the study was all the end users of information systems at the University of Nairobi and 112 technical staff who work at the ICT Center. Applying a formula for determining sample size, a sample of 68 end users and 68 technical staff were selected using stratified sampling.

Findings from end users indicated that business impact analysis, recovery strategies formulation, plan testing, conducting staff awareness program and plan maintenance are crucial steps in coming up with an IS contingency plan. The study found out that the most critical information systems at the University of Nairobi were the Student Management Information System, followed by Human Resource Management Information System and the Financial Management System.

The minimum IT resources that are required to support the critical information systems include; authentication server, web server which supports the three critical IS systems identified (SMIS, HRMIS, FIMS), database server, e-mail server, student database, LAN/WAN with associated routers, hubs and fiber connections, and power supply. The study developed an IS contingency plan which incorporated the BIA output, recovery procedures and plan appendices.

3.5.1	Validity .....	23
3.5.2	Reliability .....	24
3.6	Develop an IS Contingency Planning Model .....	24
CHAPTER FOUR: RESULTS AND DISCUSSION.....		25
4.1	Introduction .....	25
4.2	Response Rate .....	25
4.3	Demographic Analysis .....	25
4.4	Responses from End Users.....	26
4.4.1	Business Impact Analysis .....	27
4.4.2	Recovery Strategy Formulation.....	27
4.4.3	Plan Testing .....	28
4.4.4	Contingency Plan Awareness .....	29
4.4.5	Plan Maintenance.....	30
4.5	Response from Technical Staff .....	30
4.5.1	Critical Information Systems .....	31
4.5.2	Resources Supporting Critical Information Systems.....	31
4.5.3	Student Management Information System .....	32
4.5.4	Human Resource Management Information System .....	34
4.5.5	Financial Management System.....	36
4.6	IT Resources for Critical Information Systems.....	39
4.7	Outage Impacts and Allowable Outage Times.....	39
4.8	Prioritization of Resource Recovery .....	40
4.9	Result of the BIA and the Model IS Contingency Plan .....	41
CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS .....		42
5.1	Summary of Achievements .....	42
5.2	Limitation of the Study.....	45
5.3	Conclusion.....	46
5.4	Further Research and Practice.....	47
REFERENCES .....		48
Appendix I: Proposed University of Nairobi Information Systems Contingency Plan.....		52
Appendix II: Information Systems End Users Questionnaire .....		77
Appendix III: ICTC Staff Questionnaire .....		82

## LIST OF TABLES

Table 2. 1: Contingency Plan Elements (Source: Researcher, 2011).....	18
Table 3. 1: Criteria for Selecting Sample Size .....	21
Table 3. 2: Sample Size ICTC Staff .....	22
Table 3. 3: Sample Size End Users.....	23
Table 3. 4: Reliability Test .....	24
Table 4. 1: Response Rate .....	25
Table 4. 2: Gender Cross Tabulation .....	25
Table 4. 3: Age Cross Tabulation .....	26
Table 4. 4: Length of Service .....	26
Table 4. 5: College/ Campus .....	26
Table 4. 6: Recovery Strategies Formulation .....	28
Table 4. 7: Critical Information Systems.....	31
Table 4. 8: Outage Impacts and Allowable Outage Time .....	40
Table 4. 9: Recovery Priority.....	40

## LIST OF FIGURES

Figure 2. 1: Contingency Planning; an element of Risk Management .....	7
Figure 2. 2: Security Risk Planning Model .....	8
Figure 2. 3: Contingency Planning: NIST Model.....	14
Figure 2. 4: Disaster Recovery Planning Model : ISO/IEC 24762:2008 .....	17
Figure 2. 5: Proposed University of Nairobi IS Contingency Plan Model .....	19
Figure 4. 1: Business Impact Analysis .....	27
Figure 4. 2: Plan Testing.....	29
Figure 4. 3: Contingency Plan Awareness.....	30
Figure 4. 4: Plan Maintenance .....	30
Figure 4. 5: SMIS Servers .....	32
Figure 4. 6: SMIS Databases .....	32
Figure 4. 7: SMIS Network Resources.....	33
Figure 4. 8: SMIS Operating Systems .....	33
Figure 4. 9: SMIS End Computing Devices .....	34
Figure 4. 10: HRMIS Servers .....	34
Figure 4. 11: HRMIS Databases.....	35
Figure 4. 12: HRMIS Network Resources.....	35
Figure 4. 13: HRMIS Operating Systems.....	36
Figure 4. 14: HRMIS End Computing Devices.....	36
Figure 4. 15: FIMS Servers .....	37
Figure 4. 16: FIMS Databases .....	37
Figure 4. 17: FIMS Network Resources .....	38
Figure 4. 18: FIMS Operating Systems .....	38
Figure 4. 19: FIMS End Computing Devices .....	39

# CHAPTER ONE: INTRODUCTION

## 1.1 Background of the Study

The use of ICT's has the potential to enhance the quality of teaching and learning, the research productivity of the faculty and students, and the management and effectiveness of learning institution (KENET, 2006). However information systems are vulnerable to a variety of attacks such as power shortages, disk failure, equipment destruction, fire and even terrorist attack.

Though it is impossible to eliminate all the risks that would affect information systems, the effect of these risks can be eliminated or minimized through technical, management or operational solutions. IS contingency planning refers to a coordinated strategy involving plans, procedures and technical measures that involve the recovery of IS operations and data after a disruption (NIST, 2002). Measures adopted to restore the IS services may include relocation of IS and operations to an alternate location, using alternate equipments or performing the affected business processes manually. By developing an information systems contingency plan, an organization is able to reduce losses during times of information systems disruptions while abiding to serve customers and maintain administrative operations.

There is an inherent relationship between information systems and the business process they support; hence an IS contingency plan must be part of a broader emergency preparedness environment that includes business process continuity and recovery planning.

Other plans within this environment includes business continuity plan, business recovery plan, continuity of operations plan, crisis communication plan, cyber incident response plan, disaster recovery plan and occupant emergency plan.

Every hour that an organization's information resources are unavailable not only costs revenues, it damages its reputation and competitive advantage. The challenge is worse off for an organization that offers online services to customers and is struck by a disaster without a



contingency plan since the customers get to know about the disruption at the same time as the host organization (Smith, 2003). The cost of information systems disruptions is substantial and organizations must therefore be proactive in protecting this important resource.

Information systems contingency plan is not only vital for profit oriented organizations but also for educational institutions which are facilitating teaching, learning and research activities. For institutions of higher education, contingency plan ensures the ability to resume information processing operations in a timely manner to the management, faculty, students and other stakeholders, should a disruption to the institutions information systems occur. The failure of an institution to prepare a comprehensive contingency plan could lead to significant financial consequences, interruptions to the academic schedule, the failure of current research projects, or other unforeseen delays to the completion of critical activities.

## **1.2 Problem Statement**

The potential impact of system failure can have negative consequences to academic institutions such as University of Nairobi. For instance, the failure of the integrated Financial Management System could lead to loss of revenue to the university through fraud and incorrect data capture.

In addition, it would lead to standstill in the recruitment and admission as it is used in the enrollment process. From an operation point of view, the failure of systems that capture student results would have devastating impact on the reputation of the university and threaten its future business opportunities.

The risk levels to the University information systems will probably increase as the IT adoption increases in Kenya. This trend implies that the potential threat to information systems is not only a historical phenomenon but also a current and a future problem. This reveals that if academic institutions do not put in place contingency plans to safeguard against system failure, recovery

and continuity, the threat may become real. The problem for the University of Nairobi is how to continue effective service delivery in case of system failure.

### **1.3 Purpose of the Study**

The purpose of this study was to design a model for an IS contingency plan appropriate for any Kenyan university to enable the universities to continue effective delivery of services in the event that information system failure occur. The case of University of Nairobi was investigated to form a basis for the comparison of the contingency planning process in a Kenyan university and international approved models.

### **1.4 Research Objectives**

The research objectives for this study were:

- a) To establish the critical information systems within the University of Nairobi that are most vulnerable.
- b) To establish a systematic approach that can be used to develop an IS contingency plan.
- c) To develop a model IS contingency plan based on best practice as demonstrated by literature review.

### **1.5 Research Questions**

The researcher attempted to answer the following research questions.

- a) What are the critical information systems that are most vulnerable to system related failures at the University of Nairobi?
- b) What information system contingency plan model identified in the literature can be adapted to form a basis for the development of a contingency plan for the University of Nairobi?
- c) Does the contingency plan model meet the contingency requirements of the University of Nairobi information systems?

## **1.6 Justification**

There is a growing consumption of Information Technology in the accomplishment of university core business of research and dissemination of knowledge. Most universities have a well established ICT department which supports circulation of information within the university and with its stake holders, as well as facilitate other business process at the university. Coupled with this is the fact that there are threats, risks and vulnerabilities that threaten or cause disruption to Universities information systems. It is therefore the responsibility of the custodian of such systems to develop and document a contingency plan that would be implemented incase such threats strike and render the information systems unavailable. The findings of this study will provide a blue print for IS contingency planning incase of system failure at the University of Nairobi.

The study discuss the concept of contingency planning for information systems, uncover the critical information systems within the University of Nairobi that are most vulnerable, identify contingency planning models, and recommended a model that can be adapted by a Kenyan University to implement a contingency plan.

## **1.7 Significance of the Study**

It is hoped that the findings and the output of this study will be of major importance to the University of Nairobi stakeholders. Decision and policy makers will be able to make sound decisions and policies regarding the protection and recovery of information systems from an informed point of view. For instance, the University of Nairobi ICT Center may use the findings of this study as a blue print for contingency planning. Operation departments may also use the study findings in order to assess the risk inherent to their information systems and therefore put in place risk reduction and transfer mechanisms. The other Universities will also benefit since they can refer to the contingency plan model and improve or develop their own.

## CHAPTER TWO: LITERATURE REVIEW

### 2.1 The Need for IS Contingency Plan

According to Hoffman (1998), nearly 150 companies without disaster recovery plans did not survive when a bomb wrecked the World Trade Center in New York in February 1993. It was a case of learning too late that, organizations without working procedures for reacting to and recovering from a disaster places all its other plans and objectives in jeopardy.

Toigo (2003) posits that the time taken to recover critical business processes after a disruption is a universal determinant of a successful recovery. An interruption on an organization IS can cost a business heavily in terms of revenues, reputation, customers, and investors. The objective of IS contingency plan is to recover mission-critical processes within the least time possible following a disruption, to minimize its duration and costs.

Successful recovery and continuity of an IS largely depends on the availability of the following: a contingency plan which is regularly tested, a trigger mechanism to initiate the execution of the plan when a disaster strikes, a trained and assigned personnel to implement the Plan and resources with which to manage the recovery (Malombe, 2005)

The expressions “contingency planning” and “disaster recovery” concern the preparation of plans to be auctioned when unexpected adverse events occur that would have ill effects on an organization’s computer facilities, and thus on the organizations ability to do business (Blakley et al, 2002). This study therefore assumes that both contingency plan and Disaster Recovery Plan have the same meaning and refer to a formal written plan to cater for any contingencies within an information systems environment.

## **2.2 University of Nairobi**

In the Education sector, the adoption and use of ICT services is realized through the extent to which ICT supports and fosters innovative research, learning and teaching in addition to supporting administrative processes in these institutions. The University of Nairobi realized the strategic importance of ICT, and created a fully fledged ICT function, the ICT Centre in 2002, with the head of the centre, the Director ICTC reporting directly to the Vice Chancellor (UoN, 2009). To support the function, the University had over 112 highly qualified professional ICT staff to plan, implement and support its ICT infrastructure and services by the year 2011. Over 50% of the professional staff had Masters Degrees and above while the rest had B.Sc. or Higher Diploma in relevant areas.

The University of Nairobi Information and Communication Technology Policy Guidelines (2010) was developed to guide developers and users of information and ICT resources on appropriate standards to be adopted at the University.

The policy guideline has several elements which include;

- a) Network Development and Management Policy
- b) ICT Security and Internet Policy
- c) Software Development, Support and Use Policy
- d) User Support Policy
- e) ICT Equipment Maintenance Policy
- f) ICT Training Policy
- g) Database Administration Policy
- h) Procurement Policy

A critical review of the above policy indicates that conscious consideration of contingency planning has not been taken into account. The ICT security and internet policy touches on the backup requirements since it has a sub topic on systems backup policy. Specifically, the subtopic on system backup policy states that “All ICTC sections that operate key University systems shall

formulate and implement systematic schedules for performing regular backups on the systems in their custody". However, it does not specifically identify a documented information system contingency plan that would be implemented in the event of information system failure.

### 2.3 IS Contingency Planning and Risk Management Process

Risk management encompasses a broad range of activities to identify, control, and mitigate risks to information systems. From an IS contingency planning perspective, risk management has two primary functions: First, it should identify threats and vulnerabilities such that appropriate controls are put in place to prevent and limit the effects of a disruption. Second, it should identify residual risks for which contingency plans must be developed.

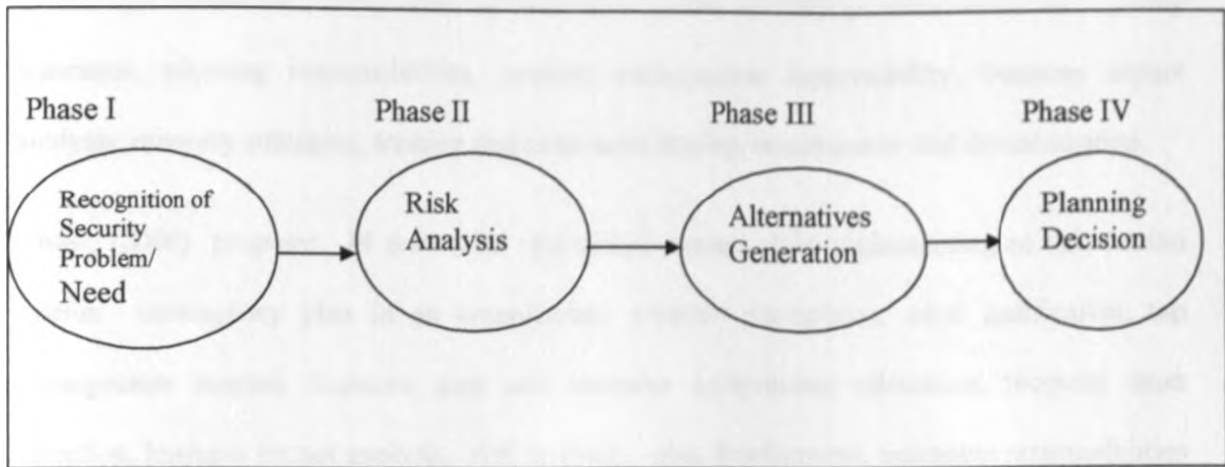
Figure 2.1 illustrates the relationship between identifying and implementing security controls, developing and maintaining the contingency plan, and implementing the contingency plan once the event has occurred (Swanson et al., 2002).



Figure 2. 1: Contingency Planning; an element of Risk Management.

### 2.4 The Security Risk Planning Model for Information Systems

This model derives its structures from Simon's model of decision making (Baskerville, 1993). It place risk analysis as a bridge between problem formulation and generation of alternatives and preceding the planning decision phase.



**Figure 2. 2: Security Risk Planning Model**

### **2.5 Information System Contingency Plan Constructs**

Most of the literature that discusses information systems contingency plan/Disaster Recovery Plan enumerates the factors that determine the success of such a plan either as events, components of the plan, operational steps, phases or constructs.

A study on the disaster recovery process of Chi/Cor Information Management Inc (Francis, 1993) proposes that there are ten phases followed in the implementation of an information systems contingency plan. They are: project organization, business impact analysis, security review, strategy development, testing the plan, plan maintenance and periodic audit of the plan.

A similar study by Dwyer (Dwyer et al, 1994) identifies nine success factors for information system contingency plan as from the reference guidelines of the System Auditability and Control report. These success factors are: organizing and managing the project, conducting organizational impact assessment, determine the minimum processing resources, analyzing system risks, prioritizing the tasks recovery process, selecting and analyzing alternatives, developing the contingency plan, testing the plan, and plan maintenance.

Smith and Sherwood (1995) come up with nine phases of DRP process which are: policy statement, planning responsibilities, incident management responsibility, business impact analysis, recovery strategies, training and awareness, testing, maintenance and documentation.

Chow, (2000) proposes 14 successful operational events while implementing an information system contingency plan in an organization: problem recognition, need justification, top management support, finances, time and resource commitment allocation, recovery team selection, business impact analysis, risk analysis, plan development, assigning responsibilities to the recovery team, back-up procedures, disaster implementation task, post-plan activities, testing and maintenance.

Wong et al. (2004) propose that an effective DRP for information system functions should consist of nine procedural steps which include: obtaining top management commitment, establishing a planning committee, performing risk and impact analysis, prioritizing recovery needs, selecting a recovery plan, selecting a vendor and developing agreement, developing and implementing the plan, continual testing and evaluating the plan.

Blatnik (1998) proposes nine phases for the successful implementation of an information systems contingency plan. These phases are: enforcement of policy, analysis of threat, back-up plan, training of recovery teams, testing the plan, Plan documentation, schedule and regular reviews, regular updates, and information system users' participation.

## **2.6 Information System Contingency Plan Constructs Discussion**

### **Top management commitment**

Top management commitment is considered the most vital construct to the success of IS contingency plan. Ginn (1989) states three reasons to support such a claim: first, top management finalizes an annual budget to support implementation of the Plan in an organization;



second, top management decides when and how the plan should be implemented in an organization;

third, top management dictates the level of cooperation and support that should be provided by the various departments when the plan is launched in an organization. Furthermore, this construct is considered as critically important because IS contingency plan requires long-term planning, and that it involves ongoing capital investment (Chow, 2000; Cerullo et al., 2004).

#### **Risk assessment and impact analysis**

Risk assessment and impact analysis determine how long an organization can survive without the support of critical business functions when a disaster strikes (Cerullo, 2004).

All critical functions must be pre-determined before a contingency plan strategy is chosen for an organization (Chow, 2000). Here, the risk assessment identifies the events that are most likely to pose threats to a firm (Cervone, 2006), and the impact analysis refers to the evaluation of the consequences of a disaster, such as the financial and non-financial loss of business functions (Blakley, 2002)

#### **Minimum processing requirement**

When a disaster strikes, no organization has sufficient time or resources to recover every business function in a short period of time. An effective IS contingency plan should therefore address the minimum processing requirement that would ensure that company operations are recovered to an acceptable level (Cerullo et al, 2004). The minimum processing requirement determines an acceptable recovery time, that is, the point in time to which data must be restored and the maximum allowable downtime of business functions that a company or functional unit can withstand (Wong et al., 2004).

#### **Alternative site**

Firms that highly dependent on IS applications must consider an alternative site with which they can back up their IS resources, so that they can be recovered easily in the event of a disaster (Blake, 2002).

Alternative sites can be operated on either an external site or in-house site, and can be implemented in the mode of a hot site, a cold site, mobile recovery facilities, or a mirrored site (Hawkins et al, 2000). The practice of each of these alternative sites has trade-off value, thus one must establish its selection criteria and then perform cost benefit analysis.

### **Recovery team**

The recovery team coordinates recovery tasks in an effective manner when a disaster strikes. Chow (2000) states that a team approach to managing the recovery process in the event of a disaster is important for two reasons: first, all relevant staff may not be presented when a disaster strikes; secondly, when more of the right people are involved, more intelligent answers to recovery problems may be generated.

### **Testing**

A series of test programs needs to be developed to make sure the IS contingency plan is a complete and accurate product. Testing should be designed in such a way that the weaknesses of the plan can be identified (Lee and Ross, 1995). The IS contingency plan should also be tested in such a way that it renders minimal disturbance to the daily operations of an organization.

