British Journal of Applied Science & Technology
4(3): 492-509, 2014

SCIENCEDOMAIN ***international***
www.sciencedomain.org

Embracing Contingency Planning for University Information Resources

Christopher A. Moturi[1*] and Godfrey Chege Karugu[1]

[1]School of Computing and Informatics, University of Nairobi, Nairobi, Kenya.

Authors' contributions

This work was carried out in collaboration between both authors. Author CAM designed the study, correlated the results and made the draft. Author GCK made the literature review, collected and analyzed data. Both the author read and approved the final manuscript.

Original Research Article

Received 11th August 2013
Accepted 17th October 2013
Published 7th November 2013

ABSTRACT

Aims: This paper discusses the concept of contingency planning for information systems in a university context, uncovers the critical information systems within a university that are most vulnerable, identifies contingency planning models, and establishes a systematic approach that would be followed when implementing a contingency plan program in a university environment.
Study Design: Adapted conceptual model.
Place and Duration of Study: The University of Nairobi between April and July 2012.
Methodology: The adapted model was applied to the University of Nairobi, ICT Centre. The study used primary data that was collected through self-administered questionnaires; one set was administered to the end users spanning across seven departments and another set was distributed to ICT staff.
Results: This study identified the critical university information systems, identified the minimal IT resources that support the critical information systems, established a systematic approach that should be followed when implementing a contingency plan program in university environments, and developed a model contingency plan.
Conclusion: The findings of this research would be of major importance to university policy makers and stakeholders who would be able to make sound decisions and policies regarding the protection of information assets from an informed point of view.

**Corresponding author: E-mail: moturi@uonbi.ac.ke;*

Keywords: Contingency planning; contingency plan model; disaster recovery planning; business continuity planning.

1. INTRODUCTION

1.1 Background

There is a growing consumption of Information and Communications Technology (ICT) in the accomplishment of university core business of research and dissemination of knowledge. The use of ICT 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 institutions. Most universities have well established ICT departments which support core business process. However, there are threats, risks and vulnerabilities that threaten or cause disruption to university information systems. 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. In addition, it would lead to standstill in the recruitment and admission as it is used in the enrollment process. Failure of systems that process examination results would have devastating impact on the reputation of the university. It is therefore the responsibility of the custodian of such systems to develop and document a contingency plan that would be implemented in case such threats strike and render the information systems unavailable. This paper discusses the concept of contingency planning for information systems, uncovers the critical information systems within a university that are most vulnerable, identifies contingency planning models, and recommends a model that can be adapted by a Kenyan university to implement a contingency plan.

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. The risk levels to the university information systems increases as the IT adoption increases in Kenya. This trend implies that the potential threat to information systems is not only a historical occurrence but also a current and 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. Information systems 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 [1].

1.2 The Need for Information Systems Contingency Planning

According to Hoffman [2], about 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. The time taken to recover critical business processes after a disruption is a universal determinant of a successful recovery [3]. 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. Contingency planning concerns 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 [4].

At university level, the 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 ICT Centre was created in 2002 and has over 112 highly qualified professional ICT staff who plan, implement and support the ICT infrastructure and services [5]. The University's ICT policy guidelines [6] has several elements which include: Network Development and Management; ICT Security and Internet; Software Development, Support and Use; User Support; ICT Equipment Maintenance; ICT Training; Database Administration; and Procurement Policy. A critical review of the policy indicates that conscious consideration of contingency planning has not been taken into account.

1.3 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 [1].

1.4 Information System Contingency Plan Constructs

Smith and Sherwood [7] identified nine phases of disaster recovery plan process: policy statement, planning responsibilities, incident management responsibility, business impact analysis, recovery strategies, training and awareness, testing, maintenance, and documentation. A framework based on how the phases for disaster recovery planning can be used to address concerns beyond boundaries of an organization is presented by Heikkinen and Sarkis [8]. Chow [9] proposed fourteen 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. [10] proposed that an effective disaster recovery plan 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.

