UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

RESEARCH

TOPIC

Integrating Risk Management in the ICT Service Management Frameworks: The Case of ITIL Service Management Framework in a Local Airline Industry.

Submitted by

Titus M. Kitavi

P56/P/7277/05

Supervisor

Dr. Daniel Orwa

July, 2014

Submitted in partial fulfillment of the requirement of a Master of Science degree in information Systems of the University Of Nairobi

Declaration

I, Titus Makau Kitavi, declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the Thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Signature:................................... Date:...................................
Titus Makau Kitavi
P56/7277/05

APPROVAL

This research project has been submitted as part of fulfillment of requirements for the Master of Science in Information Systems with my approval as the Supervisor.

Signature:................................... Date:...................................
Dr. Daniel O. Ochieng
School of Computing and Informatics,
University of Nairobi

Abstract

The complexity of managing IT Service delivery has led to growth of IT Service management (ITSM) as an important area of focus in the IT industry. Organizations are therefore investing in IT service management best practices to manage their IT services. ITIL is considered as one of best framework for IT Service Management and it is widely used in the business world. This framework is strong on delivery and support processes in that it describes how to structure operational processes but is weak on risk management processes.

The broad objective of this research was to come up with a framework of ICT service management that improves the current ITIL service delivery framework to incorporate Risk Management. Specifically the research sought to identify risk management attributes that could be applicable to ICT services, determine what needs to be incorporated in the ITIL service management framework to address risk management gaps and further to develop a conceptual ITIL Service management framework that incorporates Risk management. Both quantitative and qualitative research approaches were used to complement each other. The research used questionnaires, data from the ITSM tool, focused group discussions, targeted interviews, as well as independent observation of processes.

From the findings, there were Gaps in Disaster preparedness and they only came to the light once disaster struck. It was also noted that once a risk item was identified, mitigation were put in place urgently. However, there were no post implementation reviews. Precisely, ITIL processes that had not integrated risk management adequately include Strategy management, IT financial management, Service portfolio management, demand management and service catalogue process. Significant findings emanating from this research were that, apart from driving change through continual improvement, the organization must be prepared for rapid transitions and transformations driven by changes in an organization environment or internal situation while managing potential risks. Changes may be driven by sourcing decisions, actions of competitors, technology innovations and shifts in customer preferences hence IT Service management should respond effectively and efficiently.

In conclusion, it is apparent that the value of ITIL to organizations is undeniable as it helps reduce IT costs, increase IT performance and improve business performance through IT-business alignment. However ITIL service management framework does not provide a clear concept on how to treat risk yet risk management is essential to all organizations. It is therefore important to ensure that organizations Integrate or adapt a risk management framework, embedded it into ITIL, document the methodology, processes and create key risk indicators, link them to strategic responses and develop metrics to measure compliance as well as ensure effective communication.

Acknowledgements

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

IT – Information Technology

ICT- Information Communication Technology

I.S. – Information Systems Department or Function

OGC ®, Office of Government; OGC ® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom

ITIL® - Information Technology Library; ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries

ITSM - Information Technology Service Management

SLA - Service Level Agreement

COBIT® - Control Objectives for Information and related Technologies. Created in 1995 as an audit framework and has matured to become an overall IT Management Framework

ISO/IEC 20000:2005 - promotes the adoption of an integrated process approach to effectively deliver managed IT services to meet business and customer requirements.

ISO/IEC 15504 - provides a framework for the assessment of process capability. Is also known as SPICE-Software Process Improvement and Capability determination

ISO/IEC 19770:2006 - Developed to enable an organization to prove that it is performing software asset management (SAM) to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall

M_o_R® - Management of Risk and it provides an alternative generic framework for the management of risk across all parts of an organization – strategic, programme, project and operational.

PMBOK® -Project Management Body of Knowledge; is owned and authored by the Project Management Institute (PMI). The Project Management Body of Knowledge is the sum of knowledge within the profession of project management.

CMMI - Capability Maturity Model Integrated; was created by Software Engineering Institute in 1991 as a model for demonstrating the maturity of software development processes. CMMI has grown and is now the de facto standard for measuring the maturity of any process.

Six Sigma - The fundamental objective of the Six Sigma methodology is the implementation of a measurement-based strategy that focuses on process improvement and variation reduction through the application of Six Sigma improvement projects.

MOF - Microsoft Operations Framework; delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. It encompasses the entire IT lifecycle by integrating

ITSMF - IT Service Management Forum; is an independent, internationally, not-for-profit organization of IT professionals worldwide who promote ITIL best practice by supporting education and training, discussing the development of ITSM tools, initiating advisory ideas about ITSM and holding conventions. The ITSMF is a brand and trademark which is often copied by partners, member and local chapters.

 ENISA - European Network and Information Security Agency.

CHAPTER ONE: INTRODUCTION

1.1 Background to the Research

Organizations are increasingly dependent upon Information Technology (IT) to support their business strategies. This growing dependency necessitates quality IT services that is matched to business needs and user requirements. Information Technology Service Management (ITSM) is a process-based practice intended to align the delivery of information technology (IT) services with needs of the enterprise, emphasizing benefits to customers. ITSM involves a paradigm shift from managing IT as stacks of individual components to focusing on the delivery of end-to-end services using best practice process models (Margaret Rouse, August 2005). In addition ITSM is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organization.

Information Technology industry has developed several frameworks to manage organizations IT requirements. Organizations need to comprehend which framework will better manage their IT services, by considering the market and organization requirements (OGC SS, 2007). ITIL (Information Technology Infrastructure Library) is one such comprehensive suite of best practice process models and an authoritative framework for ITSM which helps organization and individuals to govern IT services in a structured format and ensure meeting service standards both within the organization or across third party service providers (Cory Janssen, 2010).

Organization operate in a web of risks which span from the cluster of natural catastrophic failure related to human acts, breach of security, financial turmoil, unsteady business environments and project failures. Risk management is an increasingly important element of corporate governance and is closely associated with the pursuit of improved business performance, innovation and productivity. The identification, analysis, acknowledgement and mitigation of risks are essential to the process of acquiring and implementing new IT products. By identifying potential risks before undertaking a business activity or business decision, management can determine the likelihood and potential impact of the risks identified, as well as strategies to avert or minimize the threats that each risk poses.

To support the business strategy, one of the local airline industry players in Kenya has invested in the ITIL framework to provide a structured way of delivering IT service to the end users. These services range from the traditional Oracle Enterprise Resource Planning, collaboration platforms such as Microsoft Exchange and Microsoft SharePoint to other specific airline applications. With the recent technology developments in Kenya, other unique services such as Mpesa, Airtel Money and Yu - cash have emerged and are strongly influencing the way business transactions are processed. These unique services plus an upwards trend of adoption of web applications pose a great challenge and necessitate IS managers to re-look at the way ICT services are managed with an aim of managing associated risks. The research focused on improving risk management within ITIL framework adopted by this selected local airline.

1.2 Statement of the problem

The complexity of managing IT Service delivery has led to growth of IT Service management (ITSM) as an important area of focus in the IT industry. IT is a key business driver and hence competitive organizations are not just investing in expensive IT infrastructure but also implementing service and customer centric IT service management best practices. ITIL is considered a framework of best practice guidance for IT Service Management and it is widely used in the business world. In spite of this, ITIL has some gaps in Risk Management specification. Despite ITIL stating that risk should be identified, measured and mitigated, it is not clear on how to execute these since no actual process is defined on how to deal with risk (Sarah Villa, 2012). As a matter of fact, there are many

books dealing with ITIL but these publications do not prescribe how to adopt, adapt or implement the risk management guidelines as part of a service management strategy.

This gap has made it necessary for organizations to invest in multiple expensive frameworks to manage their IT services end – to – end thereby increasing costs and management complexity. The selected local airline had adopted Information Security Management framework (ISMS) to manage IT risk despite having implemented the robust ITIL framework for IT service management. It was essential therefore to come up with a framework of ICT service management that improves the current ITIL service delivery framework to incorporate Risk Management.

Few studies have to date examined ITIL implementation within an environment where risk management is integrated as part of the framework. Other researchers argue that ITIL adoption will lead to improved risk management practices. These isolated cases, however, need to be supported with further empirical research, which this research intended to provide.

1.3 Purpose of the research

The purpose of the research was come up with a conceptual ICT service management framework that improves the current ITIL service delivery framework to incorporate Risk Management.

1.4 Objectives

The research sought to:-.

- Identify Risk management attributes that could be applicable to ICT services.
- Determine what needs to be incorporated in the ITIL service management framework to address the risk management gaps.
- Develop a conceptual ITIL Service management framework that incorporates Risk management.