### **Training**

Once the IS contingency plan is developed, all staff involved in the plan must know their roles and duties. A training program is therefore required to ensure that all staff understands their positions, which will subsequently reduce the potential for operational errors and the opportunity for miscommunication when the plan is implemented during a real disaster (Farahmand et al, 2003).

### **Documentation**

The documentation construct refers to a set of manuals and procedures that outlines for the IS contingency plan recovery team all respective events related to IS recovery in the event of a disruption. In addition, the exact details of functions, personnel, responsibilities, contact names and numbers, and resources for the recovery, involved with a disaster, must be documented (Hawkins et al, 2000).

### **Maintenance**

Cerullo (2004) claims that the creation of a IS contingency plan without periodic testing and ongoing maintenance is worse than not having a plan at all. The maintenance construct is important to reduce the likelihood of incorrect decisions being made and to decrease the stress of disaster-team members during the recovery process (Chow, 2000). Each time IS contingency plan is altered, those changes must be updated.

### **User's participation**

The users of information systems must participate and monitor the development processes of IS contingency plan in an organization (Wong et al, 2004). Due to the fact that the employees should know their duties and responsibilities within the disaster recovery process, they should review the plan and check whether the recovery operation procedures are operated as planned. In addition, IS personnel should review the IS contingency plan regularly from a technical standpoint so that minimum information systems service disruption are sustained (Blatnik, 1998).

## **2.7 Summary of IS Contingency Plan Constructs**

From the literature review, there are recurring constructs identified by the studies referred to in this study. These constructs can broadly be grouped together as they relate to each other from the different studies. The following grouping was considered in this study:

- a) Need for IS contingency plan: top management commitment, policy goals and steering committee.
- b) Business Impact Analysis and risk Analysis: Risk assessment and impact analysis, Prioritization, Minimum processing requirement.
- c) Prevention and recovery strategies: Alternative site, Backup storage, Recovery team.
- d) Documentation: Plan development.
- e) Training and Plan Testing: training, testing and personnel participation.
- f) Plan Maintenance: Plan maintenance.

This classification was informed by standard models used in the development of information systems contingency plan reviewed in this study. These models are:

- a) NIST model: IS Contingency Planning Guide.
- b) ISO/IEC 24762:2008: Framework for Disaster Recovery Planning.

## **2.8 NIST Model**

NIST (National Institute of Standards and Technology) is the body charged by the US Government with the development of standards for technology implementation to be used by government departments. It has developed a comprehensive guide that is used in the US to develop contingency plan for information systems by US government Departments. To develop and maintain a viable CP program for IS systems, the NIST model has recommended the following phases:

- Develop the contingency planning policy statement. A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
- Conduct the business impact analysis (BIA). The BIA helps to identify and prioritize critical information systems and the related components.
- Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

- Develop recovery strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- Develop contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
- Plan testing, training, and exercises. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall preparedness.
- Plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements.

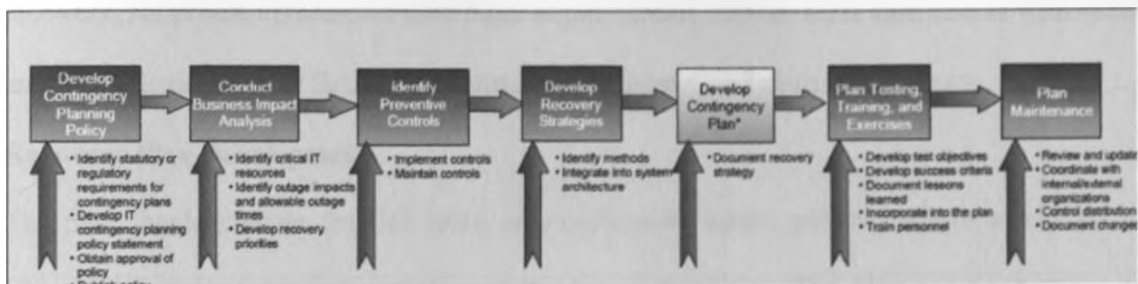


Figure 2. 3: Contingency Planning: NIST Model

## 2.9 ISO/IEC 24762:2008 Framework for Disaster Recovery Planning

To develop and maintain a viable contingency plan program for IS systems, ISO/IEC 24762:2008 recommends that an organization should implement the following phases:

### Business Impact Analysis

Business impact analysis will determine how long an organization can survive without the support of critical information systems during a disruption. BIA assists the plan coordinator to characterize the system requirements, process and interdependencies. The main purpose of BIA is to correlate system components with critical services that they support and characterize the consequence of a disruption. Based on this information the coordinator is able to identify critical IT resources, identify disruption impacts and their allowable outage times and hence develop recovery priorities.

### **Recovery Strategy Formulation**

The outage impacts identified in the BIA can be reduced by preventive measures that detect, deter or reduce disruption impacts on the system. Common preventive measures include; use of UPS, diesel-powered generators, fire and smoke detectors, offsite storage and frequent scheduled backup. Recovery measures, unlike preventive controls provide for information system recovery after a disruption. The strategies address disruption impacts and allowable outage times identified in the BIA. Some of the recovery strategies used include, alternate site, backup recovery, reciprocal agreements with other organizations, service level agreements with vendors and technologies such as RAID, UPS, automatic fail-over, and mirrored systems.

### **Recovery Plan Development**

The plan should contain detailed roles, responsibilities, teams, and procedures associated with restoration of the information systems following a disruption. The planning production stage includes detailed procedures that are executed during the Notification/Activation, Recovery and Reconstitution phases in case of a disruption. Identifying the teams and responsibilities for each team is an important activity of this stage.

### **Plan Testing**

Plan testing reveals the deficiencies in the plan. This also helps evaluate recovery teams' ability to implement the plan. Areas addressed in a contingency plan test include system recover on an alternate platform, coordination among recovery teams, internal and external connectivity, restoration of normal operations and notification procedures.

### **Plan Awareness**

Training of personnel should complement testing. Training should be provided at least annually; new hires who will have plan responsibilities should receive training shortly after they are hired. Staff should be trained to exercise the plan without the actual document, in case the document is

not available for the first few hours following a disaster. The personnel should be trained on specific plan elements such as; cross-team coordination, reporting procedures, individual and team responsibilities during the plan activation. A training program is therefore required to ensure that all staff understands their positions, which will subsequently reduce the potential for operational errors and the opportunity for miscommunication when the plan is implemented during a real disaster (Farahmand et al, 2003).

### **Recovery Plan Maintenance**

The implementation and feedback stage ensure that the contingency plan is a living document and reflect the current position of the information systems.

To keep up with the ever-changing information system technology, the IS contingency plan should be reviewed and tested on a regular basis and the findings incorporated in the respective phases of the plan.

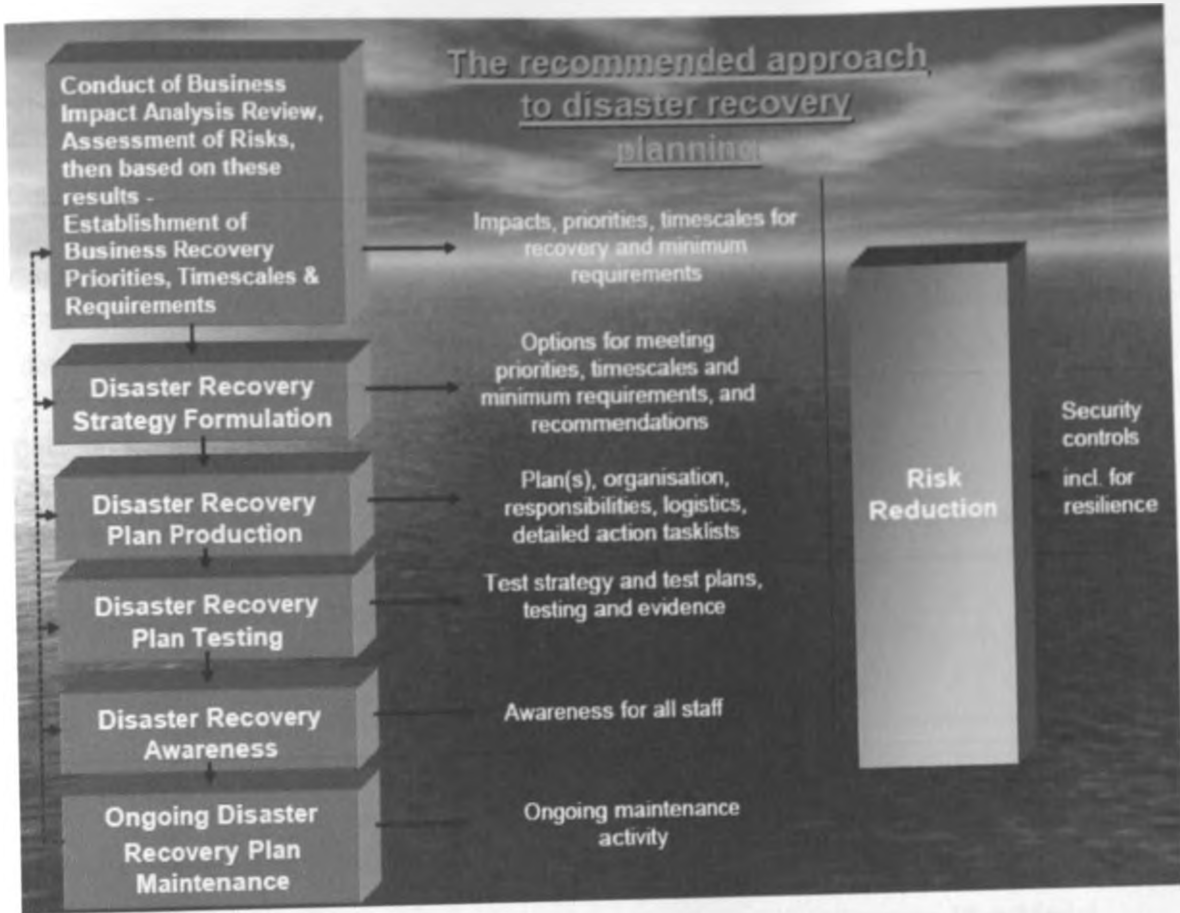


Figure 2. 4: Disaster Recovery Planning Model: ISO/IEC 24762:2008



## 2.10 Contingency Planning Elements from the Two Models: Comparison

NIST 800-34	ISO/IEC 24762:2008
Contingency Planning Policy Statement	Conduct BIA
Conduct BIA	
Identify Preventive Control	Recovery Strategy Formulation
Develop Recovery Strategies	
Develop Contingency Plan	Recovery Plan Development
Plan Testing, Training and Exercise	Plan Testing
	Plan Awareness
Plan Maintenance	Recovery Plan Maintenance

**Table 2. 1: Contingency Plan Elements (Source: Researcher, 2011)**

## 2.11 Proposed University of Nairobi Information System Contingency Plan Model

Based on the literature review and the standards referred to in this study, the researcher proposes the following information system contingency plan model for the University of Nairobi. This model is adapted from the ISO/IEC 24762:2008 model, since unlike the NIST model which is specifically for the USA government department, the ISO/IEC 24762:2008 is more flexible and can be adapted by organization in the world seeking to implement a comprehensive contingency plan. The NIST model requires implementation of the contingency plan to be aligned to specific regulator procedures which have been formulated for the USA departments.

However the two models identify the same elements for implementation of a contingency plan, with the exception of the contingency policy statement recommended by NIST, which requires an organization to identify the statutory requirements supporting the contingency plan development.

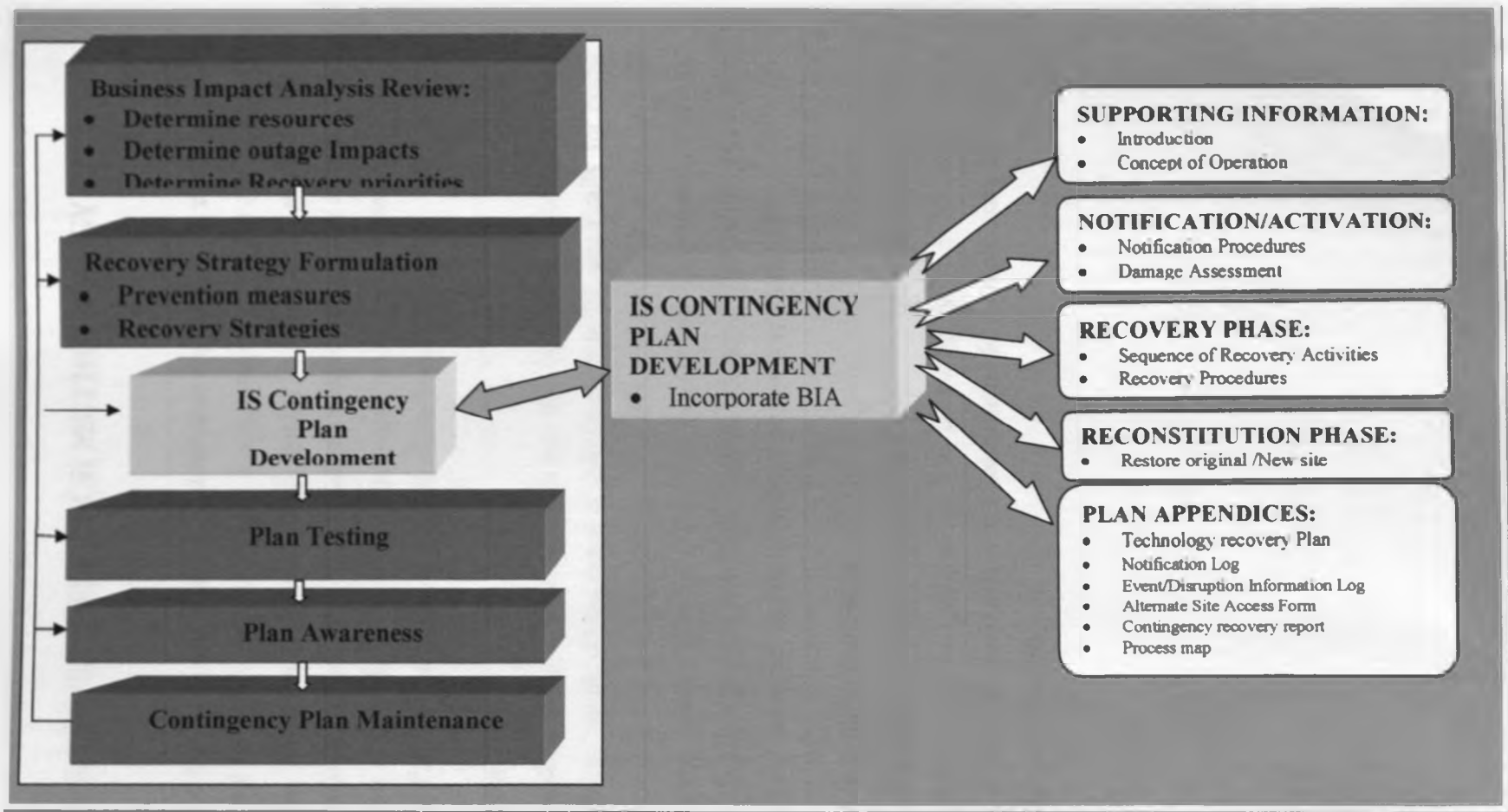


Figure 2. 5: Proposed University of Nairobi IS Contingency Plan Model

## **CHAPTER THREE: RESEARCH METHODOLOGY**

### **3.1 Research Design**

This study was conducted through a cross sectional descriptive case study. A cross sectional case study design is used to gather information on a population at a single point in time (Mugenda and Mugenda, 2003). Descriptive research design is a scientific method which involves observing and describing the behavior of a subject without influencing it in any way. Cross sectional descriptive case study is therefore appropriate because it is possible to obtain data from a cross section of staff at the University of Nairobi respectively.

### **3.2 Population of the Study**

In a research study, population refers to those who can provide the required information (Peil, 1995). A population therefore entails all the cases or individuals that fit specifically for being sources of the data required addressing the research problem. The target population was the staff in the four ICTC departments namely MIS Services, User Support and Maintenance, Network Infrastructure Services, Communication and Data Centre Services. The target population consisted of the 112 staff as given by the website link <http://ict.uonbi.ac.ke/node/274>.

### **3.3 Sample Size and Sampling Technique**

A simple approach to sample size calculation is to use the formula for calculating a sample size without putting into consideration the population. The following table is extracted from Mugenda and Mugenda (2003) and summarizes the calculations for sample sizes for survey research, assuming a probability of 50/50.

Accuracy (+/-) (Margin of error)	Confidence Level		
	90%	95%	99%
1	6765	9604	16576
2	1691	2401	4144
3	752	1067	1848
4	413	600	1036
5	271	384	663
10	68	96	166
20	17	24	41

**Table 3. 1: Criteria for Selecting Sample Size**

Mugenda and Mugenda (2003) further recommend the following formula for sample size determination;

$$n = p(1 - p) \left( \frac{z}{d} \right)^2 \quad \text{Where:}$$

n= sample size

z= the table value for the level of confidence, for instance 95% level of confidence =1.96, 90% level of confidence =1.645.

d= margin of error

p= proportion to be estimated, Mugenda and Mugenda (2003) recommends that if you don't know the value of p then you should assume p=0.5

Therefore, the sample size of this study was calculated as follows:

$$68 = 0.5(1 - 0.5) \left( \frac{1.645}{0.10} \right)^2$$

Therefore a stratified random sampling technique was used and yielded the following respondents. To identify the actual respondents, a form of random sampling technique known as the lottery method was used. A proportion of 68/112 was used to arrive at the number of respondents in each department.

Department	Population	Sample size
MIS Services	32	20
User Support and Maintenance Services	41	25
Network Infrastructure Services	9	5
Communication and Data Centre Services	30	18
<b>Total</b>	<b>112</b>	<b>68</b>

**Table 3. 2: Sample Size ICTC Staff**

The formula by Mugenda and Mugenda (2003) was also used to identify the number of users across the departments of users. This sample size was arrived at after considering seven departments namely Student Registration, Finance, Administration and Human Resource, Health, Performance Contract, Accommodation, and Library. Eleven users of information systems from every department and two from performance contract department were selected so as to give detailed account of the questionnaire.

To identify the actual respondents, a form of random sampling technique known as the lottery method was used.

$$n = p(1 - p) \left( \frac{z}{d} \right)^2 \quad \text{Where:}$$

n= sample size

z= the table value for the level of confidence, for instance 95% level of confidence =1.96, 90% level of confidence =1.645.

d= margin of error, ( 10% for current study)

p= proportion to be estimated, Mugenda and Mugenda (2003) recommends that if you don't know the value of p then you should assume p=0.5

Therefore, the sample size of this study was calculated as follows:

$$68 = 0.5(1 - 0.5) \left( \frac{1.645}{0.10} \right)^2$$

<b>Department</b>	<b>Sample</b>
Student Registration	11
Finance	11
Administration and Human Resource	11
Health	11
Performance Contracting	2
Accommodation	11
Library	11
Total	68

**Table 3. 3: Sample Size End Users**

### **3.4 Data Collection**

The study used primary data that was collected through a self administered questionnaire. According to Peil (1995) a questionnaire is a means of eliciting the feelings, beliefs, experiences, perceptions, or attitudes of some sample of individuals. The questionnaire is preferred because it is easier to administer, analyze and economical in terms of time and money. The questionnaire comprised both open and closed ended questions.

There were two sets of questionnaires. One set was administered to the end users spanning across seven departments. Another set of a questionnaire was distributed to technical respondents who are conversant with technical ICT details. The respondents are spread across the four ICTC departments.