1.5 Information System Contingency Plan Constructs Discussion

a) *Top Management Commitment:* Top management commitment is considered the most vital construct to the success of IS contingency plan. Top management finalizes an annual budget to support implementation of the plan, decides when and how the plan should be implemented; and dictates the level of cooperation and support that should be provided by the various departments when the plan is launched. This construct is considered as critically important because IS contingency plan requires long-term planning, and that it involves ongoing capital investment [9,11].

b) *Risk Assessment and Impact Analysis*: This determines how long an organization can survive without the support of critical business functions when a disaster strikes [11]. All critical functions must be pre-determined before a contingency plan strategy is chosen for an organization [9]. Risk assessment identifies the events that are most likely to pose threats to a firm 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 [4]
c) *Minimum Processing Requirement:* The minimum processing requirement determines an acceptable recovery time, 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 [10,11].
d) *Alternative Site:* Organizations that highly dependent on IS applications must consider an alternative site with which they can back up their IS resources [12]. Alternative sites can be operated on an external site or in-house site, and can be implemented in the mode of hot site, cold site, mobile recovery facilities, or mirrored site [13].
e) *Recovery Tea:* A team approach to managing the recovery process in the event of a disaster is important for two reasons: all relevant staff may not be presented when disaster strikes; when more of the right people are involved, more intelligent answers to recovery problems may be generated [9].
f) *Testing:* Testing should be designed in such a way that the weaknesses of the plan can be identified [14].
g) *Training:* Training is 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 [15].
h) *Documentation:* The exact details of functions, personnel, responsibilities, contact names and numbers, and resources for the recovery, involved with a disaster, must be documented [13].
i) *Maintenance:* Cerullo et al. [11] says 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 [9].
j) *User Participation:* The users of information systems must participate and monitor the development processes of IS contingency plan in an organization [10]. 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. IS personnel should also review the IS contingency plan regularly from a technical standpoint so that minimum information systems service disruption are sustained.

From the literature reviewed, the recurring constructs identified were broadly grouped as follows:

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

This classification was informed by the standard models used in the development of information systems contingency plan in this study. These models are: a) NIST Model: IS Contingency Planning Guide; b) ISO/IEC 24762:2008: Framework for Disaster Recovery Planning.

1.6 The NIST Model

NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems [1], provides instructions, recommendations, and considerations for federal information system contingency planning. The guide defines seven progressive steps that an organization may apply to develop and maintain a viable contingency planning program. The steps, designed to be integrated into each stage of the systems development life cycle, are as follows: develop the contingency planning policy; conduct the business impact analysis (BIA); identify preventive controls; create contingency strategies; develop an information system contingency plan; ensure plan testing, training, and exercises; ensure plan maintenance.

1.7 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 [16] recommends that an organization should implement the following phases: business impact analysis, recovery strategy formulation, recovery plan development, plan testing, plan awareness, recovery plan maintenance.

1.8 Proposed University Information Systems Contingency Plan Model

Based on the literature reviewed and the two standards referred, we propose the following information system contingency plan model for embracing contingency planning for university information resources (Fig. 1). 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.