1.5 Research Questions
- What are the Risk management attributes that could be applicable to ICT services?
- What needs to be incorporated in the ITIL Service management framework to address risk management?

1.6 Significance of the Research

The research sought to determine what needs to be incorporated in the ITIL service management framework to address risk management gaps and improve the current ITIL service delivery framework to incorporate Risk Management thus adding to the body of knowledge.

The Research benefits the following:-

- **IS managers** - The research benefits IS Managers by introducing a "one-stop-shop" improved service delivery framework that addresses all the variables of ICT service management namely Usability (Customer Satisfaction), Availability, Capacity, Security, Continuity and Risk Management.
- **Academia** - The research benefits the academic fraternity by understanding Risk Management within the context of a service industry.
- **Other researchers** -The research benefits other researchers by coming up with an improved service delivery framework that incorporate Risk Management hence adding to the body of knowledge.

2

1.7 Scope of the Research

Quite a number of risks exist within various processes in an organization which need different levels of attention. This research was limited to risk management within the context of ITIL implementation in the local airline industry and an independent observation of processes made on a regional carrier with local presence.

1.8 Limitations of the Research

i) The local airline industry may not have been representative enough to provide a typical research compared to the international airlines industry.

ii) The extent of ITIL implementation in the local airline industry – Not all local airlines have implemented ITIL and the one that have already implemented ITIL, the implemented processes are at different maturity levels. This may not represent a typical ITIL implementation.

1.9 Delimitation of the research

There exists a wide literature base and experiences on various ITSM frameworks. These presented an opportunity of comparing and contrasting the frameworks so as to come up with a better conclusion on how to address gaps related risk management within ITIL framework. It was also noted that one of the local airlines had adopted ITIL for almost a decade and thus the employees were conversant and willing to participate in the research.

1.10 Assumptions of the research

i) The local airline industry environment presented a typical business case research.

ii) The results of the research were generic enough to address risks in any service industry.

1.11 Chapter Summary

This chapter highlighted the origins and importance of IT Service Management Frameworks and how they are increasingly being adopted by organizations to deliver IT services and-to-end. It also highlighted the dilemma that organizations face while trying to deliver these IT services end-to-end. The chapter has also laid down the intended research and the research questions under which the research was undertaken. The importance and the scope of research have also been highlighted, with the scope covering the local airline industry.

2.1 Introduction

As a consequence of the fact that information technologies strategically differentiates Organizations, structuring and managing IT activities has become one of the main focuses of the organizations (Lui et al, 2010). In addition, IT assets (computer hardware, software, telecommunications facilities and human knowledge capital) have become essential for effective organizational management as they provide great value to business (Cruichy et al, 2005 &Kouns et al, 2010). To be successful in business, IT infrastructure should be effectively managed in the organization because of the fact that "IT is now at the core of most organizations" to execute strategy (OGC SS, 2007). The practice of IT governance has emerged as a discipline to enable organizations better manage IT assets and more so investments. In addition to this, to enable effective management of IT, a great number of IT governance standards and frameworks have emerged, including ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and Related Technology), ASL (Application Services Library), Six Sigma, CMM/CMMI, IT Service CMM, SAS70, ISO 17799,SOX (Sarbanes Oxley), SysTrust, PRINCE2 (OGC SS,2007).

Figure 1: **International standard frameworks**
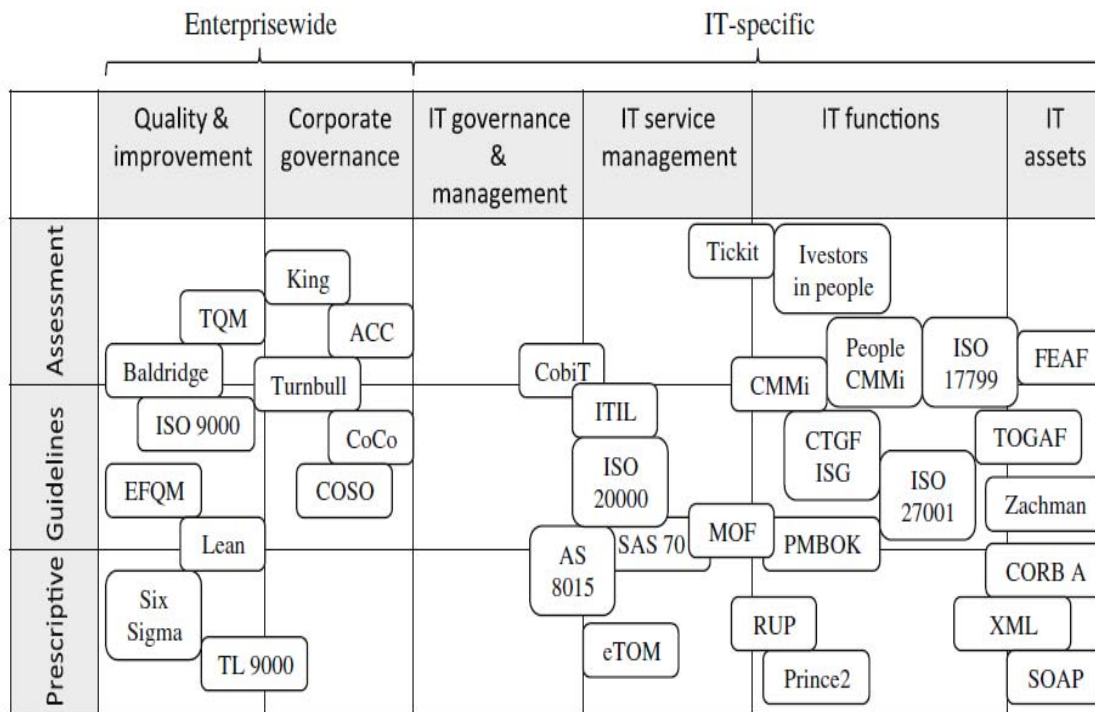
Source: Gartner, Inc., www.gartner.com accessed 13th August 2013

These frameworks cover different aspects of governance and not a single one is adequate to provide effective IT Governance and Management. To manage IT as a whole efficiently, different models should be applied together (OGC SS, 2007). However, implementing different models into an organization is considerably difficult and requires more expertise. Moreover, these frameworks have been translated to a few different languages. An example is Turkish language which has not been in the list of the translated languages; hence this issue has become one of the reasons that has prevented organizations in Turkey from adapting the frameworks easily and effectively.

According to the European Network and Information Security Agency (ENISA, 2010) the major problems in risk Management include:-

i). Low awareness of management activities within the public and private sector.

ii). Absence of a common language in the area of risk management to facilitate communication among stake holders.

iii). Lack of surveys on existing methods, tools and good practices.

iv). Limited or non-existent interoperability of methods and integration with corporate governance.

Another issue is the use of tools to support risk management. In the use and benefits of tools for project risk management article, a large number of tools to support the various phases of the risk management process are shown and those associated with successful projects are highlighted. Other elements used to support risk management are the metrics. These metrics help the organization to be in a better position to manage future events. There are two metrics that stand out; the Key Risk Indicators (KRI) and the Key Performance Indicators (KPI).

While KPIs provide high level overview of the performance of the organization, they focus exclusively on its historical performance of key units as well as operations, whereas KRIs provide timely lead indicator information about immerging risks. In some cases KRIs may represent key ratios that the management tracks as indicators of evolving risks and potential opportunities which point out the need for action to be taken (Elieson, 2006).

2.2 ICT Related Risk

Successful ICT risk management in organizations has been a concern for businesses over the past 10 years. For example, a computer security institute research shows that $202 million was lost in computer crime in 2003 (McAdams 2004). A report by the Audit Commission of the United Kingdom identifies increase in ICT abuses and frauds, regardless of whether organizations have concrete ICT governance arrangements in place (Audit Commission 2005). A government report in the USA shows that over 80 percent of ICT development projects have failed in whole or in part due to poor ICT risk management (Center for Technology in Government 2008). ICT risks have been identified for business and are categorized into operational, technical or security and strategic risks.

a) **Operational risks**- Human resources are imperative factor in organizations because their roles and responsibilities directly affect the processes of information flow and audit related to risk management (Willcocks et al 2006). However these resources can also be risk factors to organizations.

b) **Technical or security risks** - Technical or security risks result from any ICT infrastructure and security systems breaches. ICT infrastructure refers to the scope of the ICT domain where ICT produces data through input, processing, output (IPO) processes and disseminates information to internal and external parties where as information security component is focused to ensure that data and information are protected through identification and authentication, authorization, confidentiality and integrity (Smith & Eloff 2002, p. 268). If any of these parameters is weak, then there is a probability that the organization is exposed to risk.

c) **Strategic risk** - Strategic risk is at the planning level. Information system architecture (ISA) development can be difficult for users at the conceptual level (i.e. strategic plan), at the logical level (i.e. process and method of work) and/or at the physical structure level (i.e. the action plan or the operational plan) (Segars and Grover 1996). This implies that the setting of the strategic plan at the corporate level and the setting of the action plan at the operational level may not be clearly defined and communicated to users due to the

inclusion of difficult or complex strategic terminology, and documentation may therefore be misinterpreted or difficult to interpret (Segars and Grover 1996). This can result into inflexible IT architectures and misalignment.