### **3.5 Pilot Test**

The questionnaire was subjected to a review by experts in the area of information systems security who gave their contribution towards the content of the data collection tool. This was done to check whether the concepts in the questionnaire were clear. The input from this discussion was added to the questionnaire before distributing the questionnaire to the respondents.

#### **3.5.1 Validity**

According to Cooper & Schindler (2007) validity is extent to which a given finding shows what is believed to show. In order to confirm the validity of the research tool they were carefully examined to confirm proper coverage of the research objectives and ensure content validity. Patton (1990) refers to content validity as meaning that the instruments comprised a representative sample of all the possible items for each category area.

### 3.5.2 Reliability

Reliability is that quality of measurement method that suggests that the same data will be collected each time in repeated observation of the same phenomenon (Chandran, 2004). The reliability of the questionnaire was determined through a pilot study. According to Kothari (1990) 1 to 5% of sample size is adequate for pilot testing. The respondents for pilot test were 8 members of staff working at the University of Nairobi. Cronbach's coefficient Alpha formula was used to estimate the internal consistency of the study tool (Breakwell, 1995). The reliability coefficient of 0.7 and above was recommended (Cronchbach, 1951).

Section	No of questions	Cronbach alpha	Cutoff	Comment
Conducting Business Impact Analysis	5	0.789	0.7	Reliable
Recovery Strategy Formulation	13	0.842	0.7	Reliable
Plan Testing	12	0.875	0.7	Reliable
Contingency Plan Awareness	4	0.892	0.7	Reliable
Plan Maintenance	2	0.800	0.7	Reliable

Table 3. 4: Reliability Test

### 3.6 Develop an IS Contingency Planning Model

The final outcome of all these activities was to develop an information systems contingency planning model. The researcher used the results of the questionnaire as the basis of the IS contingency plan model. The model is attached as appendix I.

## CHAPTER FOUR: RESULTS AND DISCUSSION

### 4.1 Introduction

The chapter attempted to analyze the data and derive meaningful findings. The discussion of the data results and the implications of the finding were also presented in this chapter. Overall, data analysis was done in line with study objectives.

### 4.2 Response Rate

The successful response from the end users category was 59% while the technical staff category had a successful response rate of 51%. Overall, the successful response rate was 55% implying that out of the 136 questionnaires handed out, only 75 were properly filled and/or returned. According to Mugenda and Mugenda (2003), a response rate of 50% or more is adequate for data analysis.

	Successful	Unsuccessful	Total
End users	40-59%	28-41%	68
Technical staff	35-51%	33-49%	68
Total	75-55%	61-45%	136

Table 4. 1: Response Rate

### 4.3 Demographic Analysis

#### Gender Cross Tabulation

Overall ,there were more male respondent (61%) than female (39%) as indicated by table 4.2

	Male	Female	Total
End users	22-55%	18-45%	40-100%
Technical staff	24-69%	11-31%	35-100%
Total	46-61%	29-39%	75-100%

Table 4. 2: Gender Cross Tabulation

#### Age Cross Tabulation

Results indicate that overall, the majority of respondents were aged 31 to 40 years (56%). This was supported by a majority response from the end user category (58%) and technical user category (56%). The finding may imply that majority of the sample respondents are youthful and dynamic.



	21-30 years	21-30 years	31-40 years	31-40 years	41-50 years	41-50 years	Total
End user	0	0%	23	58%	17	43%	40
Technical staff	12	34%	19	54%	4	11%	35
Total	12	16%	42	56%	21	28%	75

**Table 4. 3: Age Cross Tabulation**

#### **Length of service Cross Tabulation**

A majority of respondents in the end user category (58%) had worked with the University of Nairobi for more than 5 years. Respondents in the technical user category had worked for the University for between 3-5 years (37%) .

	< 1 year	< 1 year	1-3 years	1-3 years	3-5 years	3-5 years	> 5 years	> 5 years	Total
End user	0	0%	12	30%	5	13%	23	58%	40
Technical staff	13	37%	13	37%	0	0%	9	26%	35
Total	13	17%	25	33%	5	7%	32	43%	75

**Table 4. 4: Length of Service**

#### **College/Campus**

A majority of respondents from the technical user category were from the Chiromo campus (71%). This is evident since the ICTC is located at the Chiromo Campus where most of the technical staff are located. The other campuses only have user support staff stationed there to assist the end users in their daily operations.

	Upper Kabete	Chiromo	Main Campus	Kikuyu Campus	Kenya Science	Lower Kabete	Total
End user	2-5%	3-7.5%	22-55%	4-10%	3-7.5%	6-15%	40
Technical staff	2-6%	25-71%	2-6%	2-6%	2-6%	2-6%	35
Total	4-11%	28-78.5%	24-61%	6-16%	5-13.5%	8-21%	75

**Table 4. 5: College/ Campus**

#### **4.4 Responses from End Users**

This section attempted to determine the crucial steps in coming up with an information systems contingency plan. Several steps were investigated ranging from business impact analysis to plan maintenance.

#### 4.4.1 Business Impact Analysis

The study sought to establish whether conducting a Business Impact Analysis is a crucial step in coming up with an information systems contingency plan. Results indicate that a majority of end users strongly agreed with the statement that BIA is important in identifying and prioritizing critical information systems (63%), identifying outage impacts and allowable outage times (43%), identifying critical IT resources (60%), determine the minimum IT resources for critical information systems (63%) and prioritizing information systems recovery during a disruption (60%).

The findings agree with those of Chow (2000) who argues that risk assessment and impact analysis determine how long an organization can survive without the support of critical business functions when a disaster strikes.

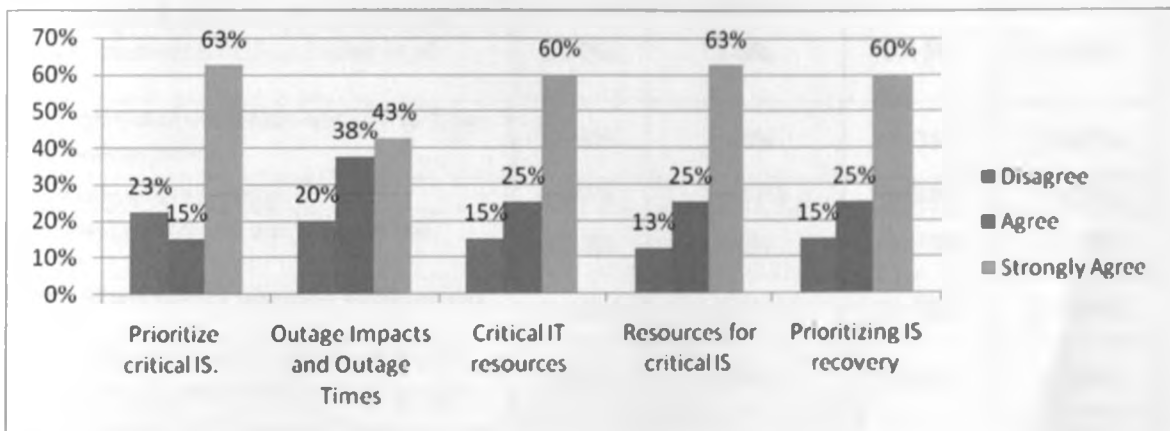


Figure 4. 1: Business Impact Analysis

#### 4.4.2 Recovery Strategy Formulation

The study sought to establish whether identifying preventive controls and recovery measures is a crucial step in coming up with an information systems contingency plan. A majority of end users strongly agreed that it is important to have frequent, scheduled backups (78%), commercial contracts for information systems recovery with cold, warm, or hot site vendors (35%), uninterruptible power supplies (UPS) to provide short-term backup power to all systems (60%), diesel-powered generators to provide long-term backup power (45%), fire, smoke detectors and suppression system (53%). However, the respondents could not make up their mind about air-conditioning systems (43%) and reciprocal agreements with internal or external organizations (48%). The findings agree with those of Blake, (2002) who asserts that firms that are highly dependent on information systems must consider an alternative site with which they can back up

their information systems resources, so that they can be recovered easily in the event of a disaster. The findings further agree with those of Hawkins et al, (2000) who argues that alternative sites can be operated on either an external site or in-house site, and can be implemented in the mode of a hot site, a cold site, mobile recovery facilities, or a mirrored site.

	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Frequent, scheduled backups	4-10%	0-0%	5-13%	31-78%
Commercial contracts for IS recovery with cold, warm, or hot site vendors	5-13%	10-25%	14-35%	11-28%
Uninterruptible power supplies (UPS) to provide short-term backup power to all systems	8-20%	3-8%	5-13%	24-60%
Diesel-powered generators to provide long-term backup power	8-20%	0-0%	14-35%	18-45%
Air-conditioning systems	4-10%	17-43%	8-20%	11-28%
Fire, smoke detectors and suppression system	4-10%	0-0%	21-53%	15-38%
Water sensors in the computer room ceiling and floor	0-0%	0-0%	23-58%	17-43%
Plastic tarps that may be unrolled over IT equipment to protect it from water damage	5-13%	4-10%	20-50%	11-28%
Heat-resistant and waterproof containers for backup media and vital non electronic records	5-13%	4-10%	10-25%	21-53%
Emergency master system shutdown switch	5-13%	9-23%	11-28%	15-38%
Technologies such as automatic fail-over and mirrored systems	0-0%	11-28%	12-30%	17-43%
Reciprocal agreements with internal or external organizations	5-13%	19-48%	5-13%	11-28%
Service level agreements (SLAs) with the equipment vendors	5-13%	6-15%	20-50%	9-23%

**Table 4. 6: Recovery Strategies Formulation**

#### 4.4.3 Plan Testing

Results indicate that a majority of end users strongly agreed with the statement that system recovery on an alternate platform from backup media should be addressed in an information systems contingency plan test (63%), coordination among recovery teams should be addressed in an information systems contingency plan test (53%), internal and external connectivity should be

addressed in an IS contingency plan test (38%), system performance using alternate equipment should be addressed in an IS contingency plan test ( 53%), restoration of normal operations should be addressed in an IS contingency plan test (65%), notification procedures should be addressed in an IS contingency plan test (40%).

The findings agree with those of Lee and Ross(1995) who argues that a series of test programs needs to be developed to make sure the IS contingency plan is a complete and accurate product.

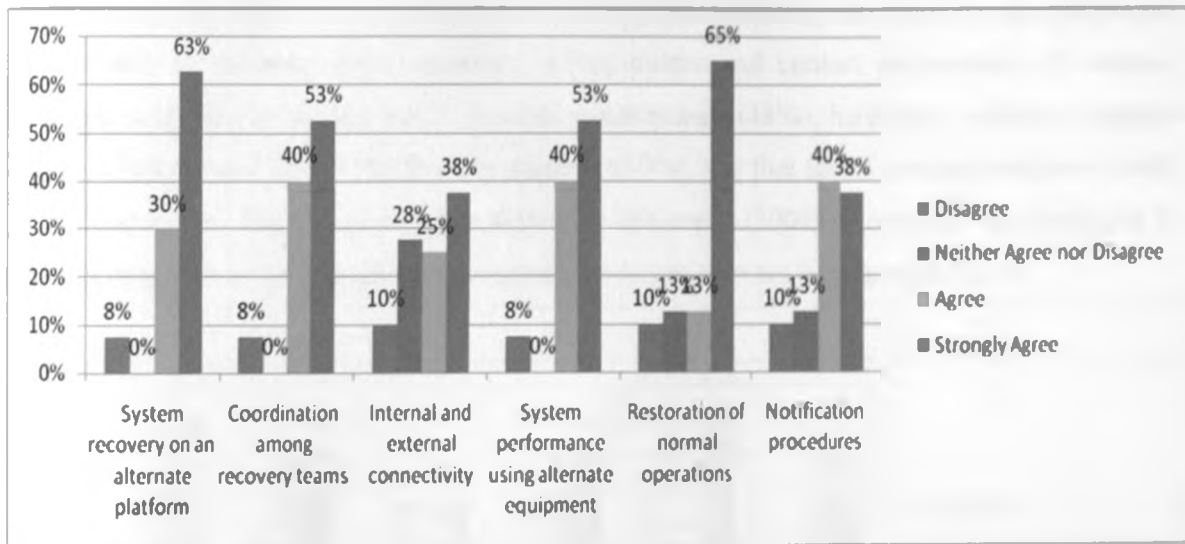


Figure 4. 2: Plan Testing

#### 4.4.4 Contingency Plan Awareness

Results indicate that a majority of end users strongly agreed with the statement that conducting staff awareness program for IS contingency planning is an important step in developing a contingency plan (65%), mandatory training for new employees in handling IS contingencies is an important step in developing a contingency plan (68%). The findings are consistent with those of Mitome et al (2001) who argues that once the IS contingency plan is developed, all staff involved in the plan must know their roles and duties. This ensures that all staff understands their positions, in the plan implementation and thus reduces the potential for operational errors and miscommunication.

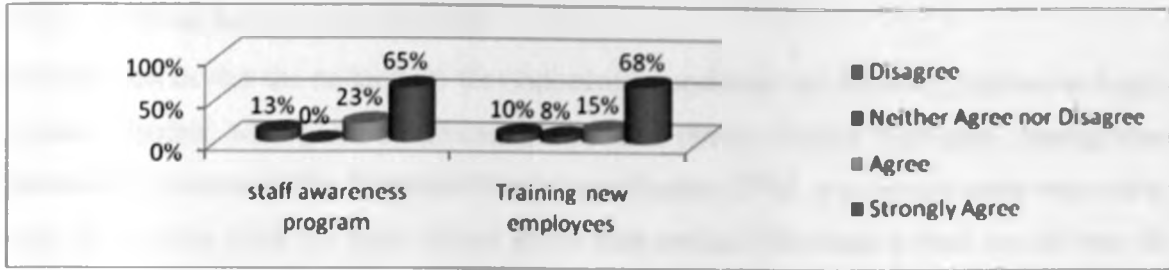


Figure 4. 3: Contingency Plan Awareness

#### 4.4.5 Plan Maintenance

Results indicate that the majority of respondents strongly agreed that at a minimum, the contingency plan should be reviewed and updated on the following elements, names and contact information of recovery team members (55%), names and contact information of vendors, alternate and off-site vendor POCs Security requirements (48%), hardware, software, changes (45%), alternate and offsite facility requirements (50%), and that the IS contingency plan should be audited (75%). The finds are in line with those of Cerullo (2004) who claims that having an IS contingency plan without ongoing maintenance is worse than not having a plan at all.

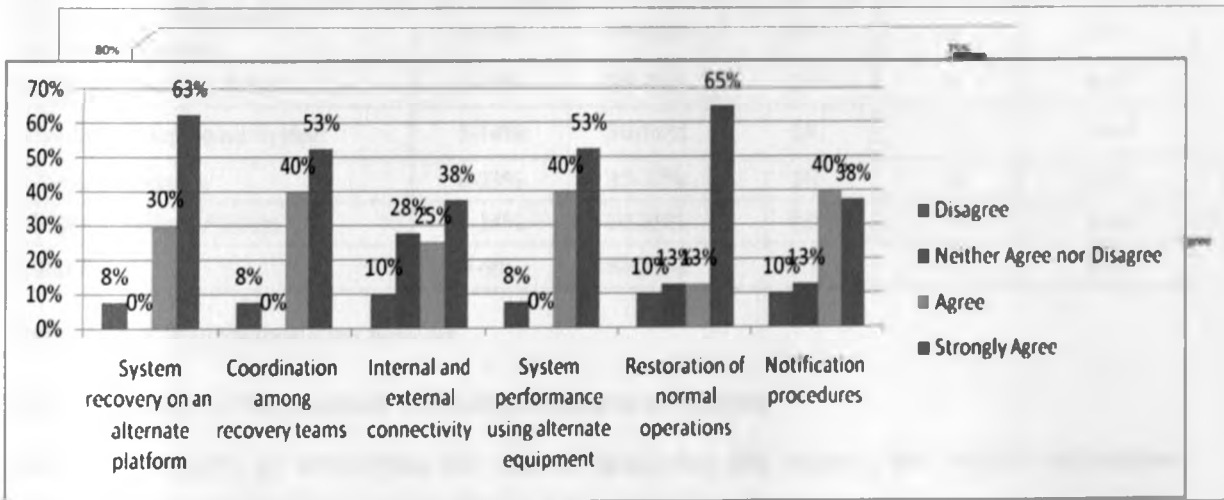


Figure 4. 4: Plan Maintenance

#### 4.5 Response from Technical Staff

The study attempted to get technical information from ICTC staff, the technical information provided the basis on which the information systems contingency plan was formulated.

#### 4.5.1 Critical Information Systems

Results indicate that the majority of the respondents considered the following systems as highly critical, Student Management Information System (86%), Human Resource Management Information System (66%), Financial Management System (57%). An average score was used to rank the systems from the most critical to the least critical. The most critical system was the Student Management Information System (0.86), followed by Human Resource Management Information System (0.66) and the Financial Management System (0.57) in that order.

System	Critical=1	Not critical=0	Number of respondents	Total score	Average Score
Student Management Information System	30-86%	5-14%	35	30	0.86
Human Resource Management Information System	23-66%	12-34%	35	23	0.66
Financial Management System	20-57%	15-43%	35	20	0.57
Online Room Booking and Allocation System	18-51%	17-49%	35	18	0.51
Performance Management Information System	6-17%	29-83%	35	6	0.17
University Health System	6-17%	29-83%	35	6	0.17
Joint Admission Board System	5-14%	30-86%	35	5	0.14
E-Learning System	8-23%	27-77%	35	8	0.23
Student Clearance System	5-14%	30-86%	35	5	0.14
Q-Pulse	3-9%	32-91%	35	3	0.09

**Table 4. 7: Critical Information Systems**

#### 4.5.2 Resources Supporting Critical Information Systems

The study sought to investigate the various resources that support the critical information systems. This was done by focusing on the specific information systems.

### 4.5.3 Student Management Information System

#### Servers

Several resources were found to be important in supporting the Student Management Information System. These were; web server (100%), database server (83%), application server (83%), and authentication server (67%). This is supported by the fact that all operations at University are performed online, making servers to be among the critical resources.

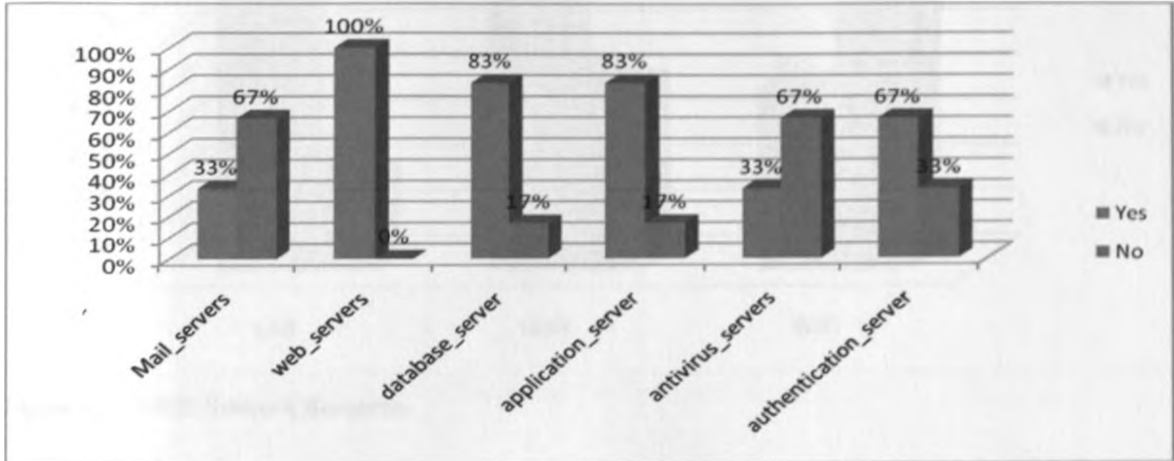


Figure 4. 5: SMIS Servers

#### Databases

The specific databases that are crucial in supporting the Student Management Information Systems include the student database (71%) and the financial database (57%).