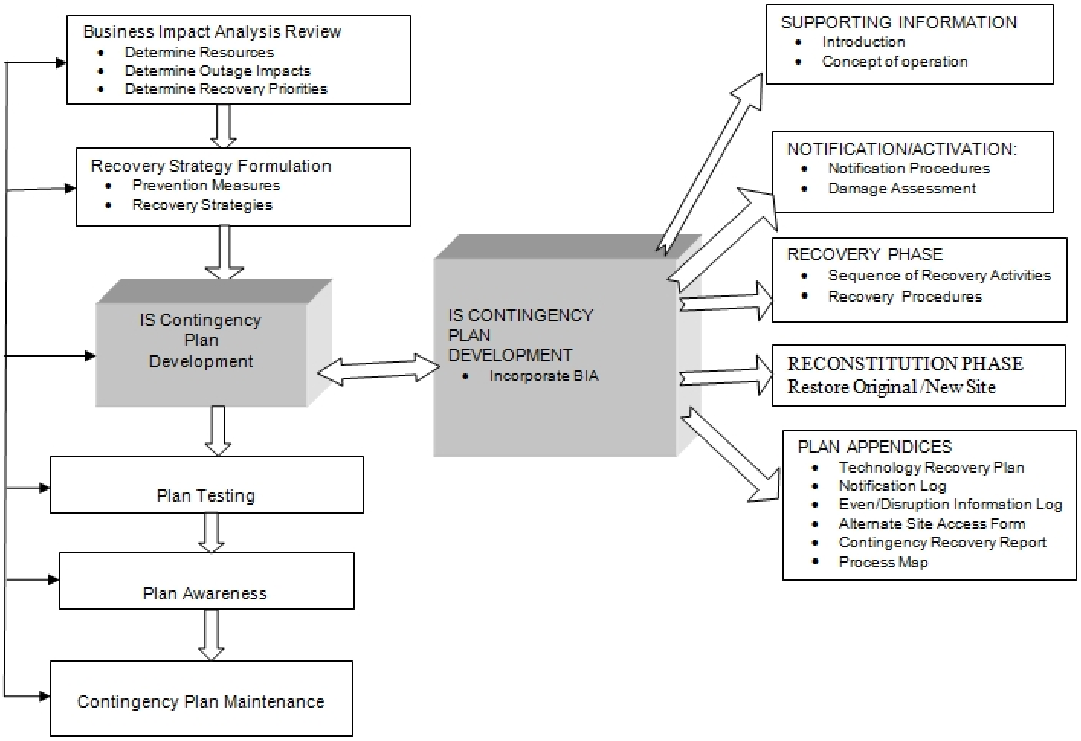
Business Impact Analysis Review
• Determine Resources
• Determine Outage Impacts
• Determine Recovery Priorities
Recovery Strategy Formulation
• Prevention Measures
• Recovery Strategies
IS Contingency Plan Development
IS CONTINGENCY PLAN DEVELOPMENT
• Incorporate BIA
Plan Testing
Plan Awareness
Contingency Plan Maintenance
SUPPORTING INFORMATION
• Introduction
• Concept of operation
NOTIFICATION/ACTIVATION:
• Notification Procedures
• Damage Assessment
RECOVERY PHASE
• Sequence of Recovery Activities
• Recovery Procedures
RECONSTITUTION PHASE
Restore Original /New Site
PLAN APPENDICES
• Technology Recovery Plan
• Notification Log
• Even/Disruption Information Log
• Alternate Site Access Form
• Contingency Recovery Report
• Process Map

Fig. 1. Proposed University IS Contingency Plan Model

2. METHODOLOGY

2.1 Research Design

This study was conducted through a cross sectional descriptive case study to obtain data from a cross section of staff at the University of Nairobi. The target population was the staff in the four departments of the ICT Centre namely Management Information System (MIS); User Support and Maintenance; Network Infrastructure; Communication and Data Centre. The target population consisted of the 112 staff as given by the website link http://ict.uonbi.ac.ke/. A stratified random sampling technique was used and yielded the respondents shown in Table 1.

Table 1. ICT Staff Respondents

Department	Population	Sample Size
MIS	32	20
User Support and Maintenance	41	25
Network Infrastructure	9	5
Communication and Data Centre	30	18
Total	112	68

Random sampling was used to identify the number of end users across the departments. This sample size was arrived at according the formula by Mugenda and Mugenda [17] after considering seven user departments namely: Student Registration; Finance; Administration and Human Resource; Health; Performance Contracting; Accommodation; and Library. Eleven users of information systems from every user department and two from Performance Contracting department were selected so as to give detailed account of the questionnaire.

2.2 Data Collection and Analysis

The study used primary data that was collected through a self-administered questionnaire. 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 the seven departments. Another set was distributed to technical respondents who are conversant with technical ICT details. The respondents are spread across the four ICTC departments.