2.3 ICT Risk management

Several researchers have shown that ICT risk management must be practiced in an organized way in order to avoid and/or prevent risks (Dhillon & Backhouse 1996; Viator & Curtis 1998; Carnaghan 2006). Badenhorst and Eloff (1994, p. 411) suggest that the scope of a risk management process should be focused on risk identification, risk analysis, risk assessment (e.g. risk evaluation and risk allocation), risk resolution (e.g. risk decision, risk conclusion, risk financing, risk regulation and risk control) and risk monitoring (e.g. risk administration), Whereas Bandyopadhyay et al. (1999) highlight that the four major elements of ICT risk management process are risk identification, risk analysis, risk reduction measures and risk monitoring. According to them, all these need to be applied to the planning stage of system development and to continue throughout the development process'(Bandyopadhyay et al. 1999).

Risk identification must occur at the application level, the organizational level and the inter-organizational level (Bandyopadhyay et al. 1999, p. 438). Identifying risk at the application level accounts for the technical risk or implementation failure of ICT applications, including internal threats to ICT assets such as unauthorized physical access and system abuse, and external threats such as natural disasters, acts of competitors, hackers and computer viruses. Risk identification at the organizational level needs to account for the impact of ICT throughout all functional areas of the organization. Lastly, identifying risk at the inter-organizational level is primarily focused on external telecommunications; including electronic data interchange (EDI) when an organization places transactions online with suppliers, customers and distributors. How this identification of risk takes place relates to risk analysis processes that are integral to risk management. McEvoy and Whitcombe (2002, pp. 91-92) further add that risk identification is dependent on understanding the ICT environment in order to identify the information assets that the service must manage and to understand the physical architecture of the system within which this information is stored and manipulated.

Risk-reduction measures are defined as helping an organization prevent the occurrence of losses as a result of either the internal environment (i.e. data security, disgruntled employees, strategic risks) or the external environment (i.e. natural disasters, computer viruses and legal risk) (Bandyopadhyay et al. 1999). Badenhorst and Eloff (1994) argue that such measures rely on risk assessment (e.g. risk evaluation and risk allocation). Risk-reduction measures focus on investigating how ICT might help an organization deal with potential risk and developing a plan based on risk identification and risk analysis (clinch & Jim, 2009).

Once risks are identified and assessed, the right risk minimization strategy needs to be applied (Bojanc & Jerman-Blazic 2008). Such strategies include avoiding, reducing, transferring or even accepting to live with the risk if the benefits outweighs the cost of mitigation (Stoneburner et al. 2002). These four strategies are seen as minimizing the risks after an organization has performed a risk management process. Avoiding entails the elimination of the sources of risk, that is, the threats and attacks (Bojanc & Jerman-Blazic 2008). The reduction strategy engages appropriate technology or tool implementation or appropriate security policy adoption to mitigate an asset's exposure to risk (Bojanc & Jerman-Blazic 2008). Transferring is a strategy whereby an organization partially shifts its responsibilities to outsourcing security agents who take action on the identified risks (Bojanc & Jerman-Blazic 2008).

With the accepting strategy, an organization accepts the costs of risk retention embedded in the security measures, but still seeks to keep such risk under control (Bojanc & Jerman-Blazic 2008).

Risk monitoring is the last component which helps an organization ensures that potential risks are controlled and appropriate countermeasures put in place (Bandyopadhyay et al. 1999). It includes a continuous audit function that relates to a number of audit tools such as Computer Assisted Audit Tools and Techniques (CAATT), and monitoring tools such as tools for tracking websites (Bandyopadhyay et al. 1999, p. 443). Monitoring of risk has often led to the development of control measures.

2.4 IT Service Management

ITIL defines Service Management as "a set of specialized organizational capabilities for providing value to customer in the form of services" (ITIL Service Strategy: 15). In case of IT, the IT Service Management, or ITSM, is about maintaining a reliable, stable and cost-effective IT infrastructure to support business services and processes. This means that the IT department then moves from being a technology provider to a service provider (Pink Elephant. 2009: 3). Services depend on good management of IT assets in today's technology dependent world. The Information Technology Infrastructure Library (ITIL) was developed to provide a best practice framework for IT organizations to improve their IT Service Management. (Cartlidge, Alison et al. 2007: 6.)

2.5 Frameworks for ITSM

IT industry has developed some frameworks to manage their IT services. Organizations need to comprehend which framework will better manage their IT services, by considering the market and organization requirements (OCG SD, 2007).

Some firms constitute their own unique IT frameworks with attention to their organizational requirements, such as Microsoft Operations Framework (MOF) which is especially for Microsoft Corporation. Other firms use the predefined popular frameworks. Some of these are as discussed in the following sections.

2.5.1 COBIT Framework

The Control Objectives for Information and related Technology (COBIT) is acknowledged internationally as the ICT governance standard. The COBIT framework is also recognized as a top-down or high-level framework for governance, security and control over ICT (Khan 2006; Smith & McKeen 2006). The COBIT framework helps organizations align business processes with ICT processes as well as manage ICT-associated risks (Lainhart 2001a). The COBIT framework provides good practice across a domain and process framework and presents activities in a manageable and logical structure.

The process-oriented approach is presented in the COBIT framework as a reference process model that provides process details for everyone in an organization to adopt in order to manage ICT activities and ICT risks. The COBIT framework includes four domains as shown below.

Figure 2: The four interrelated domains of the COBIT framework

Plan and Organize
PO1 Define a Strategic IT Plan and direction
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Monitor and Evaluate
ME1 Monitor and Evaluate IT Processes
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance
ME4 Provide IT Governance

Acquire and Implement
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

Deliver and Support
DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

The four domains of the COBIT framework focus on the governing body and ICT management (Figure 2). This framework assists an organization to build ICT processes and controls which are appropriate for implementing and developing ICT governance and management (Smith & McKeen 2006). The four domains consist of 34 processes and 210 control objectives that help an organization define and follow its own approach to the management of ICT risks (ITGI 2007).

- **The plan and organize domain (PO):** This domain provides ICT strategy and tactics that help ICT achieve the optimal contribution to the business objectives (ITGI 2007). The ITGI (2007) classifies this domain into 10 processes in combination with 74 control objectives that provide guidance on structuring an organization. The ten processes are defined to ensure that business strategy, policies, procedures, processes and roles and responsibilities are determined by high-level management (ITGI 2007). In other words, people, process and organizational structure are all considered when planning how to deal with ICT risk.
  The acquire and implement domain (AI): This domain allows for the realization of ICT strategy based on the outcomes of the plan and organize domain to ensure that ICT solutions are identified, developed, acquired, implemented and integrated into the business processes in turn to achieve business objectives

(ITGI 2007, p. 13). The ITGI (2007) classifies this domain into seven processes in conjunction with 40 control objectives that provide guidance on maintaining and adapting existing organizational ICT systems. Seven processes are defined to assist in managing change, and whether the existing system or a new system could best deliver ICT solutions to meet business objectives (ITGI 2007). The control objectives for this domain are aimed at ensuring that all ICT investment or new ICT projects are acquired to meet the needs of current business operations (ITGI 2007). In other words, the planning of ICT infrastructure and systems is considered necessary for dealing with ICT risks.

- **The deliver and support domain (DS):** This domain enables the realization of service activities such as the delivery of required services, security management and continuity, service support for users, data management and operational facilities in order to meet the requirements of day-to-day ICT operations (ITGI 2007). The ITGI (2007) defines this domain according to 13 processes along with 71 control objectives to ensure that ICT service activities serve ICT operations to meet business objectives. This domain implies that an organization needs to consider which service activities best support ICT operations and control ICT processes to meet overall business operations.