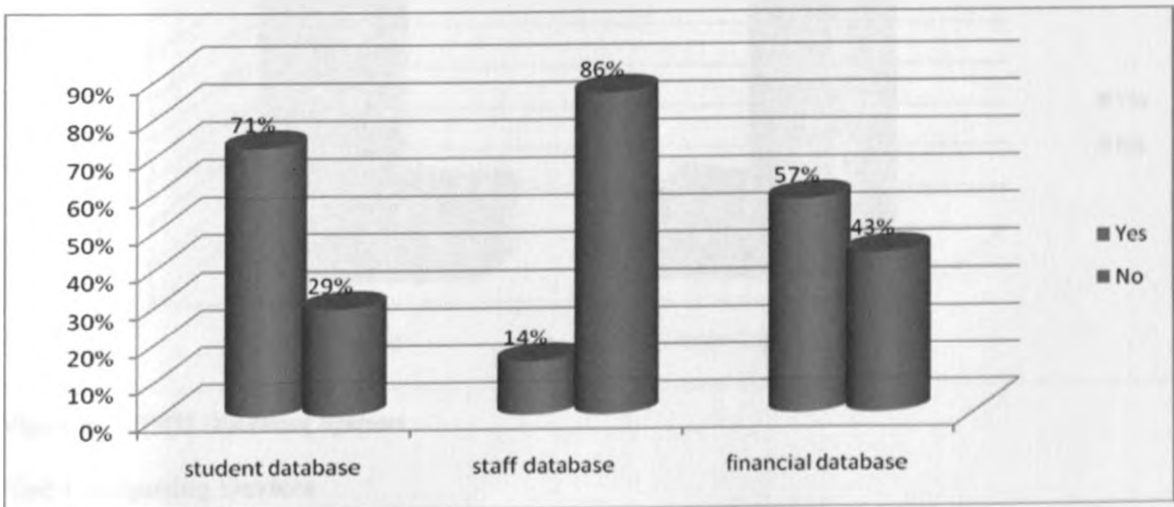


Figure 4. 6: SMIS Databases

### Network Resources

The network resources that supported the Student Management Information system included LAN resources as indicated 80% of the technical staff followed by WAN resources (60%).

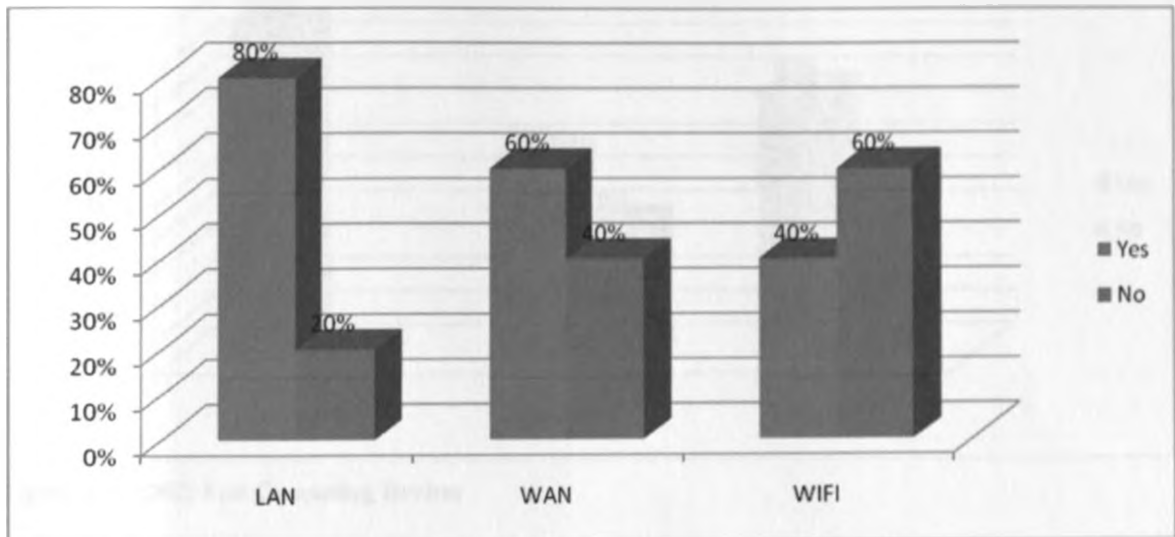


Figure 4. 7: SMIS Network Resources

### Operating Systems

The type of operating system that supports the Student Management Information System is Linux based as indicated by 80% of the technical staff.

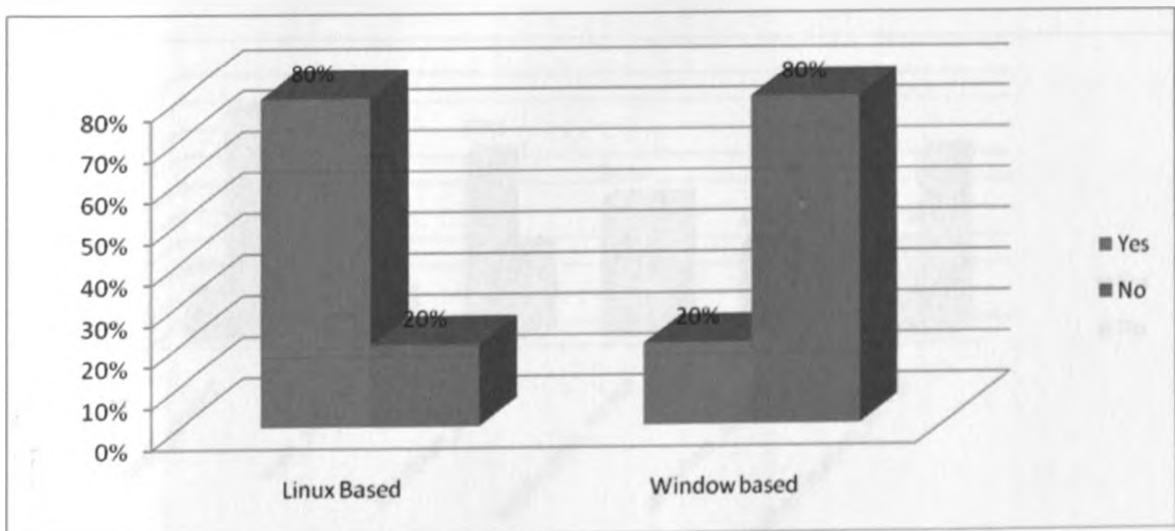


Figure 4. 8: SMIS Operating Systems

### End Computing Devices



The end computing devices that supported the Student Management Information System included desktops (100%), mobile (60%) and ipads (80%). Technical staff also indicated that laptops were some of the other end computing devices that are used.

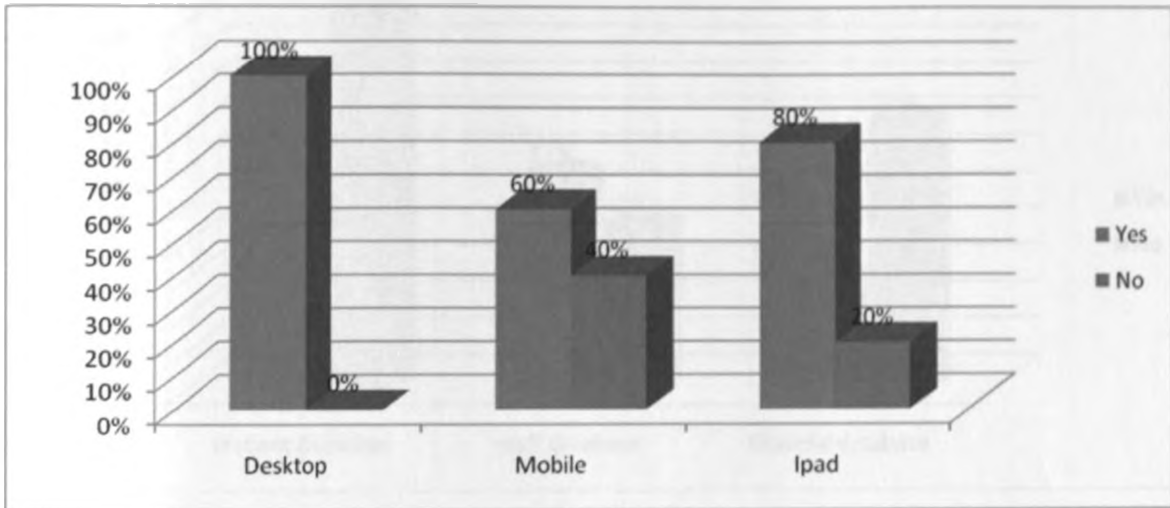


Figure 4. 9: SMIS End Computing Devices

#### 4.5.4 Human Resource Management Information System

##### Server

The servers that were found to be important in supporting the HRMIS included the web server (83%), database server (67%), and the application server (50%).

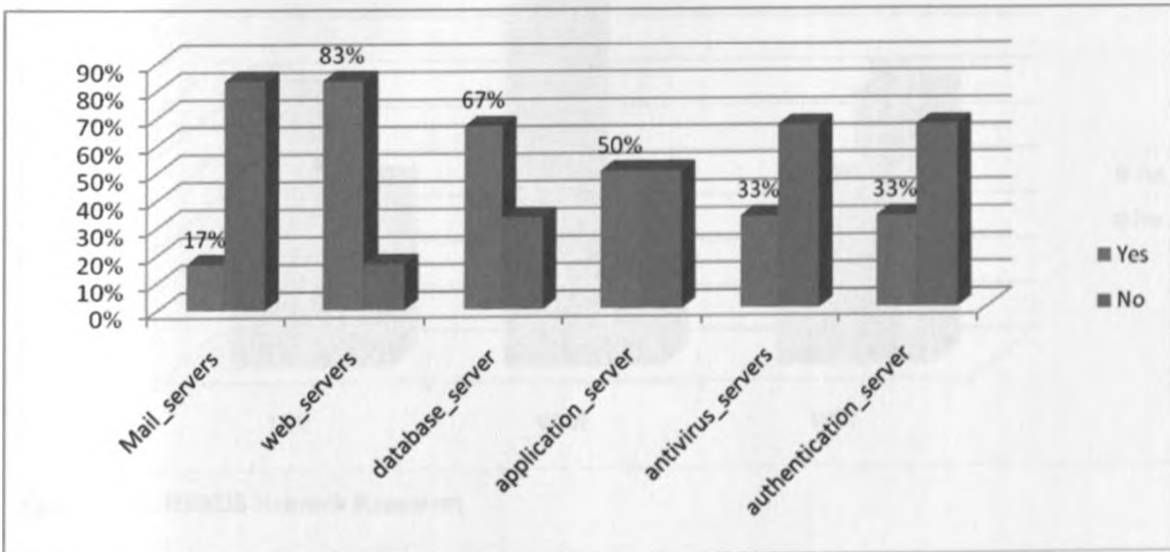


Figure 4. 10: HRMIS Servers

##### Database

The specific databases that are crucial in supporting the HRMIS include the staff database (57%). The financial database is also used though infrequently (29%).

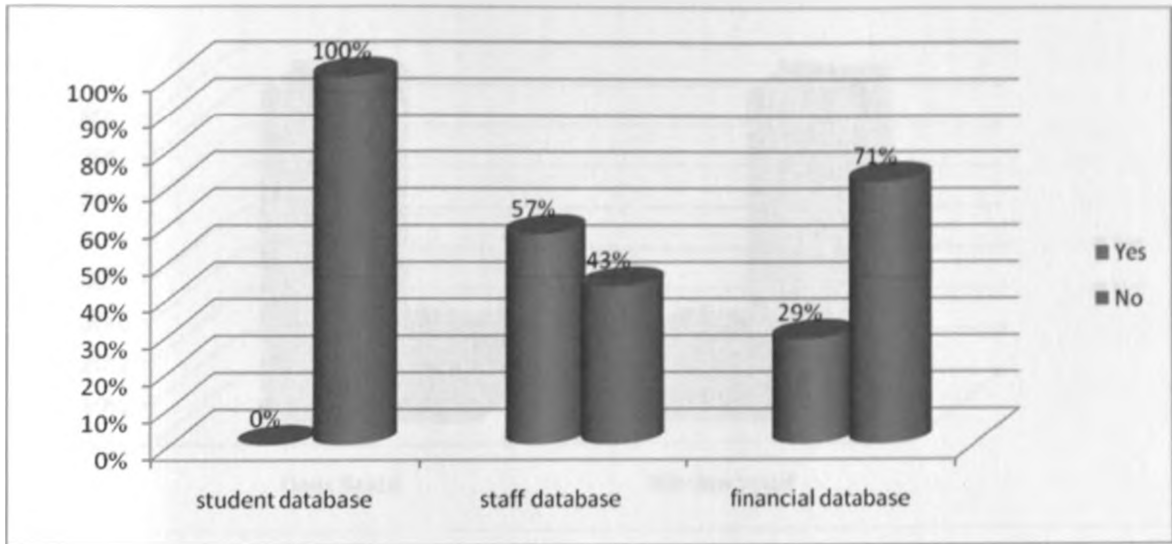


Figure 4. 11: HRMIS Databases

### Network Resources

The network resources that supported the HRMIS included WAN as indicated by 80% of the technical staff followed by LAN (60%).

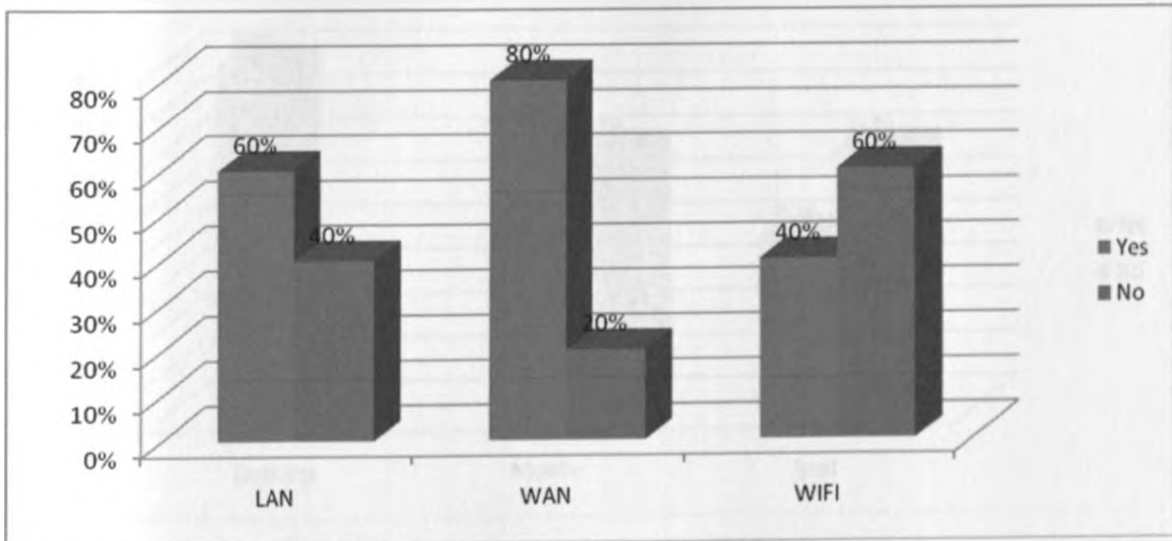


Figure 4. 12: HRMIS Network Resources

### Operating Systems

The type of operating system that supports the HRMIS is Linux based as indicated by 80% of the technical staff.

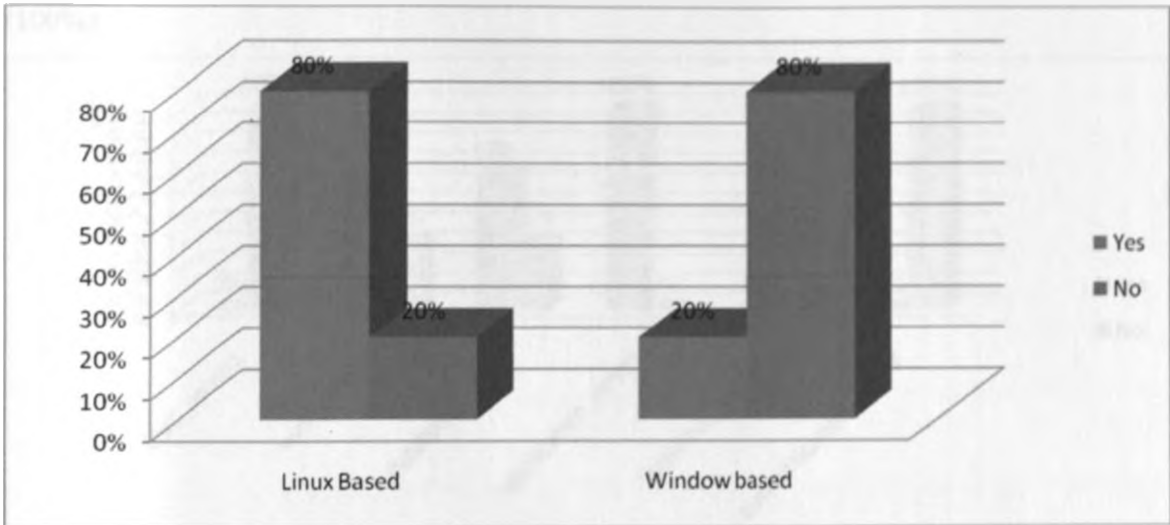


Figure 4. 13: HRMIS Operating Systems

#### End computing Devices

The end computing devices that supported the HRMIS included desktops (80%), mobile (60%) and ipads (60%). Technical staff also indicated that laptops were some of the other end computing devices that are used.

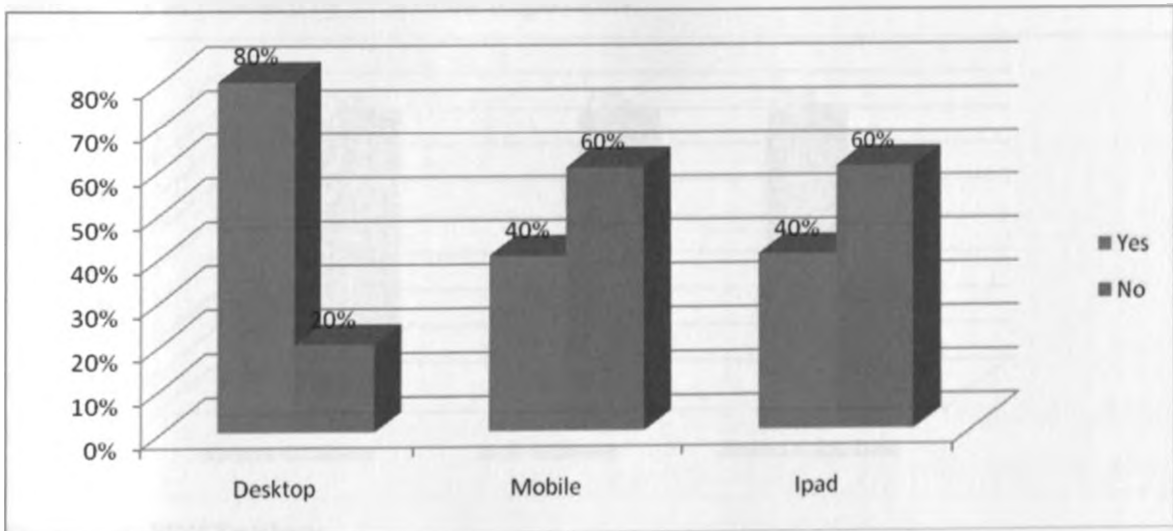


Figure 4. 14: HRMIS End Computing Devices

#### 4.5.5 Financial Management System

##### Server

The server resources that were found to be important in supporting the Financial Management System included the web server (67%), database server (67%), and the application server (100%).