The objective of the end-user questionnaire was to find out the integral components of an IS contingency plan. The objective of the technical questionnaire was to conduct a Business Impact Analysis (BIA) in order to identify the critical business process at university; identify the critical IT resources that support these business process; determine the outage impacts and the allowable outage times; and determine the recovery priority in the event of a disruption.

The key questions in the end-user questionnaire involved the following key issues:

i. Conducting a Business Impact Analysis - determining whether conducting a Business Impact Analysis is a crucial step in developing information systems contingency plan.
ii. Recovery Strategy Formulation - determining whether identifying preventive and recovery controls is a crucial step in developing information systems contingency plan.
iii. Plan Testing, Training and Exercises - determining whether Plan Testing, Training, and Exercises is a crucial step in developing information systems contingency plan.
iv. Contingency Plan Awareness - determining whether staff awareness is important in an information systems contingency planning.
v. Plan Maintenance - determining whether Plan Maintenance is a crucial step in coming in developing information systems contingency plan.

The key questions in the ICT staff questionnaire involved the following issues:

i. Identification of the critical information systems at the University.
ii. Identification of the specific resources that support the critical information system identified.
iii. Link critical information systems to critical - identification of the minimum IT resources required to support the critical information systems identified.
iv. Identification of outage impacts and allowable outage times - the effect on the critical process if a critical resource is unavailable and identification of the maximum acceptable period that a resource could be unavailable before unacceptable impacts resulted.
v. Prioritize resource recovery – listing the priority associated with recovering a specific resource, based on the outage impact and allowable outage times.

3. RESULTS AND DISCUSSION

3.1 Data Validity and Reliability

The reliability of the questionnaire was determined through a pilot study involving 8 members of staff at the University. The Cronbach's coefficient Alpha formula was used to estimate the internal consistency of the study tool and with a reliability coefficient as shown in Table 2 below. This is above the recommended 0.7.

Table 2. Reliability test

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

Out of the 136 questionnaires handed out, 75 were properly filled and/or returned with a response rate of 59 per cent among end users, 51 per cent technical staff category, and overall 55 per cent. According to Mugenda and Mugenda [17] a response rate of 50% or more is adequate for data analysis.

3.2 Responses from End Users

3.2.1 Business impact analysis

The study sought to establish whether conducting a Business Impact Analysis is a crucial step in developing an information systems contingency plan. 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 [9] 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.

3.2.2 Recovery strategy formulation

The study sought to establish whether identifying preventive controls and recovery measures is a crucial step in developing 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%), 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 [12] who asserts that firms that are highly dependent on information systems must consider an alternative site with which they can back up so that they can be recovered easily in the event of a disaster. The findings further agree with those of Hawkins et al. [13] 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.

3.2.3 Plan test

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 at al. [14] 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.

3.2.4 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. [18] 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.

3.2.5 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 et al. [11] who assert that having an IS contingency plan without ongoing maintenance is worse than not having a plan at all.

3.3 Responses from Technical Staff

3.3.1 Critical information systems

The study sought to identify the critical information systems at the University. An average score was used to rank the systems from the most critical to the least critical. Table 3 below shows this ranking.

Table 3. Ranking of critical information systems

System	Average Score
Student Management Information	0.86
Human Resource Management Information Systems	0.66
Financial Management System	0.57
Online Room Booking and Allocation System	0.51
University Health System	0.17
Joint Admission Board System	0.17
Student Clearance System	0.14
Quality Management System (Q-Pulse)	0.09

3.3.2 Resources supporting critical information systems

The study sought to investigate the various resources that support the critical information systems.

3.3.2.1 Student management information systems (SMIS)

Table 4 below summarizes the resources required for the SMIS. The servers which were found to be important in supporting the Student Management Information were web server, database server, application server, and authentication server. This is supported by the fact that all operations at university are performed online, making servers to be among the critical resources.