- **The monitor and evaluate domain (ME):** This domain raises awareness of ICT quality assurance required by an organization to address performance management, monitoring of internal controls, regulations and governance (ITGI 2007). The ITGI (2007) categorizes this domain into four processes along with 25 control objectives to ensure that ICT performance is measured to detect problems before they occur, internal controls are effective and efficient, ICT performance can be linked back to business goals and can maintain confidentiality and integrity and availability controls are considered in terms of information security.

In summary, COBIT compiles an up-to-date international set of generally accepted control objectives for day-to-day use by business managers and IT managers. It addresses IT governance and the key performance indicators associated with process improvement and therefore provides a more global view of IT processes at the IT organization management principles than ITIL. The research will therefore borrow from this strength.

2.5.2   M_o_R Framework

The M_o_R is a Risk Management Framework proposed by Office of Government Commerce, 2010 for risk management and is based on four concepts.

- **Principle**: Essential to the development of good risk management; it is derived from corporate governance principles, which are based on corporate governance principles and ISO31000 guidelines;
- **Approach**: adaptation of the principles to suit the organization;
- **Process:** describes the inputs, outputs and activities involved in ensuring that risk is identified, assessed and controlled;
- **Embedding and Reviewing:** ensure that principles, approach and process are consistently applied across the organization and that their application undergoes continual improvement in order for them to be effective.

Figure 3*: M_o_R Framework.*
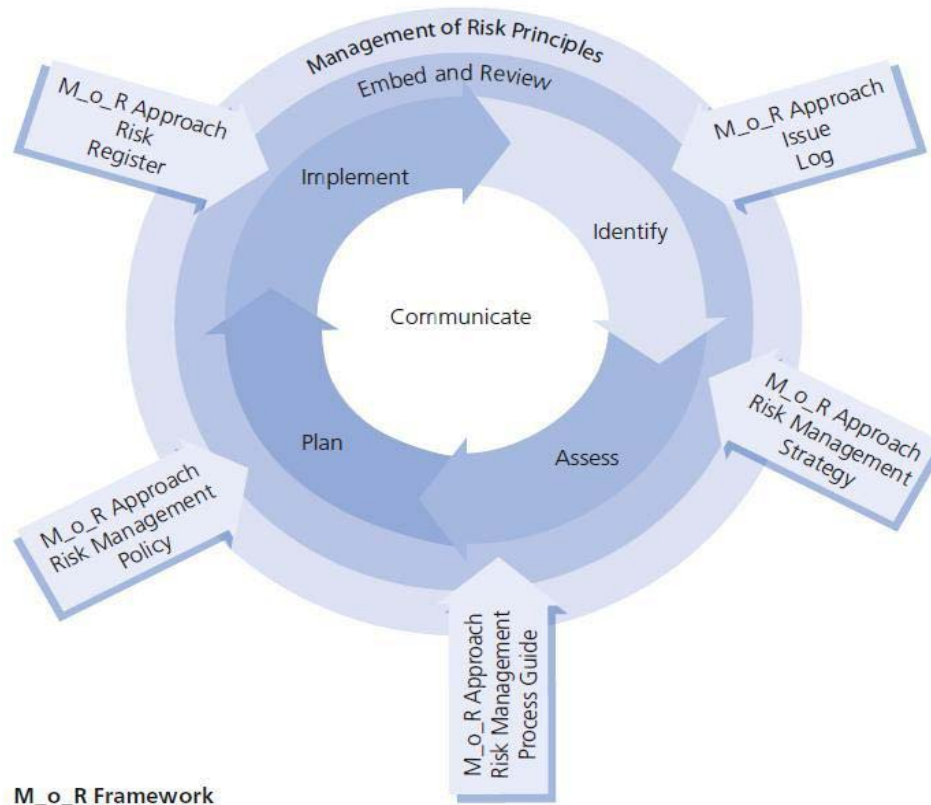
Source: OGC SS (2007). ITIL Service Strategy. 2nd ed. UK: TSO. 130

In summary, M_o_R is a route map for risk management, bringing together principles, an approach, a set of interrelated processes, and pointers to more detailed sources of advice on risk management techniques and specialism. It provides advice on how the principles, approach, and processes should be embedded, reviewed and applied differently depending on the nature of the objectives at risk. This will be a major borrowing into the research.

2.5.3 ITIL Framework

In response to the serious economic downtown in the late 1980s, the UK's Central Computer and Telecommunications Agency (CCTA) developed the IT Infrastructure Library framework to lower costs and to better manage IT service delivery (Salle, 2004). The ITIL framework is now administrated by the Office of Government Commerce and its best-practice processes are supported by the British Standards Institute's BS 15000 Standard for IT Service Management. A third version was released in July 2007 as an upgrade from version 2, published in 2000.

ITIL provides a comprehensive, consistent and coherent set of best practices for IT service management and related processes, promoting a quality approach for achieving business effectiveness and efficiency in the use of IS. ITIL service management processes are intended to underpin, but not dictate, the business processes of an organization. The generic processes described in ITIL promote best practice and may be used as a basis for achieving the British

standard for IT Service Management (BS 15000), which is currently being considered for fast-tracking to become an international standard-ISO/IEC 20000 (Massingham, 2010).

2.5.3. ITIL Structure

ITIL consists of five core publications: -

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Each publication is an individual volume intended to stand on its own, yet compliment the overall ITIL process.

Figure 4 - Elements of ITIL Service Lifecycle
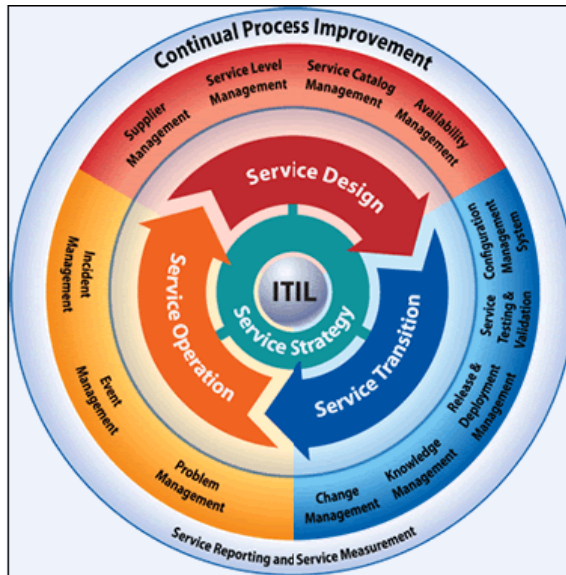
Source: http://www.hci-itil.com/ITIL_v3/references/ITIL_v3.htmlaccessed1st August, 2013

Figure 4 above demonstrates that ITIL Service Lifecycle uses a bicycle's hub and spoke design, with Service Strategy at the hub, Service Design, Transition and Operation as the revolving lifecycle stages, and anchored by Continual Service Improvement. Each part of the lifecycle exerts influence on the other and relies on the other for inputs and feedback. In this way, a constant set of checks and balances throughout the Service Lifecycle ensures that as business demand changes with business need, the services can adapt and respond effectively to inputs and feedback (The Official Introduction to the ITIL Service Lifecycle, 2007).

The full list of the specific processes under each ITIL main element is illustrated in figure 5.

Service Strategy - Service strategy provides guidance on how to design, develop, and implement ICT service management to create value for the recipient customer. There are four processes under service strategy namely; Demand Management, Financial Management, Strategy Generation and service portfolio management.

Service Design - Service design provides guidance on practical skills, tools and methods to achieve ICT Services that meet business objectives and demands for quality, reliability and flexibility. There are seven processes under service design namely; Service catalogue management, Service Level management, capacity management, availability management, Service continuity management, Information security management and supplier management.

Service Transition - Service Transition provides guidance on how to plan and manage ICT service changes and to deploy new ICT services into the production environment successfully. There are seven processes under service transition namely; Knowledge management, change management, Asset & configuration management, Release & deployment management, Transition planning and support, Service validation & testing, Service evaluation / Review

Service Operation - Service Operation provides guidance on how to coordinate, manage and support ongoing ICT Services at agreed levels to business users and customers. Service operation consists of ten processes which include incident management, problem management, event management, request fulfillment, access management, operations management, service desk, application management, Technical management and IT operations.

Continual Service Improvement - Continual Service Improvement (CSI) provides guidance on how to continually align and realign IT services to the changing business needs by identifying and implementing improvements to IT services that support business processes. CSI has three processes namely; Service measurement Service reporting and Service improvement.