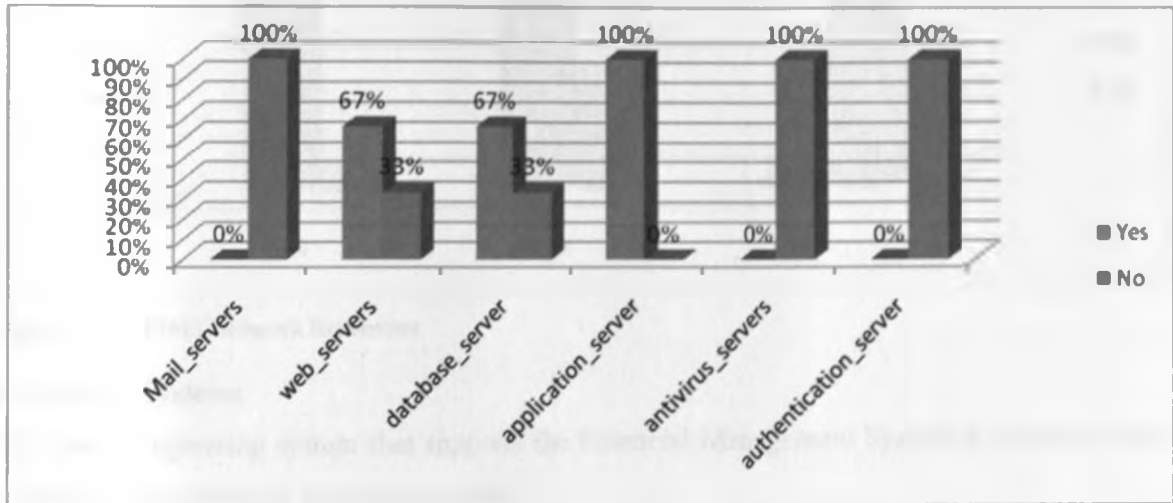


Figure 4. 15: FIMS Servers

#### Databases

The specific databases that are crucial in supporting the Financial Management System include the financial database (75%). The student and the staff database were also indicated though infrequently as indicated by 25% of the respondents.

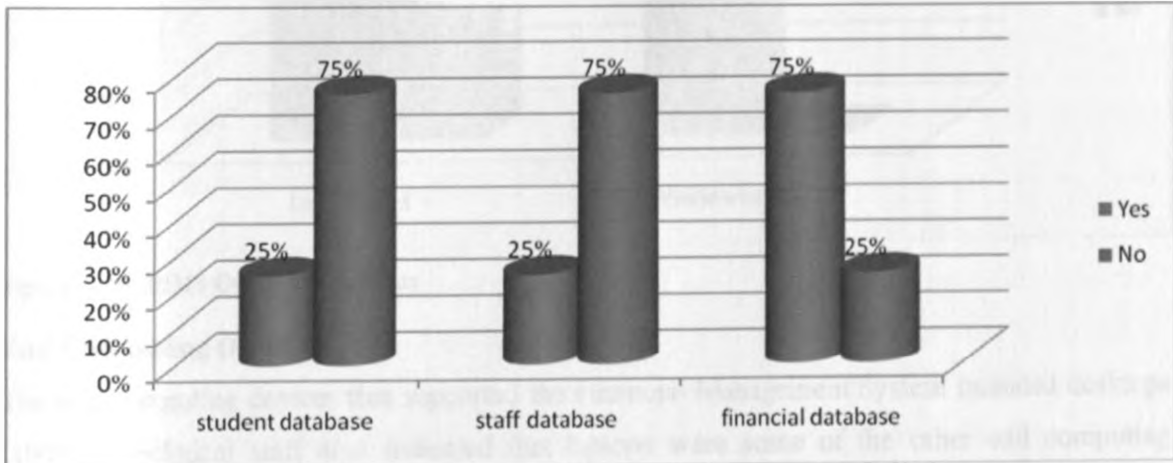
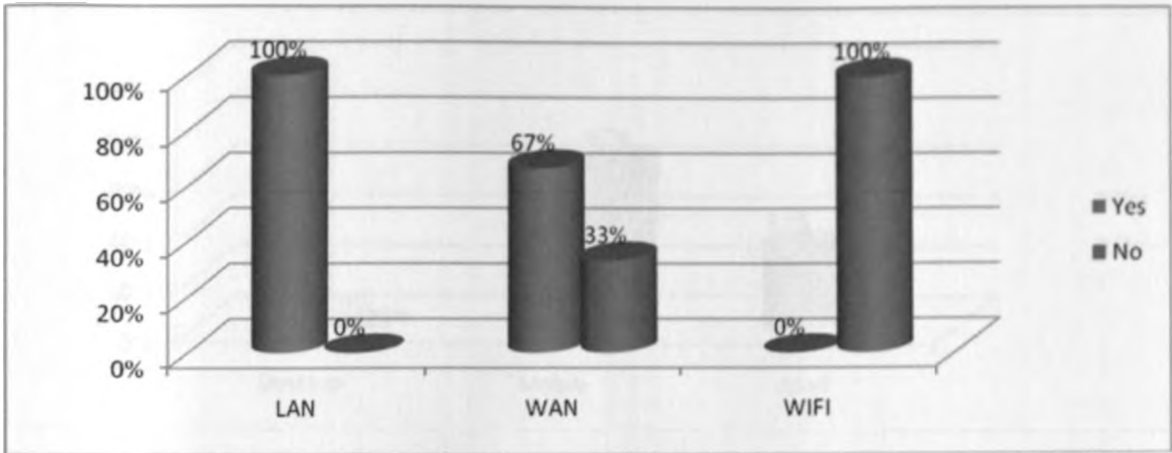


Figure 4. 16: FIMS Databases

#### Network Resources

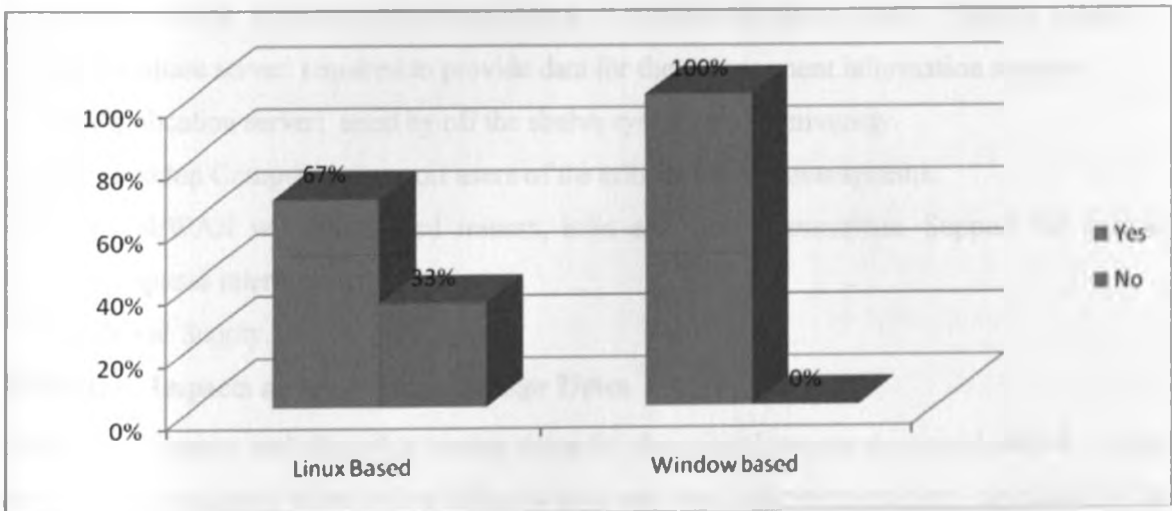
The network resources that supported the FIMS included LAN as indicated by 100% of the technical staff followed by WAN (67%).



**Figure 4. 17: FIMS Network Resources**

### Operating Systems

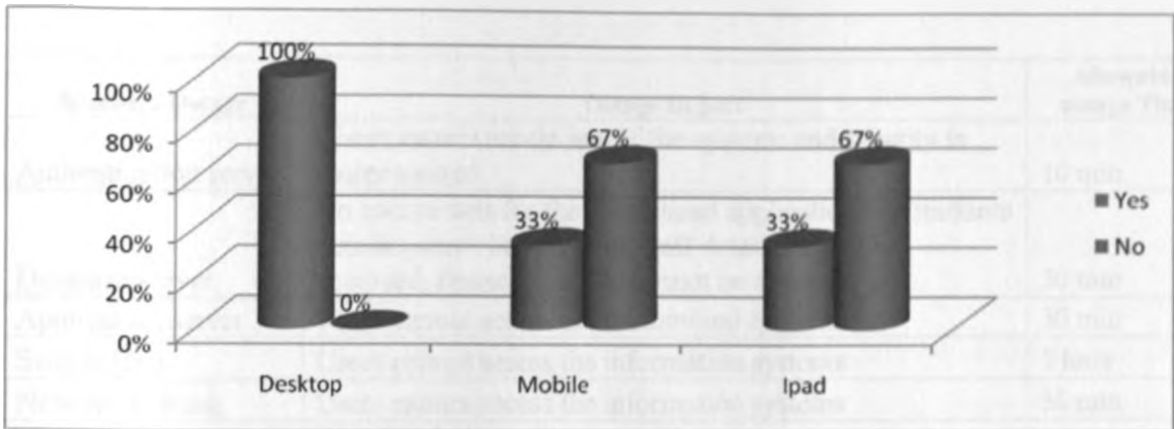
The type of operating system that supports the Financial Management System is window based as indicated by 100% of the technical staff.



**Figure 4. 18: FIMS Operating Systems**

### End Computing Device

The end computing devices that supported the Financial Management System included desktops (100%). Technical staff also indicated that laptops were some of the other end computing devices that are used.



**Figure 4. 19: FIMS End Computing Devices**

#### **4.6 IT Resources for Critical Information Systems**

The minimum IT resources that will be required to support the critical information systems include;

- a) Web server: Supporting the three critical IS systems identified (SMIS, HRMIS, FIMS).
- b) Database server: required to provide data for the management information systems.
- c) Application server: used by off the shelf system at the university.
- d) Desktop Computers: support users of the critical information systems.
- e) LAN/WAN with associated routers, hubs and fiber connections. Support the various campuses interconnections.
- f) Power Supply.

#### **4.7 Outage Impacts and Allowable Outage Times**

The outage impacts and allowable outage times for the critical resources were identified. Using the results as tabulated in the below table, the next step was to develop recovery priorities for the system resources. Use was made of a simple very high, high, medium, and low scale to prioritize the resources. Very high priority resources should be restored back before they are required. High priorities are based on the need to restore critical resources within their allowable outage times, medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

Resource Outage	Outage Impact	Allowable outage Time
Authentication server	Users cannot access any of the systems and security is compromised	10 min
Database server	No source data for the specialized applications i.e students details cannot be accessed, staff details cannot be accessed, financial details cannot be accessed	30 min
Application server	Users cannot access the customized applications	30 min
Switch/Hub	Users cannot access the information systems	1 hour
Network cabling	Users cannot access the information systems	30 min
Electric power	Users cannot access the applications	1 hour
Desk Top computers	Users cannot access the various applications	2hours
E-mail server	Users could not send and receive e-mail	6hours
Web server	Users cannot access the customized applications	2 hours
Student database	Students details cannot be accessed,	30 min
Staff database	Staff details cannot be accessed,	6 hours

**Table 4. 8: Outage Impacts and Allowable Outage Time**

#### 4.8 Prioritization of Resource Recovery

The allowable outage times were used to develop the recovery priorities for the IT resources that support the critical IS at the University of Nairobi. The recovery requirements of these resources are used to develop strategies in the contingency plan that enable all system resources to be recovered within their respective allowable outage times and in a prioritized manner.

Resource	Recovery Priority	Time
Authentication server	Very High	10 min
Application server	Very High	30 min
student database	Very High	30 min
Network cabling	Very High	30 min
Database server	Very High	30 min
Switch/Hub	High	1 hour
Electric power	High	1 hour
Desk Top computers	Medium	2 hours
web server	Medium	2 hours
staff database	Low	6 hours
E-mail server	Low	6 hours

**Table 4. 9: Recovery Priority**

#### **4.9 Result of the BIA and the Model IS Contingency Plan**

The results of the BIA were used to determine the critical information systems at the University of Nairobi. When developing an IS contingency plan, the critical information systems are determined and the critical role that they play in an organization. The outage impact and the allowable outage times help to determine the criticality of the information systems and the recovery priority that should be implemented during the recovery process. The critical information systems should be included in the contingency plan, together with the critical IT resources that support these systems. During a disruption, the recovery of the information systems should follow the recovery priority as determined in the BIA.



## **CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS**

### **5.1 Summary of Achievements**

In this study, we examined literature in the field of information systems contingency planning. Using a Case Study of University of Nairobi, we carried out a BIA to identify the critical business functions at the University and the IS resources required to support them. The study also sought to determine a systematic approach that would be employed in the development of an IS contingency plan.

The first objective of this study was to establish the critical information systems within University of Nairobi that are most vulnerable. Results indicate that the most critical information systems are Student Management Information System, which attracted a mean score of 0.86, Human Resource Management Information System, which attracted a mean score of (0.66), and the Financial Management System which attracted a mean score of (0.57). The Student Management Information System supports the process of student admission and registration, course registration, nominal roll, accommodation, fee collection and examinations. The SMIS is a critical system since in the event that it is unavailable, the University operations would be largely affected. For instance, if the SMIS is disrupted during the student registration, the students would not be able to register, which would in turn cause distress to the students. This can have unpleasant consequences in terms of damaged university reputation, loss of revenue, damage to University- student relationship and disruptions to the university operations.

BIA analysis results indicated that the minimum IT resources that are required to support the critical information systems in case of disaster include, web server which supports the three critical IS identified (SMIS, HRMS, FIMS), database servers, authentication server, application server which supports the off-the shelf information systems at the University, LAN/WAN with associated routers, hubs and fiber connections, and electric power.

The outage impacts and allowable outage times for the critical resources were identified and results indicated that authentication server had the highest outage impact and recovery priority as users cannot access any of the systems without going through the authentication server.

The authentication server is also a critical resource since it ensures the confidentiality, integrity and availability of the data used by the information systems at the University. The outage impact and recovery priority for database servers for the critical information systems, were also very high since students, and financial details could not be accessed without them. Application servers also had a high outage impact and the recovery priority was very high. Having determined the impacts that would result from the disruptions of the critical resources and the priority given to each resource, the University can then develop strategies that enable all the system resources to be recovered within their respective allowable outage times and in a prioritized manner.

The second objective of the study was to determine a systematic approach that could be used to develop a contingency plan. The study conducted a detailed literature review to identify the important elements that should be considered in an information systems contingency plan. The elements identified in the literature were then grouped based on internationally recognized contingency planning models. NIST contingency planning model and the ISO/IEC 24276:2008 model were considered during this study. The NIST model identified the critical steps in the development of an IS contingency plan as, developing the contingency planning policy statement, conduct business impact analysis, identify preventive controls, develop recovery strategies, develop the contingency plan, plan testing, training and exercises and lastly plan maintenance. The research proposed the ISO/IEC 24276 model which identified the following phases as the key elements in a comprehensive information systems contingency plan.

#### *Business Impact Analysis*

The research established that BIA is an important element in the development of an IS contingency plan. BIA is used to understand the nature of an organization business process, thereby, determine the information systems that used to achieve the core business process in the organization, which resources are critical for the organization to meet it primary objectives and the impact of the unavailability of these resources. It is therefore imperative that before engaging in the process of developing a contingency plan, the university conduct a comprehensive BIA.

#### *Recovery Strategy Formulation*

The research validated recovery strategy formulation as an important element in the development of an IS contingency plan. A majority of the respondent confirmed that it is important to have regular scheduled backups, contracts with cold, warm and hot sites, UPS, fire, smoke detectors

and suppression systems as some of the recovery strategies that can enhance the continuity and recovery of IS during a disruption.

#### *Plan testing*

The study also confirmed plan testing as an important element of the IS contingency plan development process. Plan testing ensures the adequacy and accuracy of the plan, ensures that the plan is current and working, help identify deficiencies in the plan and evaluate the ability of the recovery team to implement the plan. Classroom and functional exercises can be used to test the viability of the IS contingency plan.

#### *Contingency plan Awareness*

Results indicate that a majority of end users strongly agreed that conducting staff awareness program for IS contingency planning, mandatory training for new employees in handling IS contingencies is an important step in developing a contingency plan.

#### *Plan Maintenance*

The study established that at a minimum the contingency plan should be reviewed and updated on the following elements, names and contacts of recovery team members, vendors, alternate and off-site security requirements, hardware and software changes and that the IS contingency plan should also be audited regularly. Contingency plan maintenance primarily consists of keeping information current as to personnel, supplies, facilities and recovery procedures.

The third objective of the study was to develop a model IS contingency plan based on the results of the BIA and best practice as demonstrated by literature review. Salient features of the proposed model include;

#### *Supporting Information*

The supporting information component includes an introduction and concept of operations section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. This section indicates the purpose, applicability, the scope, record of changes and the responsibilities of the different teams.

#### *Notification/Activation Phase*

The notification/activation phase indicates the initial actions taken once a system disruption or emergency has been detected. Activities to notify the recovery teams, assess damage to the system and implement the plan are highlighted in this phase. Recovery teams should be prepared

to perform contingency measures at the end of this phase in order to restore information systems functions.

#### *Recovery Phase*

During the recovery of information systems following a disruption, recovery procedures should reflect the system priorities identified in the BIA. The recovery phase should also consider the allowable outage times determined during the BIA, to avoid significant impacts to related systems and their applications. In particular the recovery phase should include the sequence of recovery activities and the recovery procedures for every IT resource which has been identified as critical or supports the critical IS systems.

#### *Reconstitution Phase*

At the reconstitution phase, recovery activities are terminated and normal operations are taken back to the organization's primary facility or new site if the original facility is unrecoverable.

#### *Plan Appendices*

Contingency plan appendices provide key details not contained in the main body of the IS contingency plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system.

The IS Continuity Plan developed as part of this study is presented in Appendix I. It provides a framework that can be adapted by other universities when developing their own IS contingency plans.

## **5.2 Limitation of the Study**

Study presented herein has certain limitations. First, the relationship amongst the various phases in the development of an IS contingency plan were not considered. For example, the study did not show the possible relationship between BIA and formulation of recovery strategies, staff awareness, and plan maintenance.

The study also did not take into considerations the legal and the organizational issues that influence the proper planning and implementation of IS contingency plan.

The population considered for this study did not include external entities such as offsite storage backup managers, alternate site, SLAs and vendors. These parties play a crucial role during the implementation of an IS contingency plan.

While conducting the BIA, the study only considered the outage impact and the allowable outage times to determine the critical information systems and the supporting IT resources. However,

the financial implication on the University in the event that information systems are disrupted would be important in determining the critical information systems. Providing the financial losses would help the management realize the criticality of IS in a university, thus would most likely win their support in the development of an IS contingency plan.

### **5.3 Conclusion**

As information systems become indispensable in dispensation of universities core functions, IS contingency plan have also become an essential component of information systems. In this study, the critical information systems at the University of Nairobi were identified. This is important in contingency planning since during a disruption recovery should start with the critical information systems. Information systems can be complex with multiple resources, interconnections and interfaces. This study identified the minimal IT resources that support the critical information systems.