The specific databases that are crucial in supporting the SMIS include the student database and financial database. The network resources that supported the Student Management Information system included LAN resources followed by WAN resources. The type of operating system that supports the SMIS is Linux. The end computing devices that supported the SMIS included desktops, mobile and ipads. Technical staff also indicated that laptops were some of the other end computing devices that are used.

Table 4. Resources required for student management information system

System	Resources	Response Rate (%)
Servers	Web Server	100
	Database Server	83
	Application Server	83
	Authentication Server	67
	Mail Server	33
	Anti-Virus Server	33
Databases	Student Database	71
	Financial	57
	Staff Database	14
Network Resources	LAN	80
	WAN	60
	WiFi	40
Operating Systems	Linux	80
	Window	20
End Computing Devices	Desktop	100
	iPad	80
	Mobile	60

3.3.2.2 Human resource management information system (HRMIS)

Table 5 below summarizes the resources required for the HRMIS. The servers that were found to be important in supporting the HRMIS included the web server, database server, and the application server. The specific databases that are crucial in supporting the HRMIS is the staff database. The network resources that supported the HRMIS are WAN and LAN, with Linux as the operating system. The end computing devices that supported the HRMIS included desktops mobile and ipads.

Table 5. Resources required for human resource management information system

System	Resources	Response Rate (%)
Servers	Web Server	83
	Database Server	67
	Application Server	50
	Authentication Server	33
	Anti-Virus Server	33
	Mail Server	17
Databases	Student Database	57
	Financial	29
Network Resources	LAN	80
	WAN	60
	WiFi	40
Operating Systems	Linux	80
	Window	20
End Computing Devices	Desktop	80
	iPad	40
	Mobile	40

3.3.2.3 Financial management system

Table 6 below summarizes the resources required for the FMS. The server resources that were found to be important in supporting the FMS are the web server, database server, and the application server. The specific databases that are crucial in supporting the FMS is the financial database. The network resources that supported the FMS is LAN and WAN while the operating system that support FMS is Windows followed by Linux. The end computing devices that supported the FMS included desktops.

Table 6. Resources required for financial management system (FMS)

System	Resources	Response Rate (%)
Servers	Application Server	100
	Web Server	67
	Database Server	67
Databases	Financial	75
	Student	25
	Student	25
Network Resources	LAN	100
	WAN	67
Operating Systems	Linux	100
	Window	67
End Computing Devices	Desktop	100
	iPad	33
	Mobile	33

3.3.3 IT resources for critical information systems

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

i) Web server: Supporting the three critical IS systems identified (SMIS, HRMIS, FMS)
ii) Database server: required to provide data for the management information systems
iii) Application server: used by off the shelve system at the university.
iv) Desktop Computers: support users of the critical information systems.
v) LAN/WAN with associated routers, hubs and fiber connections. Support the various interconnections.
vi) Power Supply.

3.3.4 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 Table 7 below, the next step was to develop recovery priorities for the system resources. We made use 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.

Table 7. Outage impacts and allowable outage time

Resource	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 ▪ 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	I 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	2 Hours
Email Server	Users could not send and receive e-mail	6 Hours
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

3.3.5 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 (Table 8). 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.

Table 8. Recovery priority

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
Email Server	Low	6 Hours

3.3.6 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.

3.4 Discussion

This paper sought to discuss the embracing of contingency planning for information resources in a university context. A conceptual model was adapted from the ISO/IEC 24762:2008 standard. The model was applied to University of Nairobi, ICT Centre to test its applicability.

The responses received from the end users determined the crucial steps in the development of an information systems contingency plan. These end users were the custodians of the university information resources. The findings confirmed that business impact analysis, recovery strategies formulation, plan testing, conducting staff awareness program and plan maintenance are crucial steps.

The first objective of the application of the conceptual model to the technical staff 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 (0.66), and the Financial Management System (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.

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.4.5 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:

3.4.6 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.

3.4.7 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

3.4.8 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.