2.5.4. Risk Management and ITIL

Risk management covers the following processes in ITIL

Problem management: there is a proactive and reactive management, with the goal of reducing the impact of service outages;

Change management*: Good change management techniques and approaches help reduce risks, minimize the potential negative impact of change, and reduce the risk of an undesirable outcome;

Service delivery*: Services must be maintained, so it is important to have a careful design;

Availability management*: Focuses on reliability and putting in place alternative options to ensure the service continues;

IT service continuity: Assessing risk to ensure overall continuity for the business.

Consistent, repeatable processes are the key to efficiency, effectiveness and the ability to improve services. These consistent, repeatable processes are outlined in the ITIL framework. As a result, ITIL provides several benefits to organizations, such as reduced process costs in the organization, improved IT services through the use of proven best practice processes, improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time, improved resource management and usage, improved decision making and optimized risk, improved productivity as well as improved use of skills and experience (Valarie & Arraj, 2010).

All these benefits are forcing the organizations to enroll in ITIL implementation in order to optimize their IT services and align them with business. However, sometimes all benefits come with limitations such as difficulty in implementing ITIL. As a generic framework ITIL does not have a guide on how to implement risk management.

Even though ITIL could reduce the cost of the operational process in the organization, it can be costly to implement. Another challenge is that it is difficult to estimate the ROI of ITIL implementation. Culture and behavior change may also be difficult to organization thus affecting the adaptation of the framework.

Although the academic community has been slow to research the phenomenon of multiple framework adoption, some consultants and vendors (such as Borland) have recognized the opportunity to reduce the complexity by providing services related to multiple frameworks. In addition, studies show that the combination of several frameworks empowers the organization (Cater et al 2006 & Valarie Arraj, 2010)

ITIL does not stand alone in providing guidance to IT managers and the Operation Service Book appendices outline some of the key supplementary frameworks, methodologies and approaches that are commonly used in conjunction with ITIL (OGC SO, 2007).For the existing processes, risk elements and their strategic response for all potential risks were identified. All ITIL processes must have Risk Management elements according to their purpose. Naturally some processes have stronger risk management elements than others, mainly processes that provide input to others (or rather providing a base for other processes).

2.6 ITIL versus other ITSM frameworks

Although there is a wide range of ICT control standards, frameworks and documents, the COBIT framework, as a model for ICT governance, is internationally recognized and applied widely in industry and commerce (Ridley et al. 2004; Buckby et al 2009). Elieson (2006) states that the COBIT framework is used as a baseline in ICT risk management to be mapped with other standards and frameworks to build a single, integrated body of knowledge. The COBIT framework also includes a range of guidelines relevant to different areas of the business including management guidelines, business function, control objectives, ICT governance implementation guidelines, control practices and ICT assurance guidelines (Lainhart 2001a; Ridley et al. 2004; ITGI 2007).

In terms of risk management, ICT processes and controls taken from the COBIT framework are focused on gaining control over risks. Therefore, all control objectives need to be discussed to determine which one is more applicable when dealing with specific ICT risks in an organization. The high-level control objectives have been examined more in the practitioner research literature than in the academic research literature in relation to ICT control (Ridley et al. 2004; Liu & Ridley 2005; Gerke & Ridley 2006).

M_o_R focuses on principles, approach and processes throughout the organization (William & Graham, 2009). This Framework is linked to other OGC Best Practices in terms of the roles, responsibilities and terminologies used outside the subject of project management. The main difference among the other risk frameworks is the fact that M_o_R emphasizes risks as being either **threats** (downside risks) or **opportunities** (upside risks). Despite M_o_R being referred to in ITIL Books, it is unclear if this is the official way to treat risk and level of IT governance. ITIL is strong in processes and explains the process flows (i.e. the way of doing the job).Although COBIT is composed of processes, it does not contain steps and tasks to realize processes (Buckby et al, 2009).It focuses on what the organization should do but do not explain how it should be done. On the contrary, ITIL defines how processes are achieved by giving flow charts (Rouse, 2009).

Furthermore, from the implementation point of view, ITIL is the easier standard to be implemented. These is because ITIL could be implemented in a phased approach whereas COBIT is quite difficult to implement partially since it should see a process in a bigger view first before they could be implemented partially (Ridley et al. 2004)

To sum up, ITIL is strong on delivery and support processes. It describes how to structure operational processes but is weak on risk management processes. Looking at these three frameworks therefore, it can be concluded that they do in fact complement each other: one can supplement the IT operational process strengths of ITIL with the critical success factors (CSF) and key performance indicators (KPI) of COBIT, and both can make good use of the risk management principles, approach and processes defined in M_o_R to develop a robust IT service management framework that incorporates Risk management.

2.7 ITIL Framework at the local Airline Industry

As part of her vision, one of the local airlines decided to implement the Information Technology Infrastructure Library (ITIL®) framework for the provision of its IT services. The aim was to align service delivery and service support to industry best practice, thus improving productivity and customer service, and reducing costs. The airline has gone through this journey beginning with TIL v2 and thereafter transitioning to ITIL v3 in 2010. Majority of the ITIL processes have been implemented though at different maturity levels and work is still going on to improve on the existing processes as well as adopt new ones. The ITIL processes map is illustrated below.

Figure 5: **V3 ITIL® Main Elements and Associated Processes**

Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Demand Management	Service Catalogue Management	Knowledge Management	Incident Management	Service Measurement
Financial Management	Service Level Management	Change Management	Problem Management	Service Reporting
Strategy Generation	Capacity Management	Asset & Configuration Management	Event Management	Service Improvement
Service Portfolio Management	Availability Management	Release & Deployment Management	Request Fulfillment	
	Service Continuity Management	Transition Planning & Support	Access Management	
	Information Security Management	Service Validation & Testing	Operations Management	
	Supplier Management	Evaluation	Service Desk, App Mngt, Tech Mngt, IT Operations	

Source: http://www.best-management-practice.com accessed 24 July 2013.

The details of each process in Figure 5 are documented in ITIL® publications with regard to principles, Process steps, roles and performance measures.

2.8   Conceptual framework

This framework has its foundation on the related work (examples include ITIL and Corporate Risk Management by Michael Faber and Rubina Faber, March 2010; Risk Management Model in ITIL by Sarah Villa – Real Vilarinho, June 2012), the experience of experts in this field and the researchers experience with ITIL framework. Its main approach is introducing new risk elements where they are not specified and reinforcing of ITIL risk management concepts on areas with deficiency.

Figure 6*: Conceptual framework*

Independent variable   Intervening Variable

Service strategy
- Strategy management
- Service Portfolio management
- IT financial management
- Demand management
- Business relation management
- Risk management

Service Design
- Service catalogue management
- Service management
- Capacity management
- Availabitlity management
- IT continuity management
- Supplier management
- Information management

Service Transition
- Transition Planning and support
- Change management
- Knowledge management
- Service assess and configuration management
- Release and deployment management
- Service testing & deployment
- Change evaluation

Service Operation
- Operation management
- Event management
- Incident management
- Request fulfilment
- Problem management
- Access mgnt

Continual Improvement
- 7 steps improvement service
- Service measurement
- Service reporting

Nature of Organization

- Diverse process
- Organizational structure
- Size of organization

Dependent variable

IT Infrastructure Library

■ (green) Risk management satisfactorily integrated

■ (blue) Risk management partially integrated

■ (red) Process without risk management

■ (yellow) New process integrated

Source: Research

2.9 Proposed ITIL Risk Management Strategy

ITIL provides several benefits to organizations, such as reduced process costs in the organization, improved IT services through the use of proven best practice processes, improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time, improved resource management and usage, improved

decision making and optimized risk, improved productivity as well as improved use of skills and experience (Valarie & Arraj, 2010).

2.9.1 Service strategy

Service Strategy process determines which services the IT organization offers and what capabilities need to be developed. The risk part is about the ability of the organization to limit its exposure to risk. The aim should be to make an accurate risk assessment in a given situation, and analyze the potential benefits.

Table 1: **Service Strategy Key Risk Indicators**

process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
Strategic management	Definition of unstructured or un-competitive strategy.	Percentage Decrease or Increase in customer's satisfaction levels.	Define and document organization's goals, important input from clients and external service providers in a, for instance, strategy plan. Create Strategic Action Plan defining specific tasks and responsibilities.	Research
Service portfolio management	Creation of a service that is not aligned with the organization 's strategy or organization/ customer.	Percentage Decrease/Increase in customer's satisfaction levels. Decrease/Increase of customer count. Number of systems where security requirements are not met.	Analyze the impacts on existing services and the creation of new services in the organization and determine the assets required to offer the service. Analyze risks in existing services and Create security benchmarks before embarking on requirements gathering for new services.	Research COBIT (Wim & Steven, 2005).
Demand Management	Inability to identify customer demands for services.	Number of services with good feedback. Decrease / Increase of customer count.	Study customer needs (surveys, questionnaires, observation).	Research
Financial management	Plan Incorrect Budget.	Degree of Variance between actual spent and approved budget.	Accurate forecasting, priority setting, cost control and monitoring mechanism. (Create documentation)	Research
Risk Management	Inability to indentify and manage risk at all levels (strategic, Tactical and operational)	Trend analysis on the cost as a result of poor decision making or unguided actions Number of risk gaps indentified only after the disaster.	Improved corporate decision making through the effective communication of risk exposure throughout the organization; An open and supportive approach to the identification, analysis and communication of risk as well as Better awareness in all personnel of the cost and benefit implications of their actions.	M_o_R (Douw & Mark , 2010).