During a disruption, it is not possible to recover all the IT resources at the same time. Prioritizing the recovery of IT resources is therefore a crucial step in IS contingency recovery.

The study established a systematic approach that should be followed when implementing a contingency plan program in an organization. The study established that a University can develop a comprehensive IS contingency plan by adopting the following crucial steps, BIA, recovery strategies formulation, plan testing, conducting staff awareness, and plan maintenance. The final deliverable of this research was a model IS contingency plan. The model identifies three main phases in the documentation of a contingency plan, notification/ activation phase, recovery phase, and reconstitution phase.

Finally, IS contingency plan are indispensable especially because of the complexity of the computer security and IS threats and the interdependence between the various components involved. In an environment full of high risk vulnerabilities and continuous increasing levels of University operations reliance on IS, the sustained operations of universities will be at risk. Consequently, developing IS contingency plan that prevent, mitigate and ensure continuous operation is supreme.

#### **5.4 Further Research and Practice**

The study suggest that a study on the factors affecting the success of IS contingency plan be carried out. This would make use of such models such as the TAM Models by Rodgers (1983) and Davis (1989).

This would give an insight as to why some universities have not adopted an IS contingency plan despite its critical importance in enhancing the availability of Management Information Systems in an organization.

The study further recommends that testing of the IS contingency plan be conducted to ascertain the usability of the plan. Cerullo (2004) claims that the creation of a IS contingency plan without periodic testing and ongoing maintenance is worse than not having a plan at all. Testing will ensure that the contingency plan is current and working if ever the University is faced with the situation of putting the plan in action.

## REFERENCES

- Aasgaard, D. O., Cheun, P.R., Hulbert, B.J., & Simpson, M.C.( 1978). An Evaluation of Data Processing 'Machine Room' Loss and Selected Recovery Strategies. Management Information Systems Research Center Working Papers. Minneapolis, MN: University of Minnesota.
- Al-Zahrani, S. (2006). An Information Management System Model for the Industrial Incidents in Saudi Arabia: A Conceptual Framework Based on SDLC Methodology. *Journal of Computer Science*, 2(5) 447-454
- Baskerville, R.(1993). Risk Analysis as a Source of Professional Knowledge. *Computers & Security journal*, 10(8), 749-764.
- Blake, W.F. (2002). Making recovery a priority. *Security Management journal*, 36(4), 71-74.
- Blakley, B., McDermott, E., & Geer, D. (2002). Information Security is Information Risk Management, Proceedings of the 2001 workshop on New security paradigms, ACM, 97 – 104
- Blatnik, G.J. (1998). Point of failure recovery plan. *IS Audit & Control Journal*, 4(1), 24-27
- Bocij, P., Chaffey, D., Greasley, A. & Hickie, S. (2003). Business Information Systems: Technology, Development, and Management for the e-business. Harlow: Financial Times Prentice Hall.
- Botha, J. & Solms, V R. (2004). A cyclic approach to Business continuity planning. *Information Management & Computer Security*, 12(4) ,328-337
- Buffington, J. (2004). Data Protection: Business Continuity - Key Factors for Success. *Disaster Recovery Journal*, 17(1), 313-512
- Castillo, C. (2004). Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model. *Journal of Facilities Management*, 3 ( 1), 8-26
- Cerullo, M.J., McDuffie, R.S. & Smith, L.M. (2004) Planning for Disaster. *The DRJ Journal*, 6, 34-38.
- Cerullo, V. & Cerullo, M.(2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21( 3), 70-78
- Cervone, F. H. (2006). Disaster recovery and continuity planning for digital library systems. *International digital library perspectives*, 22 (3), 173-178

- Chandran, E. (2004). *Research Methods: A Quantitative Approach with Illustrations from Christian Ministries*. Nairobi: Daystar University.
- Chow, W.S. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security*, 8(2), 80-86.
- Chow, W.S. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security*, 8(2), 80-86.
- Cooper, D., & Schindler, P., (2011) *Business Research Methods*, (11th Ed). Tata McGraw, Hill: New Delhi.
- Cronbach, L.J. (1951). Coefficient Alpha and the Internal Structures of Tests. *Psychometrika*, 16, 297-334.
- Dwyer, P.D., Friedberg, A.H. & McKenzie, K.S. (1994). It can happen here: The important of continuity planning, *IS Audit & Control Journal*, 1, 30-35.
- Farahmand, F., Navathe, S.B., Enslow, P.H., & Sharp, G.P. (2003). Managing vulnerabilities of information systems to security incidents, *Proceedings of the 5th international conference on Electronic commerce* (pp. 348-354). New York: ACM.
- Francis, B. (1993). Contingency Planning and Disaster Recovery: Protecting Your Organization's Resources, *Logistics Information Management*, 9(6), 27 – 34.
- Ginn, R.D. (1989). The Case for Continuity. *Journal of Security Management*, 1, 84-90.
- Grill, M.T., (1999). *Developing A Contingency Plan For Y2k Related Computer Disruptions of Critical Infrastructures For The Sierra Vista Fire Department Executive Development*. Arizona: Sierra Vista.
- Hawkins, S.M., Yen, D.C. & Chou, D.C. (2000). Disaster Recovery Planning: A Strategy for Data Security. *Information Management & Computer Security*, 8(5), 222-229.
- Hoffman, T. (1998). Denial Stalls Disaster Recovery Plans. *ComputerWorld*. Retrieved 2<sup>nd</sup> June, 2011, from <http://911research.wtc7.net/essays/nist/>
- ISO. (2008). *Guidelines for information and communications technology disaster recovery services: ISO/IEC 24762*. ISO
- Kothari C. (1990). *Research Methodology: Methods & Techniques*. New Delhi: New age International Publishers.
- Kris, N. & Petersen, M. (1998). *Database Operating Practices – High Availability and Data Protection*. Strategic Research Corporation. Retrieved 2<sup>nd</sup> June, 2011, from <http://www.sresearch.com/reports/dop98.htm>



- Lee, S. & Ross, S. (1995). Disaster Recovery Planning for Information Systems. *Information Resources Management Journal*, 3, 18-23.
- Malombe, M (2005). The Quest for Information Systems Continuity in a Financial Institution. Unpublished masters thesis, Makerere University.
- Mitome, Y., Speer, K.D. & Swift, B. (2001). Embracing Disaster with Contingency Planning. *Risk Management Journal*, 5(48), 18-27.
- Mugenda, O. & Mugenda, A. (1999). *Research Methods: Quantitative & Qualitative approaches*. Acts Press.
- NIST. (2000). *Contingency Planning Guide for Federal Information*. U.S. Washington, Government Printing Office.
- Parnell, J.A., Crandall, W. & Menefee, M.L. (1997). Management Perceptions of Organizational Crisis: A Cross Cultural Study of Egyptian Managers. *Academy of Strategic and Organizational leadership Journal*, 1, 77-87
- Patton, M.Q. (1990). *Qualitative Research and Evaluation Methods*. Thousand Oaks, CA: Sage.
- Peil, M. (1995). *Social Science Research Methods: A handbook for Africa*. Nairobi: East Africa Printing Press
- Schwartau, W. (2000). *Cybershock: Surviving hackers, Phreakers, Identify Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York : Thunder's Mouth Press,.
- Smith, D. M. (2003). The Cost of Lost Data: The importance of investing in that "ounce of prevention". *Graziadio Business Report. Journal of Contemporary Business Practice*, 6 (3), 56-59
- Smith, M. & Sherwood J. (1995). *Business Continuity Planning*. *Computer & Security journal*, 14(1), 14-23.
- Swanson, M., Wohl, A., Lucinda, L., Grance, T., Hash, J. & Thomas, R. (2002). *Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. Washington, NIST Special Publication 800-34.
- Toigo, J.W. (1989). *Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems*. New Jersey: Yourdon Press.
- Toigo, J.W. (2003). *Disaster Recovery Planning: Preparing for the Unthinkable (3rd Ed)*. New Jersey: Prentice Hall.

University of Nairobi. (2009). ICT Developments at The University Of Nairobi For The Period 2004-2009: A High Level Summary Report Depicting Status Of Automation. Nairobi: UoN.

University of Nairobi. (2010). Information and Communication Technology Policy Guidelines. Nairobi: UoN.

Wilk, R.J. (2000). Information Systems Security Audit and Operational Data Security. International Association for Computer Systems Security (I.A.C.S.S.). New York: IACSS.

Wong, B.K., Monaco, J.A. & Sellaro, C.L. (2004). Disaster Recovery Planning: Suggestions to Top Management and Information Systems Managers. *Journal of Systems Management*, 5(4), 28-32.

**Appendix I: Proposed University of Nairobi Information  
Systems Contingency Plan**



**PROPOSED  
UNIVERSITY OF NAIROBI  
INFORMATION SYSTEMS CONTINGENCY PLAN**

**April 2012**

# 1 INTRODUCTION;

## 1.1 Purpose

This information systems contingency plan for the University of Nairobi establishes procedures to recover the information systems at the University following a disruption. The objectives of the plan are:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Notification/Activation** Phase to detect and assess damage and to activate the plan.
  - **Recovery phase** to restore temporary information systems operations and recover damage done to the original system.
  - **Reconstruction phase** to restore information systems processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out University processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated University personnel and provide guidance for recovering information systems during prolonged periods of interruption to normal operations.
- Ensure coordination between University staff, external points of contact and vendors who will participate in the contingency recovery strategies.

## 1.2 Applicability

This information systems contingency plan applies to the functions, operations, and resources necessary to restore and resume the University's information systems operations as it is installed at Chiromo Campus Nairobi, Kenya

## 1.3 Scope

### 1.3.1 Planning Principles

The applicability of the plan is predicated on two key principles:

- The University's computing facilities at Chiromo Campus, is inaccessible, and thus the University is unable to perform information systems processing.
- A valid contract exists with the alternate site. University will use the alternate site building and IT resources to recover full functionality during an emergency situation that prevents access to the computer center at Chiromo.

- The alternate site will be used to continue recovery and processing throughout the period of disruption, until the return to normal operation.

### 1.3.2 Assumptions

The following assumptions were used when developing the IS contingency plan.

- The information systems at University cannot be recovered within 2 hours.
- Key ICTC personnel have been identified and trained in their emergency response and recovery roles and they are available to activate the IS contingency plan.
- Preventive controls (e.g., generators, environmental controls, waterproof traps, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- The information systems hardware and software at the computer center are unavailable for at least 2 hours.
- Current backups of the application software and data are intact and available in the offsite storage facility.
- The equipment, connections, and capabilities required to operate the information systems are available at the alternate site.
- Service level agreements are maintained with hardware, software, and communications providers to support the emergency systems recovery.

### 1.4 Record of Changes

The table below indicates revisions, changes, or updates that have been made to this document.

This table must remain updated at all times:

Page No.	Change Comment	Date of Change	Signature

## 2 CONCEPT OF OPERATIONS

### 2.1 Line of Succession

The Director ICTC is responsible for ensuring the safety of personnel and the execution of procedures documented within this contingency plan. If the Director is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy Director (Research and Development) shall function as that authority.

### 2.2 Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the information systems at the University.

#### 2.2.1 Management Team

This team is responsible for the overall management of the recovery process. It will be responsible for activating the recovery site, recovery teams, and providing status reports to the VC.

Name	Responsibility	Primary phone	Secondary Phone
Director ICTC	Activate the IS contingency plan		
Deputy Director (Research and Development)	Coordinate recovery efforts		
Deputy Director (MIS)	Coordinate recovery efforts		
Deputy Director (Network Infrastructure Services)	Coordinate recovery efforts		
Deputy Director (User Support and Maintenance)	Coordinate recovery efforts		
Deputy Director (Communication and Data Center)	Coordinate recovery efforts		

### Management Team Tasks

- Ensure activation procedures have been followed
- Perform team briefing that include; result of damage assessment, expected duration of outage, work-in progress status, and recovery site activation.
- Coordinate with team leaders who should report to the recovery site and who should remain on standby.
- Provide updates to the VC.
- Activate any recovery sites, command centers, or alternate work-locations necessary for recovery of University's information systems.

### 2.2.2 Administrative Team

This team is to provide support to all recovery teams. Documentation, log, reports, briefings, travel arrangements, financial reports, etc, will be carried out and managed by this team.

Name	Responsibility	Primary Phone	Secondary Phone
Senior Assistant Registrar ICTC			
ICT Maintenance Manager			

### Administrative Team Tasks

- Provide support to students and staff during the disruption.
- Provide general assistance support to the Management Team and Recovery Teams.
- Assist in establishing and staffing the recovery site.
- Notify students, schools and other stake holders of the recovery status.

### 2.3 Plan Distribution

The following people have received a copy of this plan. They must keep a copy of this plan at their office and home. A master copy has been stored offsite.

Version	Name	Title	Recovery Team	Date
		Director ICTC	Management Team	
		Deputy Director (Research and Development)	Management Team	
		Deputy Director (MIS)	Management Team	
		Deputy Director (Network Infrastructure Services)	Management Team	
		Deputy Director (User Support and Maintenance)	Management Team	
		Deputy Director (Communication and Data Center)	Management Team	
		Database Administrator	Database Recovery	
		Network Engineer	Network Recovery	
		System Administrator	Server Recovery	

### 2.4 Plan Certification

The following senior management of the University have reviewed and approved this plan, as of the date stated below.

Signature	Name	Date	Title
			Director ICTC
			Internal Auditor
			Business Continuity Manager

### 3 NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to University information systems. Based on the assessment of the event, the plan may be activated by the Director ICTC.

#### 3.1 Notification Sequence

- The first responder is to notify the ICTC Director, relaying all known information.
- The Director ICTC is to contact the Damage Assessment Team Leader and inform him/her of the event, instructing the Team Leader to begin assessment procedures.
- The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time.

#### 3.2 Damage Assessment Procedure

To determine how the IS contingency plan will be implemented, the following procedures will be used to assess the nature and extent of the damage to the system.

Procedure	Notes
Cause of the disruption	
Potential for additional disruptions or damage	
Areas affected by the disruption	
Status of physical infrastructure	
Inventory and functional status of IT equipment	
Type of damage to IT equipment and data	
Estimated time to restore normal services	



### **3.3 Activation of the Contingency Plan**

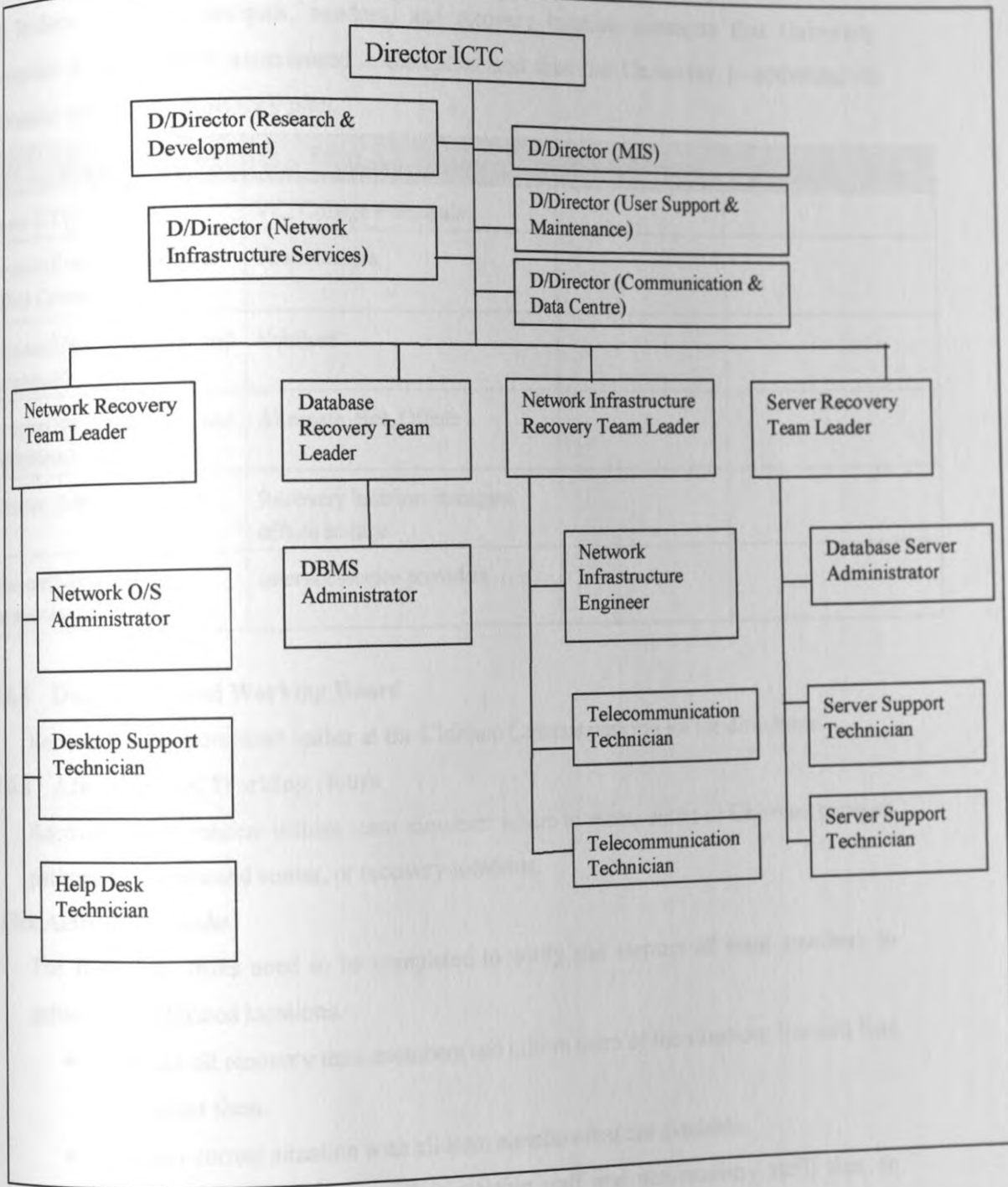
The contingency plan is to be activated if one or more of the following criteria are met:

- The information systems at the University are unavailable for more than 2 hours
- The ICT Center is damaged and will be unavailable for more than 2 hours

### **3.4 Plan Activation Tasks**

- The Director ICTC/Deputy Director is to notify all team leaders and inform them of the details of the disruption/event and if relocation is required.
- Team leaders are to notify their respective teams and assemble members for further instructions.
- Director ICTC activates the alternate facility, offsite or hot site depending on the damage assessment report.
- The Director ICTC is to inform the VC of the disruption and the recovery course being implemented
- The Director ICTC is to inform all the College Principals on the general status of the incident.

### 3.5 University of Nairobi Information Systems Contingency Plan Call Tree



### 3.6 Activation Procedures

The following team members are responsible for carrying out notification activities to inform team leaders, college principals, vendors, and recovery location managers that University information systems have experienced a disruption and thus the University is activating its information systems contingency plan.

Name	Responsibility	Primary Phone	Secondary Phone
Director ICTC	VC, College Principals		
D Director (Communications and Data Center)	Team leaders		
D Director (User Support and Maintenance)	Vendors		
D Director (Research and Development)	Alternate, Hot, Offsite		
D Director (MIS)	Recovery location managers, offsite storage		
D Director (Network Infrastructure Services)	Internet service providers		

#### 3.6.1 During Normal Working Hours

Recovery team personnel gather at the Chiromo Campus parking lot for directions.

#### 3.6.2 After Normal Working Hours

Recovery team leaders inform team members where to meet, either at Chiromo campus parking lot, command center, or recovery locations.