3.4.9 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.

3.4.10 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 provides a framework that can be adapted by other universities when developing their own IS contingency plans.

4. CONCLUSION

As information systems become indispensable in the provision of universities core functions, IS contingency plan have become an essential component of information systems. This study identified the critical university information systems. 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. Using a conceptual model adapted from ISO/IEC 24762:2008 the study demonstrates how the standard can be contextualized to a university environment. The 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 university environments. We 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. A model contingency plan has been developed. The model identifies three main phases in the documentation of a contingency plan, notification/activation phase, recovery phase, and reconstitution phase.

IS contingency plans 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 prevents, mitigates and ensures continuous operation is supreme.

It is hoped that the findings of this research will be of major importance to university 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, ICT Center may use the findings 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.

Further work will focus on the factors affecting the success of IS contingency plan in a university environment. This would make use of such models such as the Technology Adoption Model (TAM). 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. Testing of the IS contingency plan should be conducted to ascertain usability. Cerullo et al. [11] reported 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 a university is faced with the situation of putting the plan in action.

COMPETING INTERESTS

The authors declare that there are no competing interests.

REFERENCES

1. Swanson M, Wohl A, Lucinda L, Grance T, Hash J, Thomas R. Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Washington, NIST Special Publication. 2002;800-34.
2. Hoffman T. Denial Stalls Disaster Recovery Plans. ComputerWorld; 1998. Retrieved 2nd June, 2012, from http://911research.wtc7.net/essays/nist/
3. Toigo JW. Disaster Recovery Planning: Preparing for the Unthinkable (3rd Ed). New Jersey: Prentice Hall; 2003.
4. Blakley B, McDermott E, Geer D. Information Security is Information Risk Management, NSPW 2001: Proceedings of the 2001 workshop on New Security Paradigms, ACM. 2001;97 –104.
5. University of Nairobi. ICT Developments at the University of Nairobi for the Period 2004-2009: A High Level Summary Report Depicting Status of Automation. Nairobi: University of Nairobi; 2009.
6. University of Nairobi. Information and Communication Technology Policy Guidelines. Nairobi: University of Nairobi; 2010.
7. Smith M, Sherwood J. Business Continuity Planning. Computer & Security Journal. 1995;14(1):14-23.
8. Heikkinen D, Sarkis J. Disaster Recovery Issues for EDI Systems, Logistics Information Management. 1996;9(6):27-34
9. Chow WS. Success factors for IS disaster recovery planning in Hong Kong. Information Management & Computer Security. 2000;8(2):80-86.
10. Wong BK, Monaco JA, Sellaro CL. Disaster Recovery Planning: Suggestions to Top Management and Information Systems Managers. Journal of Systems Management. 2004;5(4):28-32.
11. Cerullo MJ, McDuffie RS, Smith LM. Planning for Disaster. The DRJ Journal, 2004;6:34-38.
12. Blake WF. Making Recovery a Priority. Security Management Journal. 2002;36(4):71-74.
13. Hawkins SM, Yen DC, Chou DC. Disaster Recovery Planning: A Strategy for Data Security. Information Management & Computer Security. 2000;8(5):222-229.

14. Lee S, Ross S. Disaster Recovery Planning for Information Systems. Information Resources Management Journal. 1995;3:18-23.
15. Farahmand F, Navathe SB, Enslow PH, Sharp GP. Managing Vulnerabilities of Information Systems to Security Incidents, Proceedings of the 5th International Conference on Electronic Commerce. 2003:348-354. New York: ACM.
16. ISO. Guidelines for Information and Communications Technology Disaster Recovery Services; 2008. ISO/IEC 24762.,ISO
17. Mugenda O, Mugenda A. Research Methods: Quantitative & Qualitative approaches, Acts Press; 2003.
18. Mitome Y, Speer KD, Swift B. Embracing Disaster with Contingency Planning, Risk Management Journal. 2001;48(5):18-27

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history.php?iid=307&id=5&aid=2439