Source: Research

2.9.2 Service design

The scope of Service Design includes the design and development of new services as well as changes and improvements to existing ones. It covers design principles and methods for converting strategic objectives into services and service assets. There are a number of risks directly associated to the Service Design phase of the Service lifecycle. These risks need to be identified, assessed, planned and implemented to ensure that they receive proper treatment.

Table 2: **Service Design Key Risk Indicators**

Process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
Supplier management	Expensive but poor services No value for money	Number of agreed UCs in relation to the actual services. Number of contract reviews per period. Number of suppliers (in DB) with complete information about them.	Create Supplier and Contract Management database/System. The database/system should capture complete information of the agreement(s)	Research
Information Management	Lack of appropriate information on future plans and strategies.	Gaps in Disaster Plan(s). Time lapse from identification of risk to the implementation of a suitable continuity mechanism. Number of identified gaps during Disaster plan simulations.	Register and document the main business requirements. Get sponsor buy-in (Analysis and supporting documents) Create a Business Continuity Strategy Create Disaster Recovery plan and Invocation Guideline.	Research
Availability Management	Systems unavailability	Number of Denial of service attacks	Implement the minimum security benchmarks in all systems	COBIT (Wim & Steven, 2005).

Source: Research

2.9.3 Service Transition

The objective of ITIL Service Transition is to build and deploy IT services. Service Transition also makes sure that changes to services and Service Management processes are carried out in a coordinated way while controlling the risks of failure and disruption. Associated to this model, there are some risk elements that have already been identified and addressed by ITIL.

Table 3: **Service Transition Key Risk Indicators**

Process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
Knowledge management	Inability to gather pertinent knowledge for organization.	Percentage of complete documentation vis a vis in-complete or non-existent Documentation. Frequency of training. Frequency of knowledge updates.	Create a Service Knowledge Management System (SKMS). SKMS is a central repository of the data; information and knowledge that the IT organization needs to manage the lifecycle of its services.	Research
Evaluation Management	Developing standard performance measures and measurement methods across projects and suppliers.	Number of performance measures created. Number of performance measures documented.	Create the Change Evaluation Report. Change evaluations may be used at different points in a change's lifecycle, for example before authorizing the Change/Release build or during the Post Implementation Review.	Research

Source: Research

2.9.4 Service Operation

The objective of ITIL Service Operation is to make sure that IT services are delivered effectively and efficiently. This includes fulfilling user requests, resolving service failures, and fixing problems as well as carrying out routine operational tasks. The risk management on this module is around organization routine and focuses on delivering and supporting all services. The risk management elements on this module are to monitor services, identify risks and make sure they do not materialize.

Table 4: Service Operation Key Risk Indicators

Process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
Access management	Unable to restrict access rights to unauthorized users.	Number of access attempts. Number of authorized access attempts. Number of unauthorized access attempts.	Always keep users matrix database updated. Implement an access control system Give access rights according the roles in the organization.	Research
Operations Management	Weak security features in systems	Number of security / vulnerability tests in a given period	Create and document vulnerability test schedule and implement Audit compliance to the vulnerability tests schedule	COBIT (Wim & Steven, 2005).
Incident management	Increase in number of incidents as a result of un-authorized access	Percentage increase in Number of incidents as a result of un-authorized access	Implement proper incident categorization and review the reports periodically	COBIT (Wim & Steven, 2005).

Source: Research

2.9.5   Continual Service Improvement.

The Continual Service Improvement (CSI) process uses methods from quality management in order to learn from past successes and failures. The CSI process aims to continually improve the effectiveness and efficiency of IT processes and services in line with the concept of continual improvement adopted in ISO 20000. For this, it is vital to integrate risk management into the culture of the organization, and to explain how this can be achieved and highlight the need for regular review.

While Risk Management in design and transition stages must organize concepts and mainly identify risks of the service lifecycle, a good CSI program will assess the results of Risk Management activities to identify service improvements. This can be done through risk mitigation, elimination and management as well as by regularly reviewing the goals to be achieved in order to ensure risk management is being appropriately and successfully handled across the organization. For this, it is important to embed risk management into the organization's culture and put mechanisms in place to review and confirm that the approach to risk management remains appropriate given the organization's objectives and context.

Table 5: **Continual Service Improvement Key Risk Indicators**

Process	Potential Risk	Key Risk Indicator (Measurable)	Strategic Response	Source
7-Step Improvement service	Services became static throughout time.	Service evolution rate. Percentage of new services.	Implement the seven steps improvement process, according to the organization	Research
Service Reporting	Inability to sustain continuous reporting.	Percentage of organization goals tracked/reported.	Simple, effective, customizable and automated reporting.	Research
Service measurement	Inability to Identify un-necessary measurements.	Number of defined metrics.	Have Different levels of measurement and reporting.	Research

Source: Research

2.9.6 Risk management integration in ITIL

The research therefore recommends a process that will identify, analyze, assess, control and monitor risks within the ITIL framework. This includes determining the value of ICT assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats with clear mitigation and monitoring mechanism. Risks are addressed within several processes in ITIL but, there is no process dedicated to the Risk Management. ITIL calls for "coordinated risk assessment exercises" and it would be natural to assign clear roles and responsibilities for managing risks, which would mean introducing a specific Risk Management process as part of the ITIL processes while mitigating the negative effects of organizational structure and culture.

The structure of an organization can be regarded as a framework for getting things done. It consists of the units, functions, divisions, departments and formally constituted work teams into which activities related to particular processes, projects, products, markets, customers, geographical areas or professional disciplines are grouped together. Kenya airway has a matrix organizational structure with ICT department solely responsible for spearheading ITIL implementation in the entire organization. The success of this would depend on the sequence and interaction with all the other processes.

Although system fit amongst all the elements, congruence among these specific design factors is often critical for organizational success. Each organization contains within it different types of work, from management to manual labor. The nature of each type of work must be clearly defined in order to be efficient and allow for change management.

The level of technology employed by the organization in areas such as information systems, communication, data storage and collection, internet, local area networks and computers, has a significant effect on the effectiveness of the organization. Obviously, increased technology usually requires increased financial and time investments, which some organizations simply cannot afford. Other organizations choose not to upgrade their technology because they feel they are accomplishing the mission of their organization with their current technology. (Simmons & White, 1999). That is why an organization may consider to identify and mitigate risks gaps in ITIL rather than introducing a totally new framework that will eventually turn out to be costly to the organization.

Structure describes the organizational hierarchy, or lack thereof, of the organization. It also describes the people and their integrating roles, as well as any matrices of sub-organizations that occur within the overall system. Structure also answers the question: Are there task forces and/or special networks involved in the organization? (Buttle, 1997). Organizational structure determines how the roles, power and responsibilities are assigned, controlled, and coordinated, and how information flows between the different levels of management.

Nature of an organization is characterized by the organization's objectives and strategy. In a centralized structure, the top layer of management has most of the decision making power and has tight control over departments and divisions. In a decentralized structure, the decision making power is distributed and the departments and divisions may have different degrees of independence. The structure indicates who is accountable for directing, coordinating and carrying these activities and defines a management hierarchy (the chain of command) that is responsible to whom for what at each level in the organization.

The organizational structure therefore facilitates strategy implementation, facilitates communication and allocates tasks and responsibilities and this makes any implementation process easier.

Organizations have an option of adopting the behavior system leverage points to drive and sustain change during and after the ITIL implementation. Leverage is the ratio of change in output to change in input. A leverage point is a place in a system where force can be applied. A low leverage point is a place in a system where a small amount of force causes a small change to system behavior. A high leverage point is a place in a system where a small amount of change force (the effort required to prepare and make a change) causes a large amount of predictable, favorable response.