### 3.7 Plan Activation Tasks

The following tasks need to be completed to notify and instruct all team members to gather at the defined locations.

- Contact all recovery team members and inform them of the situation. Use call lists to contact them.
- Discuss current situation with all team members that are available.
- Notify entire University staff (remaining staff and non-recovery staff) that an incident has occurred and to stand by for further instructions.

### 3.8 Recovery Procedures

The following recovery teams have been organized to respond to disruptions of various type, size, and location. Any of these teams may be mobilized depending on the parameters of the disaster. The Director ICTC will determine which team(s) to mobilize following the declaration of a disaster and activation of the contingency plan.

- Database Recovery Team.
- Server Recovery Team.
- Network Recovery Team.
- Telecommunication Recovery Team.

While multiple teams may be able to work in parallel, from the results of the BIA the Data Center and network infrastructure will normally be assigned the highest priority.

### 3.9 Recovery Teams Contact Procedure

The following procedures are to be used as a guide when notifying recovery team members of an outage and identifying the action to be taken.

#### Appendix H: Process Map (Notification Procedure)

### 3.10 Contact List

#### Recovery Team Members

Employee Name	Home Phone	Work Phone	Alternate Phone	Date/Time Notified

**Vendors Contact List**

Vendor Name	Services Provided	24 Hour Number	Alternate Number	Representative

**College Contact List**

School	Contact	Office Phone	Alternate Phone	Notify Within(hours)
CAE	Principal			1 Hour
CAVS	Principal			1 Hour
CBPS	Principal			1 Hour
CEES	Principal			1 Hour
CHS	Principal			1 Hour
CHSS	Principal			1 Hour

**3.11 Alternate Locations**

**3.11.1 Assembly Site**

In case the ICT Center facilities at the Chiromo Campus are in accessible, the recovery teams will assemble at the following sites for further instructions:

Site Name	Location	Notes
Chiromo Campus parking Lot		
Graduation Square		

### Assembly Site Tasks

- Confirm the recovery teams members.
- Brief the members about the disruption, expected recovery time.
- Using the notification procedures and the call list, contact the members who have not gathered.

#### 3.11.2 Command Center

The following locations have been identified for recovery team members to use as the command center during an information systems disruption.

Site Name	Location	Notes
Chancellors Court	Main Campus	
Taifa Hall	Main Campus	

#### Command Center Tasks

- Connect special conference phone.
- Contact all recovery team members if not yet completed.
- Activate hotline and conference line.

#### 3.11.3 Recovery Location

The following site has been predetermined by University for recovery teams to use to recover critical IT resources.

Site Name	Location	Notes

#### Recovery Site Tasks

Immediate actions that need to be taken once the recovery site is activated:

- Check in at the reception and receive security badges from the Recovery Site security staff.
- Confirm arrival at recovery site to the designated person.

- Check equipment (prior to commencing business) and refer any shortfalls to the recovery site manager. Use the equipment list as a referral.
- Validate all required resources (vital records, supplies, form) are at the recovery site and available for use.

**Directions to Recovery Location**

Map to the Recovery Location from the University

**3.11.4 Offsite Storage**

This site has been predetermined for storage of critical data, information, resources, etc. In the event of a disruption, materials should be recalled from this location.

Site Name	Full Address/Location	Notes

**Direction to Offsite Storage Location**

Map to the Offsite location from the University

**Offsite Storage Authorization Information**

Personnel Name	Title	Code/Account Numbers

#### 4 RECOVERY OPERATIONS

The following information systems have been identified as critical to the operations of the University of Nairobi.

Information System	Role
Student Management Information System	Student admission and registration, course registration, nominal roll, accommodation, fee collection and examinations.
Financial Management System	Computerizes the financial/accounting function of the University. Modules: General Ledger, Inventory Control, Accounts Receivable and payable
Human Resource Management Information System	Supports the payroll and personnel functions of the University. Also supports the budgeting, tax returns

The table below summarizes the results of the BIA. The resources categorized as critical, meaning they support critical business processes, need to be recovered within indicated time frames after a disruption. The table also indicates the Team member responsible for guiding the recovery of each resource.

Resource Outage	Recovery Priority	Allowable outage Time	Responsible Team Member
Authentication Server	Very High	10 minutes	D/Director-Network Infrastructure Services
Application Server	Very High	30 minutes	D/Director -MIS
Student Database	Very High	30 minutes	D/Director -Research and Development
Network Cabling	Very High	30 minutes	D/Director-Network Infrastructure Services
Database Server	Very High	30 minutes	Database Administrator
Switch/Hub	High	1 hour	D/Director -Network Infrastructure Services
Electric Power	High	1 hour	D/Director -User Support and Maintenance
Desk Top Computers	Medium	2 hours	D/Director -User Support and Maintenance
Web Server	Medium	2 hours	D/Director -Network



Resource Outage	Recovery Priority	Allowable outage Time	Responsible Team Member
			Infrastructure Services
Staff Database	Low	6 hours	Database Administrator
E-mail Server	Low	6 hours	D/Director –Network Infrastructure Services

#### 4.1.1.1 Recovery Sequence

The recovery sequence will be based on priority/allowable outage time. While multiple teams may be able to work in parallel, from the results of the BIA the Data Center and network/telecommunication infrastructure will normally be assigned the highest priority.

#### 4.1.1.2 Recovery Procedures

##### Appendix H: Process Map (Recovery Procedures)

To facilitate Recovery Phase operations, detailed procedures to restore the following components will be attached. Given the extensive variety of system types, configurations, and applications, the procedures will appear in this guide as an appendix.

- Database recovery plan procedures.
- Server recovery plan procedures.
- Network recovery plan procedures.
- Telecommunication recovery plan procedures.

## 5 RECONSTITUTION/RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring the University's information systems operations at the ICT Center at Chiromo Campus or at a new site. When the ICT Center at Chiromo Campus or new site has been restored, operations at the alternate site are transitioned back with the aim of providing seamless transition.

### 5.1 Computer Center or New Site Restoration

- Ensure adequate infrastructure support (electric power, telecommunications).
- Establish connectivity and interfaces with the University Network components.
- Test systems operations to ensure full functionality.
- Back up operational data on contingency system and upload it to the restored system.
- Shut down the contingency system.
- Terminate contingency operation.

- Secure, remove and relocate all sensitive material that was used at the contingency site.

**Appendix H: Process Map (Reconstitution Procedure)**

**6 PLAN APPENDICES**

The University information systems contingency plan will append the following documents to enhance its efficient operation:

**Appendix A- Technology Recovery Plans**

To facilitate Recovery Phase operations, detailed procedures to restore the following components will be attached.

- Database recovery plan procedures.
- Server recovery plan procedures.
- Network recovery plan procedures.
- Telecommunication recovery plan procedures.

**Appendix B- Notification Log**

Date & Time	Person contacted	Results of Contact				
		Reached	Unavailable	Line Busy	No Answer	Answering Machine

### Appendix C- Event/Disaster Information Log

When alerted by the Contingency Management Team or designee that the information systems contingency plan ought to be activated, the team leader or alternates should document the following information that will be communicated to recovery team members and/ or department personnel:

		Comments
	Brief Description of the Problem	
	Location to report to (recovery, assembly, etc	
	Phone number to contact the Recovery Location	
	Any immediate support required by the team	
	Whether or not the ICT Center facilities can be accessed or not.	

### Appendix D-Record Log

The following record Log should be used by the Recovery team members to record all key events during the recovery process. Each recovery team will keep track of their recovery efforts in their own log.

<b>Description of Disruption</b>			
<b>Date</b>			
<b>Time of Plan Activation</b>			
<b>Key Activities Undertaken by Recovery Team Members</b>	<b>Date and Time</b>	<b>Outcome</b>	<b>Follow-up action required</b>

**Appendix E – Alternate Site Access Form**

The alternate location managers will use the form below to allow access to individuals associated with the recovery efforts.

Name	Access Granted (Command Center, Alternate Site, Offsite Storage)	Date

**Appendix F – Recovery Status Report**

All recovery teams are required to submit status reports to the Management Team.

Team Name:	
Date & Time:	Contact Information:
Comments:	
Recovery Status	

## **Appendix G – Contingency Recovery Report**

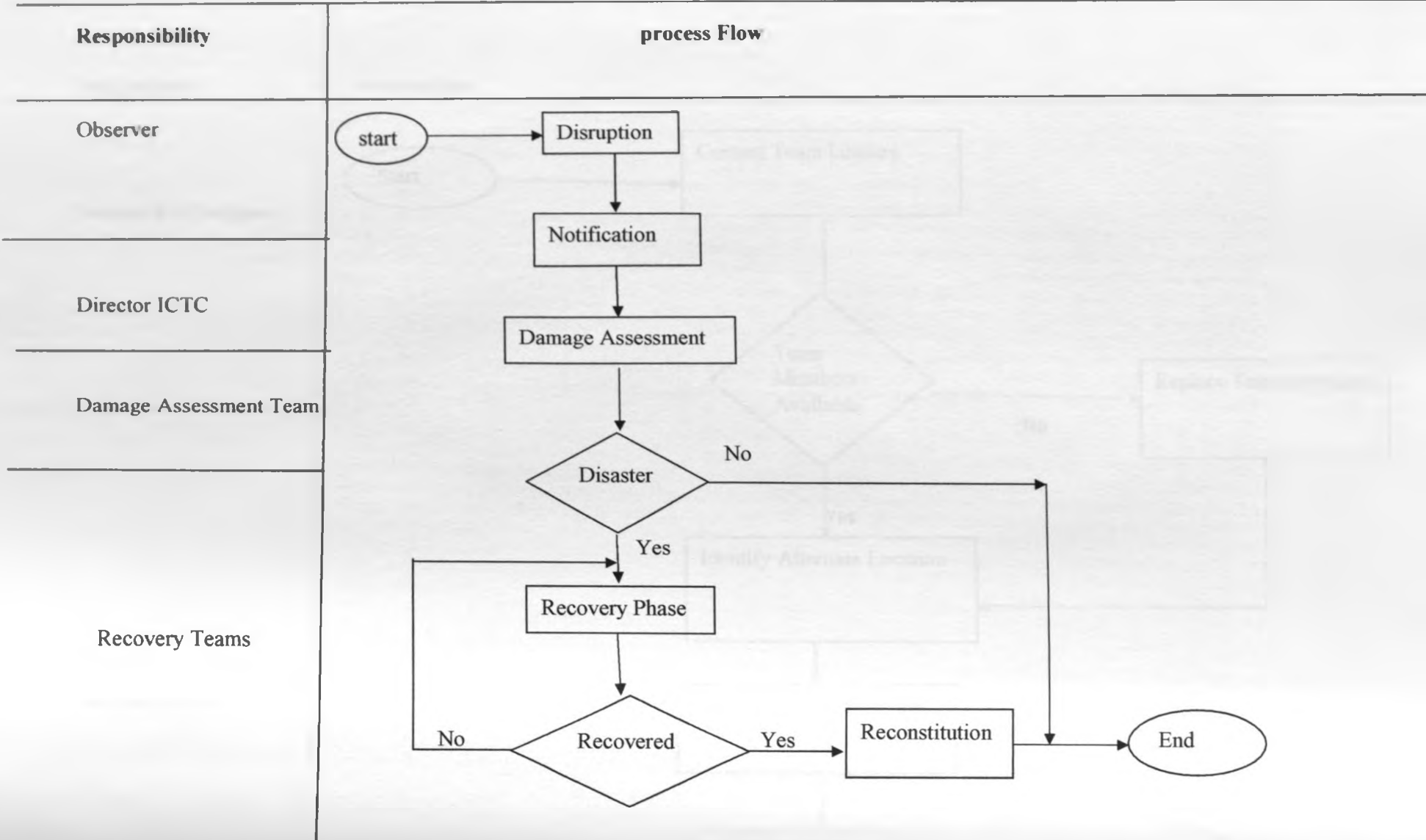
A contingency Recovery Report will be prepared by the Administrative Team Leader on completion of the information systems recovery. The contents of the report will include:

- A description of the disruption.
- Those people notified of the disruption (including dates).
- Action taken by members of the Recovery Team(s).
- Outcomes arising from actions taken.
- An assessment of the impact to normal business operations at the University.
- Assessment of the effectiveness of the information systems contingency plan.
- Lessons learned.

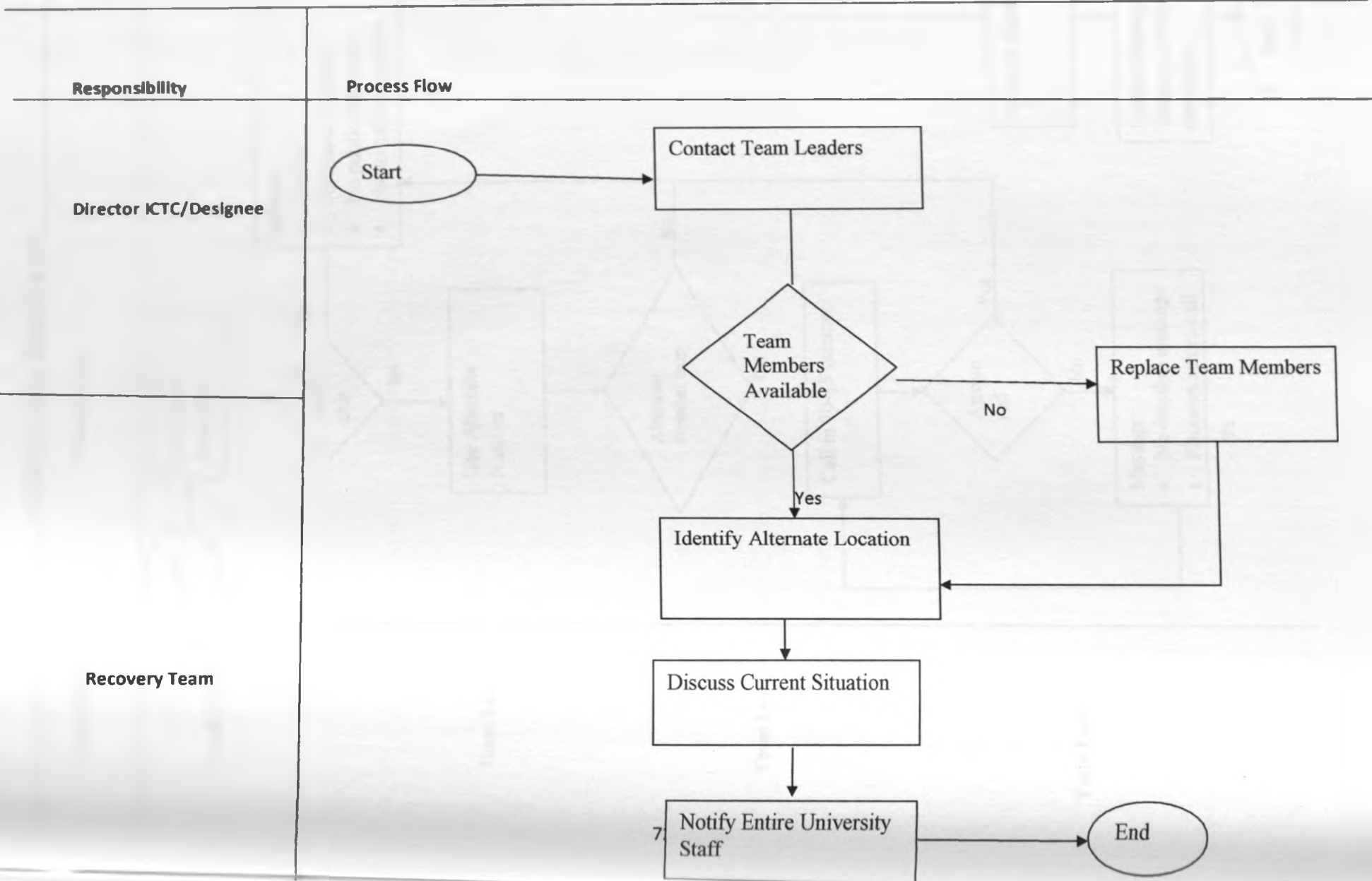
The report should be submitted to the Director ICTC.