Leverage = change in Output / Change in Input

Figure 7: System Leverage Points

Source: James P. Womack & Daniel T. Jones: 2010. 29

22

The focus on the 6 system leverage levers would enable the organization to institutionalize change because they drive behavior of the employees. The levers are both enablers of change if they are in place and barriers to change if not in place.

- **Vision** – This is the cog that turns the rest. The shared vision of the change will make sure that everybody knows what the vision is and can see the processes from end – to – end.
- **Accountability** - If an organization does not hold people accountable for their actions and behavior, any agreement to change would be discounted and no change would occur.
- **Right People** – Making sure that all the right players are involved from the start would make or break the change initiative.
- **Skills Development** – People who are changing to a new way need training, and tools to build the right skills. Without the knowledge they would not be able to change.
- **Reward and Recognition** – The organizations actions should be consistent with what they say or the change they are promoting. Any misalignment in the behavior and reward and recognition would impede the change.
- **Metrics, Policies and Processes** – This cog represent how the organization is designed. Metrics drive behavior and these factors must be aligned for change to happen.
- **Communication** – This is the cornerstone of all the levers. Any system is dynamic and the level of communication is directly proportional to how efficiently the system is running.

2.10 Chapter Summary

The chapter mentioned other frameworks used to implements different aspect of IT. Special focus was given to COBIT and M_o_R frameworks where their strengths and weaknesses of each were examined. The research borrowed from the strengths of these two frameworks to improve the current ITIL service delivery framework to incorporate Risk Management. The chapter provided an improved conceptual framework and outlined an ITIL risk management strategy with measurable Key Risk Indicators.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology that was used. This includes the research design, target population, sampling technique, data collection methods and data analysis and presentation methods.

3.2 Research Design

An exploratory research method was adopted in this research. This method allows a researcher to explore a particular phenomenon or circumstance (such as ICT risk management in an organization) in order to provide sufficient information to design, develop and execute the next research steps. In addition, a mixed mode approach was adopted as there were multiple objectives to this research. Quantitative and qualitative research approaches supplement each other to produce a mixed mode research approach. The qualitative research provided in-depth explanations, respondent's experiences, opinion and knowledge while the quantitative research approach provided statistical data. Both techniques were used to draw from their strengths and minimize the weaknesses of quantitative and qualitative research approaches hence increase validity and reliability of the data collected.

Figure 8: **Research Execution Plan**
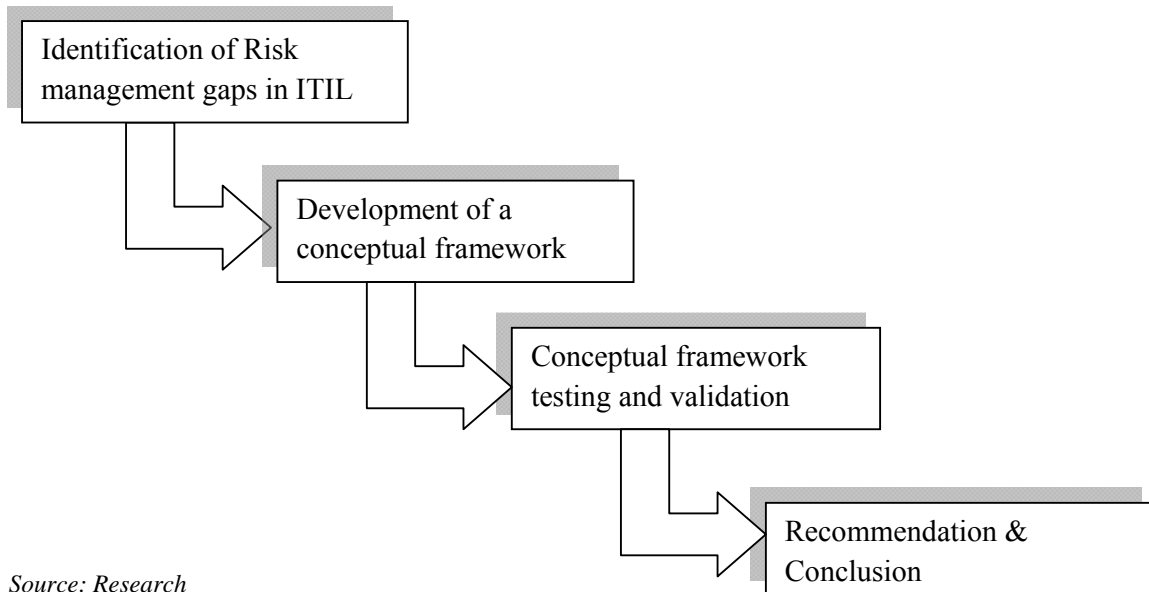
Source: Research

Identification of gaps within the ITIL framework entailed reference to other related studies; seeking opinion from subject expert as well banking on the researchers experience on the ITIL implementation process at a local airline. The Experts' opinion was gathered through research articles/publications, questionnaires and results of focus groups. The focus groups were chosen depending on their ability to articulate their opinion on the subject, work experience and availability. ITIL experts Information obtained helped the researcher formulate the conceptual framework in which the various variables were determined and a questionnaire developed accordingly. Data collected was analyzed and shared with subject matter experts for validation purposes before conclusion and recommendations were drawn. The subject experts were drawn from a local airline employees holding ITIL Expert Certification and are practicing ITIL in their day-to-day work. The results were adopted in selected sections of the organizations in order to test the robustness of the risk integrated framework.

3.3 Target Population

The target population of this research comprised of employees from all cadres in the Information Systems (IS) department at a local airline. The airlines' IS department has a total of 150 employees based at the Headquarters in Nairobi. These employees include senior managers (Director, HOD's), middle managers (Function/Line managers, Systems Analysts and Business Analysts) and non-management staff (System Administrators and support Engineers) who are currently working in the organization.

3.4 Sampling procedure

The research used a two-stage sampling procedure. Stratified sampling technique was used to identify ICT staff of different cadre's namely senior managers, middle managers and non-management staff.

On risk management in ITIL at The local airline, senior management staff were selected for the reasons that they are able to offer insight into perceptions of the top-down approach in each case because they have the ability to enrich and take charge of ICT risk management in the context of a range of processes regarding ICT governance. Support staff was also used in this research to enrich the information obtained on management strategies in relation to the bottom-up approach regarding risk management in ITIL. Simple random samples were taken proportionately from each stratum in order to select respondents out a population of 150 IS staff. Simple random sampling assisted to minimize bias when dealing with the population sample.

3.5 Sample Size

Yamane (1987) provides a simplified formula to calculate sample sizes which is as follows,

$$n = \frac{N}{1 + N(e)^2}$$

Where n is the sample size, N is the population size, and e is the level of precision (sampling error)

The minimum sample size that could be used in this research for a population (N) of 150 people at 95% confidence and with the degree of variability (P) at 0.5 was calculated as follows;

$$n = \frac{150}{1 + 150(0.05)^2}$$

$$n = \frac{150}{1.375}$$

$$n = 109$$

This implied that the sample size had to be at least 109 participants. A sample of 110 participants was purposively selected because of the fact that the experience of the participants was imperative, and that in this way rich information about integrating risk management in ITIL at the local airline would be obtained.

Table 6: Sample size

Strata	Target Population	Sample size	Percentage (%)
Senior Managers	20	15	14
Line managers	34	25	23
Support staff	96	70	63
Total	150	110	100

Source: Research

3.6 Research variables

ITIL is a framework based on service Lifecycle. A successful ITIL framework is dependent on these services namely strategy, design, transition, operation and continuous improvement. Various processes constitute these services and it is the repeatability, consistency of this process that determines the ability to improve these services (OGC SS, 2007).

3.6.1 Dependent Variables

Successful implementation of ITIL to at least Maturity level 3 is of primary interest to the local airline and was therefore considered as the dependent variable.

3.6.2 Independent Variable

The five independent variables that were considered in this research were:-

- Service Strategy,
- Service Design,
- Service Transition,
- Service Operation
- Continuous Service Improvement.

Precisely the research looked at how risk management is incorporated in processes within these services and how integration of risk management process would ultimately affect the existing ITIL framework.

3.6.3 Intervening Variable

Organizations vary in their size, type of processes undertaken and the organizational culture. How these factors affect ITIL implementation in an organization was considered in this research.

3.7 Methods of Data Collection

A tool kit comprising of a questionnaire and focus group discussion guide was used since they were considered the best tools for this type of research.

3.7.1. Questionnaire

The questionnaire was prepared based on an extensive review of the literature on implementation of ITIL. The questionnaire consisted of questions covering the risk management aspects in the context of ITIL implementation.