## **Appendix H: – Process Maps**

## CONTINGENCY PLAN PROCESS MAP



# PLAN ACTIVATION PROCEDURE



Start

Contact Team Leaders

Team Members Available

Replace Team Members

No

Yes

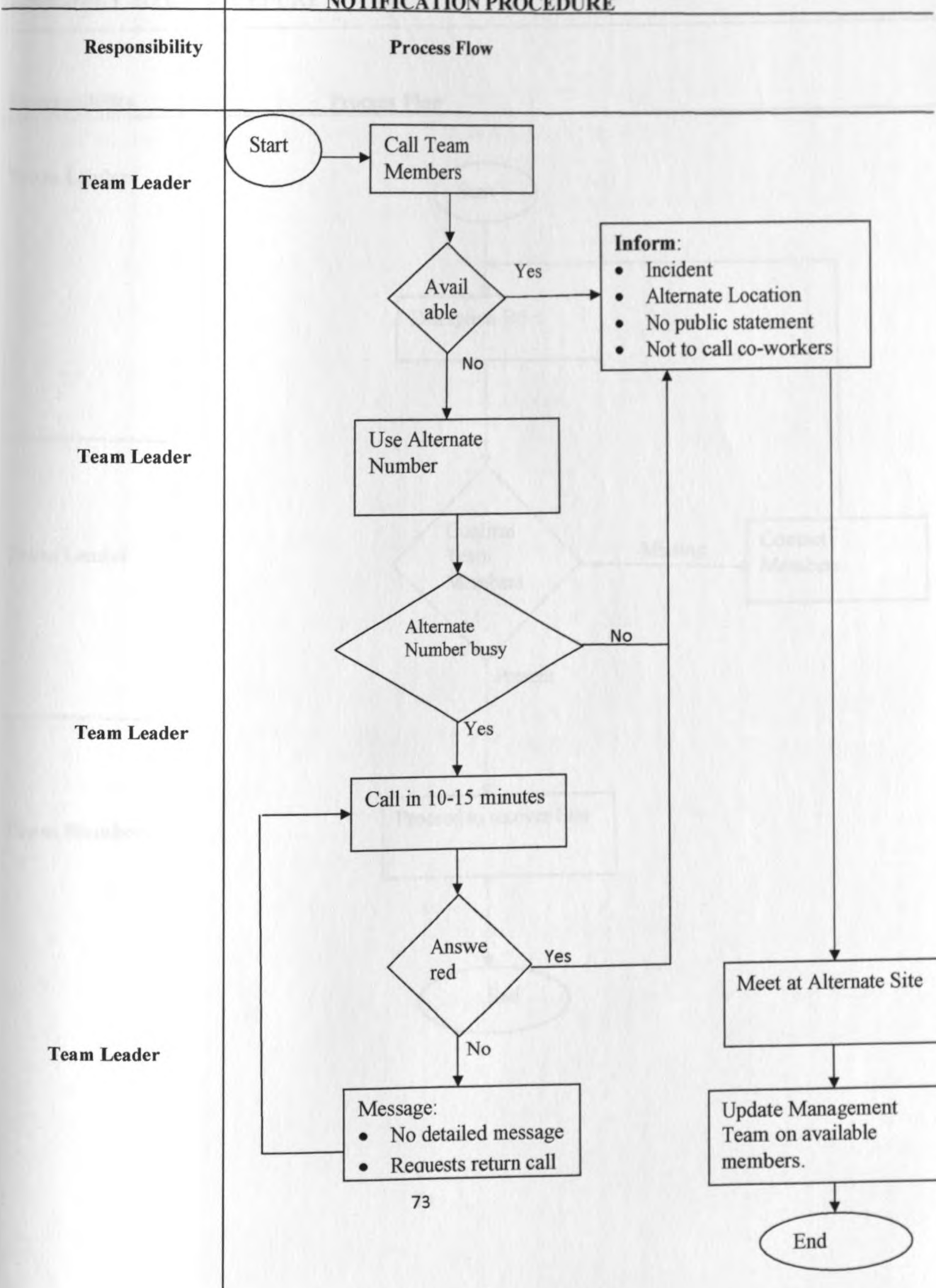
Identify Alternate Location

Discuss Current Situation

7 Notify Entire University Staff

End

## NOTIFICATION PROCEDURE





# ASSEMBLY SITE PROCEDURE

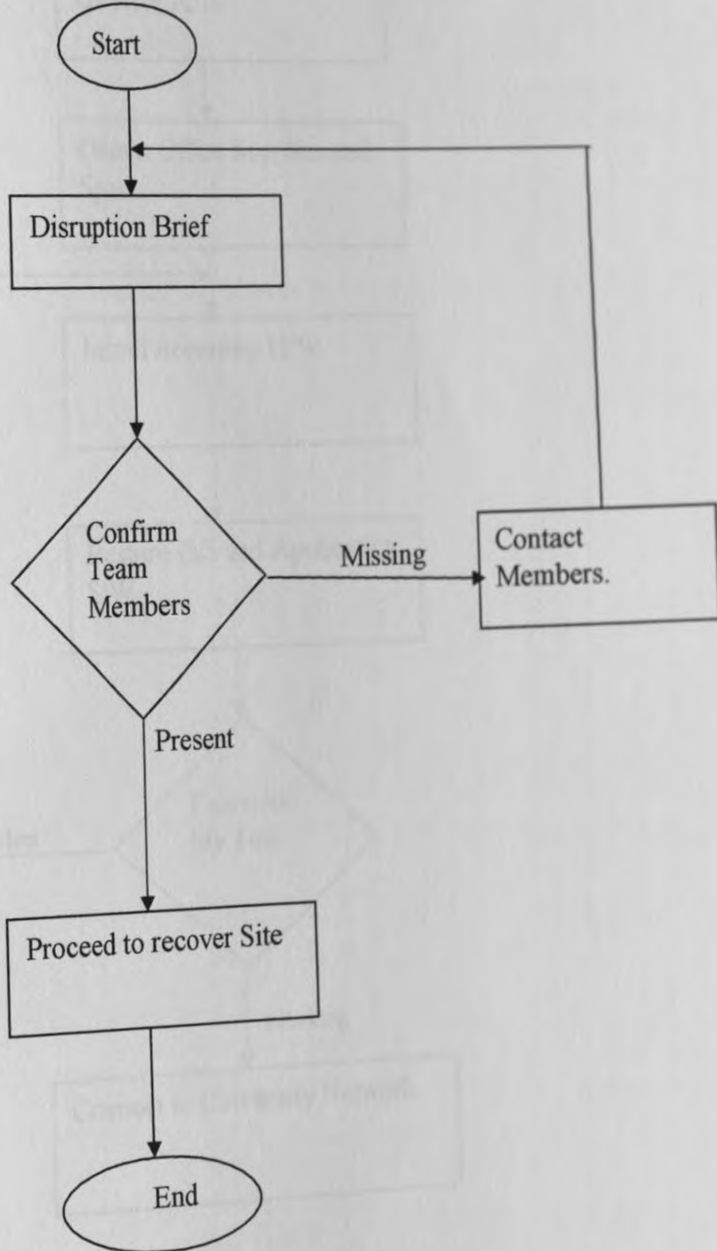
Responsibility

Process Flow

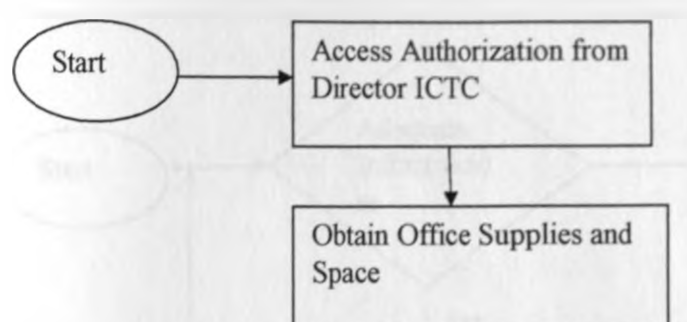
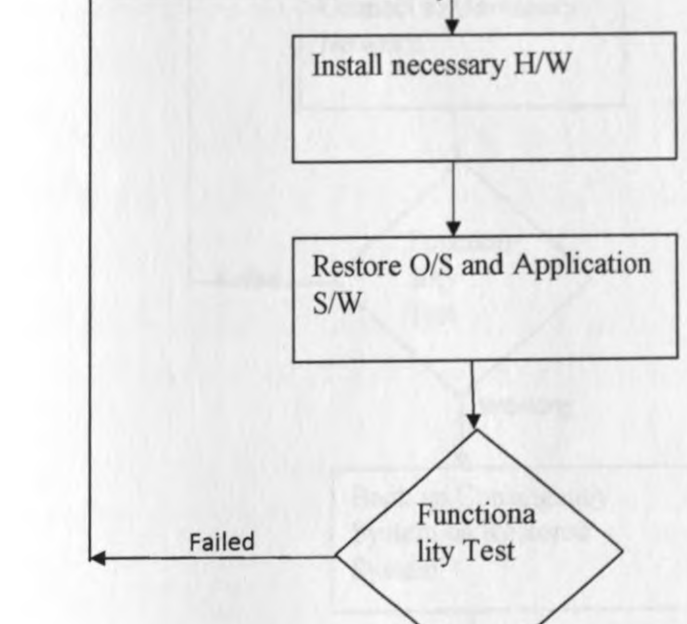
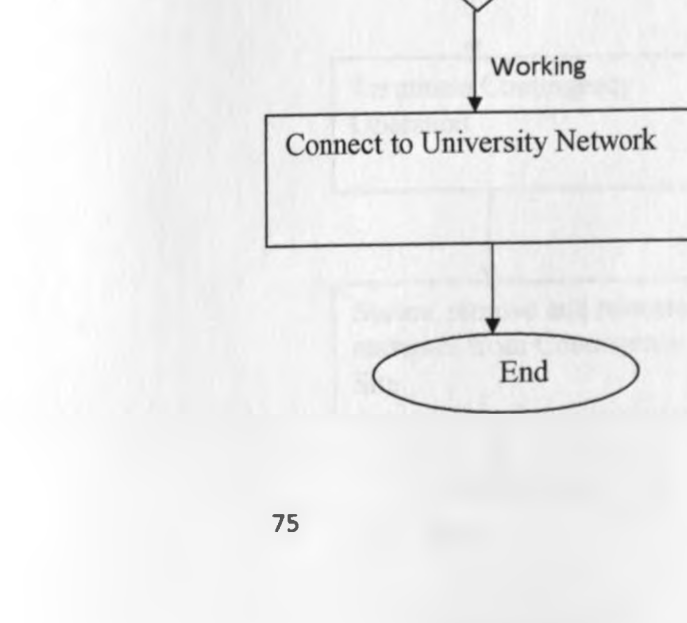
Team Leader

Team Leader

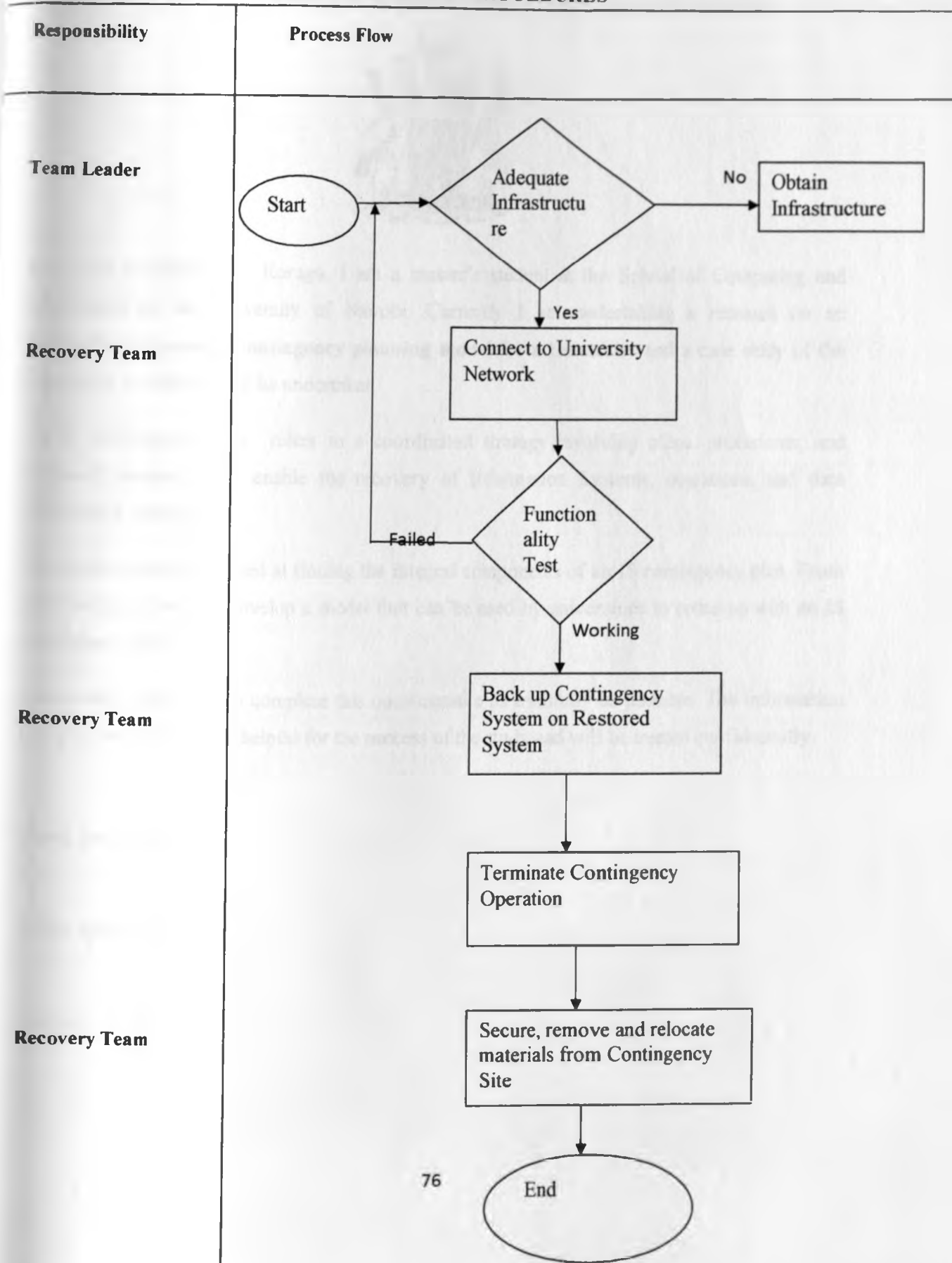
Team Members



# RECOVERY PROCEDURE

Responsibility	Process Flow
Team Leader	 <pre>graph TD; Start([Start]) --&gt; A[Access Authorization from Director ICTC]; A --&gt; B[Obtain Office Supplies and Space];</pre>
Team Members	 <pre>graph TD; B --&gt; C[Install necessary H/W]; C --&gt; D[Restore O/S and Application S/W]; D --&gt; E{Functionality Test}; E -- Failed --&gt; C; E -- Working --&gt; F[Connect to University Network];</pre>
Team Members	 <pre>graph TD; F --&gt; G[Connect to University Network]; G --&gt; H([End]);</pre>

## RECONSTITUTION PROCEDURES



## Appendix II: Information Systems End Users Questionnaire



My name is Godfrey C. Karugu. I am a master's student at the School of Computing and Informatics at the University of Nairobi. Currently I am undertaking a research on an **Information Systems Contingency planning model** for a University and a case study of the University of Nairobi will be undertaken.

An IS contingency plan refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of Information Systems, operations, and data following a disruption

This questionnaire is aimed at finding the integral components of an IS contingency plan. From the findings, I hope to develop a model that can be used by universities to come up with an IS contingency plan.

Please take some time to complete this questionnaire as truthfully as possible. The information you provide will be very helpful for the success of the study and will be treated confidentially.

Thank you in advance

Yours faithfully,

Godfrey Chege Karugu

**Section A: Conducting a Business Impact Analysis**

This section aims at determining whether conducting a Business Impact Analysis is a crucial step in coming up with an information systems contingency plan. Please indicate your agreement or otherwise with the following statements using the following likert scale

BIA is important in;	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
Identifying and prioritizing critical IT systems.					
Identifying outage impacts and allowable outage times					
Identifying critical IT resources					
Determining the minimum IT resources for critical information systems					
Prioritizing information systems recovery during a disruption					

**Section B: Recovery Strategy Formulation**

This section aims at determining whether Identifying preventive and recovery controls is a crucial step in coming up with an information systems contingency plan. Please indicate your agreement or otherwise with the following statements using the following likert scale.

<i>The following strategies are important for an IS contingency plan</i>	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
Frequent, scheduled backups					
Commercial contracts for IT recovery with cold, warm, or hot site vendors					
Uninterruptible power supplies (UPS) to provide short-term backup power to all					

<i>The following strategies are important for an IS contingency plan</i>	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
systems					
Diesel-powered generators to provide long-term backup power					
Air-conditioning systems					
Fire, smoke detectors and suppression system					
Water sensors in the computer room ceiling and floor					
Plastic tarps that may be unrolled over IT equipment to protect it from water damage					
Heat-resistant and waterproof containers for backup media and vital non electronic records					
Emergency master system shutdown switch					
Technologies such as automatic fail-over and mirrored systems.					
Reciprocal agreements with internal or external organizations.					
Service level agreements (SLAs) with the equipment vendors.					

### Section C: Plan Testing, Training and Exercises

This section aims at determining whether Plan Testing, Training, and Exercises is a crucial step in coming up with an information systems contingency plan. Please indicate your agreement or otherwise with the following statements using the following likert scale.

<i>The following areas should be addressed in an IS contingency plan test and training:</i>	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
System recovery on an alternate platform from backup media.					
Coordination among recovery teams					
Internal and external connectivity					
System performance using alternate equipment					
Restoration of normal operations					
Notification procedures					

**Section D: Contingency Plan Awareness.**

This section aims at determining whether staff awareness is important in an information systems contingency planning. Please indicate your agreement or otherwise with the following statements using the following likert scale.

<i>statement</i>	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
Conducting staff awareness program for IS contingency planning is an important step in developing a contingency plan					
Mandatory training for new employees in handling IS contingencies is an important step in developing a contingency plan					

### Section E: Plan Maintenance

This section aims at determining whether Plan Maintenance is a crucial step in coming up with an information systems contingency plan. Please indicate your agreement or otherwise with the following statements using the following likert scale.

At a minimum, the contingency plan should be reviewed and updated on the following elements:	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	1	2	3	4	5
Names and contact information of recovery team members					
Names and contact information of vendors, alternate and off-site vendors					
Hardware, software, changes (types, specifications, and amount )					
Alternate and offsite facility requirements					
IS contingency plan should be audited					

### General Information/Demographic Data

**Gender :** Male  Female

**Age:** 21-30 years , 31-40 years , 41-50 years , 51 years & above

**Number of years in the current Department**  
 Less than 1 year , 1-3 years , 3-5 years , More than 5 years

**Information System Used:** Financial Management system , Health System ,  
 Student Management Information System , Human Resource MIS ,  
 Room Booking and Allocation System , Performance MIS ,  
 Student Clearance System , Q-Pulse System

**Highest Academic Qualification**  
 Diploma  Bachelors  Masters  PhD   
 Others (Please Specify) \_\_\_\_\_



## Appendix III: ICTC Staff Questionnaire



### University of Nairobi Business Impact Analysis (BIA) Questionnaire:

My name is Godfrey Karugu. I am a master's student at the School of Computing and Informatics at the University of Nairobi. Currently I am undertaking a research on an **IS contingency plan model** for a University and a case study of the University of Nairobi will be taken. An IS contingency plan refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption

One of the major steps in developing an IS contingency Plan is conducting a Business Impact Analysis (BIA). The main objectives of this BIA questionnaire are; a) Identify the Critical Business Process at University, b) Identify the critical IT resources that support these business process, c) Determine the outage impacts and the allowable outage times, and d) Determine the recovery priority in the event of a disruption.

Please take some time to complete this questionnaire as truthfully as possible. The information you provide will be very helpful for the success of the study and will be treated confidentially.

Thank you in advance

Yours faithfully,

Godfrey Chege Karugu

**A: University of Nairobi Management Information Systems** The following Management Information Systems are used at the University of Nairobi: Which of the following information systems would you consider to be Critical( Support Critical Business Process at University )

1. Student Management Information System
2. Human Resource Management Information System
3. Financial Management System
4. University Health System
5. E-Learning System
6. Performance Management Information System
7. Q-Pulse
8. Online Room Booking and Allocation System
9. Student Clearance System
10. Joint Admission Board System

**B: Identify System Resources:** Identify the specific Resources that support the critical Information systems identified in (A) above

1. **Name of Information System:** \_\_\_\_\_

**Type of Servers:** Mail server  , Web server  , Database Server  ,  
Application Server  , Antivirus Server  , Authentication server   
Others (Specify) \_\_\_\_\_

**Databases:** Student Database  Staff Database  Financial Database   
Others (Specify) \_\_\_\_\_

**Network Resources:** LAN  WAN  WIFI

**Type of Operating Systems:** Linux based windows Based

**End computing devices:** Desktop  mobile Phone  ipad   
Others (specify) \_\_\_\_\_

Other Resources 83

2. **Name of Information System** \_\_\_\_\_

	<b>Type of Servers:</b> Mail server <input type="checkbox"/> , Web server <input type="checkbox"/> , Database Server <input type="checkbox"/> , Application Server <input type="checkbox"/> , Antivirus Server <input type="checkbox"/> , Authentication server <input type="checkbox"/> Others (Specify) _____
	<b>Databases:</b> Student Database <input type="checkbox"/> Staff Database <input type="checkbox"/> Financial Database <input type="checkbox"/> Others (Specify) _____
	<b>Network Resources:</b> LAN <input type="checkbox"/> WAN <input type="checkbox"/> WIFI <input type="checkbox"/>
	<b>Type of Operating Systems:</b> Linux based windows Based <input type="checkbox"/>
	<b>End computing devices:</b> Desktop <input type="checkbox"/> mobile Phone <input type="checkbox"/> ipad <input type="checkbox"/> Others (specify) _____
	Other Resources

3. **Name of Information System** \_\_\_\_\_

	<b>Type of Servers:</b> Mail server <input type="checkbox"/> , Web server <input type="checkbox"/> , Database Server <input type="checkbox"/> , Application Server <input type="checkbox"/> , Antivirus Server <input type="checkbox"/> , Authentication server <input type="checkbox"/> Others (Specify) _____
	<b>Databases:</b> Student Database <input type="checkbox"/> Staff Database <input type="checkbox"/> Financial Database <input type="checkbox"/> Others (Specify) _____
	<b>Network Resources:</b> LAN <input type="checkbox"/> WAN <input type="checkbox"/> WIFI <input type="checkbox"/>
	<b>Type of Operating Systems:</b> Linux based windows Based <input type="checkbox"/>
	<b>End computing devices:</b> Desktop <input type="checkbox"/> mobile Phone <input type="checkbox"/> ipad <input type="checkbox"/> Others (specify) _____
	Other Resources

**C: Link Critical Information Systems to Critical Resources:** Identify the minimum IT resources required to support the critical information systems Identified in (A) above

Critical Information System	Resources
1.	