Pilot testing of questionnaires was carried out on 10% of the research population and necessary adjustments made accordingly. Some of the key improvements noted were:-

- The needs to include a comments section to allow the respondents give comments/justification for the score given on question regarding their opinion to particular questions.
- Dropping of the age and gender questions as these were not going to give any significant input to the research.

The improved questionnaire is attached on Appendix 1.

Questionnaires were distributed to non-management, senior and middle management staff at the local airline. The questionnaires were structured to allow both open-ended and close-ended questions. To enrich this information, an independent observation of processes and data from the IT service management tool was also used.

3.7.2.   Validity and reliability of the instrument

Measurement validity is the degree to which a measure does what it is intended to do. This means that the measure should provide a good degree of fit between the conceptual and operational definitions of the construct, and that the instrument should be usable for the particular purposes for which it was designed (Blanche & Durrheim, 2009:83). Sarantakos (1994) asserted that validity is a methodological element for qualitative and quantitative research. It is the correlation between data and conclusion. Validity will be ascertained by comparing qualitative and quantitative data and see whether they corroborate one another.

Reliability refers to the dependability of a measurement instrument, that is, the extent to which the instrument yields the same results on repeated trials (Blanche & Durrheim, 2002:88). In other words, reliability relates to matters such as the consistency of the measure (Wilkinson, 2000:42).

On the validity of instruments, a pilot research to appraise soundness of the items and to estimate time required to answer the questions was carried out. The pilot research covered 10 members in the sample population. The results of the pilot research were discussed with the respondents and adjustments made accordingly.

Haeri (2005) considers the reliability of the instruments to be the degree of consistency of the instruments or procedures. The reliability of a standardized test is usually expressed as a correlation coefficient, which measures the strength of association between variables. Such coefficient vary between 0.00 and 1.00 with the former showing there is perfect reliability which is an ideal situation.

Reliability was ascertained by splitting the instruments into two: placing all odd numbered in one sub-set and all even numbered items in another subset and then finding the coefficient of internal consistency.

Formula for calculating reliability coefficient is as follows;

$$r_{kR\ 20} = \left(\frac{k}{k-1} \right)\left(1 - \frac{\sum pq}{\sigma^2} \right)$$

Where

$r_{kR\ 20}$ is the Kuder- Richardson formula20

k   is the total number of test items

Σ   indicates to sum

p is the proportion of the test takers who pass an item

q is the proportion of test takers who fail an item

σ is the variation of the entire test

In research, 10 questionnaires (instruments) were used in the pilot study which means that k =10. Next the value of p for each item was calculated; the proportion of the sample who answered each item correctly (the value p) and the proportion of those who did not respond to the questions correctly (the value q) were calculated. Since the respondents either got or missed each question, the sum p+q=1. The proportion of a whole sample is always 1. Values of p and q obtained were as follows:-

Table 7: Reliability Co-efficient

p	0.40	0.53	0.80	0.80	0.47	0.73	0.67	0.67	0.80	0.73
q	0.60	0.47	0.20	0.20	0.53	0.27	0.33	0.33	0.20	0.27
Pq	0.24	0.25	0.16	0.16	0.25	0.20	0.22	0.22	0.16	0.20

The standard deviation and the variance from the resultant values were calculated as follows:-

$$\sigma = \sqrt{\frac{\sum (x - \mu)^2}{N}} = 2.36$$

$$\Rightarrow \sigma^2 = (2.36)^2 = 5.57$$

The standard deviation therefore was 2.36 and the variance was 5.57.

Substituting all values in the formula we get;

$$r_{kR\,20} = \left(\frac{10}{10-1}\right)\left(1 - \frac{\sum 2.05}{5.57}\right)$$

$$r_{kR\,20} = 0.70$$

The reliability coefficient obtained of 0.700 implied that the research instrument have a reliability of 70 % which is acceptable.

Correlation coefficient measures the strength of association between two variables, in this case p and q. This was calculated using the formula for calculating correlation coefficient of a sample denoted by *r* as follows;

$$r = \frac{\sum (pq)}{\sqrt{[(p^2)x(q^2)]}} \ldots\ldots\ldots\ldots\ldots(i)$$

Where *p*= p$_i$ - p   and n *q* = q$_i$- q

From the table 7, the values of x and y were derived as follows;

Table 8: Correlation co-efficient

p	0.40	0.53	0.80	0.80	0.47	0.73	0.67	0.67	0.80	0.73
$p=(p-\bar{p})$	-0.26	-0.13	0.14	0.14	-0.19	0.07	0.01	0.01	0.14	0.07
q	0.60	0.47	0.20	0.20	0.53	0.27	0.33	0.33	0.20	0.27
$q=(q-\bar{q})$	-0.28	0.34	-0.14	-0.14	0.19	-0.07	-0.01	-0.01	-0.14	-0.07
p^2	0.07	0.12	0.02	0.02	0.04	0.01	0.00	0.00	0.02	0.01
q^2	0.08	0.12	0.02	0.02	0.04	0.01	0.00	0.00	0.02	0.01

Substituting the values of p and q in equation (i) we get

$$r = \frac{0.012}{0.31 \times 0.63} = 0.65$$

The value 0.65 lies between -1 and 1 and signifies a positive linear correlation between the value of *p* and that of *q*. This implied that the two sets of instruments being tested had a positive correlation (strong) hence reliable.

For validating the research findings, email communication between the interviewer and interviewees was maintained. The informants came together in a focus group for approximately 60 minutes. All focus group's responses were digitally recorded and transcribed.

3.8   Focus Group Discussions

A focus group provides an opportunity for participants to explore their own experiences of phenomena with others. Morgan (2008) argues that the effective focus group structure is highly related to the degree of control by the moderator. He claims that two elements determined the group effectiveness. First, the relevance of questions asked to the topics discussed; second, how the participants' interactions are managed.

The focus group is a popular research approach in both IS research (Myers 2009) and managerial research (Iden 2009). The purpose of a focus group is not to reach an agreement, rather to observe a wide range of ideas or feelings that people have about phenomena (Kitzinger 1995; Myers 2009; Neuman, 2011). This data gathering methodology was also used to get a practitioners view of how risk management can be integrated into ITIL framework.

Six focus groups each consisting of five participants were utilized in this research. The focus groups were drawn from IS staff stationed at various divisions of the local airline; namely Information Systems, Finance &HR, ,Ground Operations & Cargo, Flight Operations, Commercial and Technical. There was only one focus discussion group per division and the members were selected randomly. The basis of the discussions was purely guided by the questionnaire and research questions. Pilot research was conducted by a sample group comprised of two members from each division. Recommendations from the pilot research were factored when coming up with the final questionnaire. The participants met for 1 hour bi-weekly for a period of three weeks after which a report was compiled. The reports were analyzed, compared and a summary generated. The focus group guide used is attached on Appendix 2.

3.9   Data Analysis

At the base of the analysis were the research questions. Different data analysis methods were used for the different data collected. Quantitative data that was collected using semi structured questionnaires and data from the IT service management system was analyzed using SPSS statistical software. Measures of central tendency such as

mean, median, mode and standard deviation were used to analyze quantitative data obtained. Prior to the analysis, a codebook for the various quantitative variables was prepared. The code book was based on the numbering system of the questionnaires. This was significant in isolating the quantitative data from the qualitative data from each of the structured questionnaires. For qualitative data, which was mainly gathered from the management staff's in-depth interviews and to a lesser extent from the open-ended questions in the questionnaires, the interview notes were first transcribed and trends in the data noted. Qualitative data was analyzed using frequency tables and percentages.

Quantitative and qualitative research approaches complement each other to produce a mixed mode research approach. The qualitative research provided in-depth explanations, respondent's experiences, opinion and knowledge while the quantitative research approach provided statistical data. In this regard, a comparative analysis of the quantitative and qualitative results was carried out and a casual relationship drawn. This helped in showing the degree of relationship between the variables.

3.10 Chapter Summary

The chapter focuses mainly on the research methodology. Both Quantitative and qualitative research approaches were used to supplement each other to produce a mixed mode research approach. The research design, population and sampling techniques were discussed. The main method of data collection was highlighted as questionnaires, Data from the service management tool, focused group discussions, and targeted interviews, as well as independent observation of processes. Finally the chapter discussed the analysis methods. Quantitative data was analyzed using SPSS statistical software and represented in central tendency measures such as mean, median, mode and standard deviation. For qualitative data, the interview notes were first transcribed and trends in the data noted and analyzed using frequency tables and percentages.

4.1 Introduction

This chapter presents the analysis, findings and interpretations of the data collected. The research was conducted on a sample of 110 respondents drawn from employees in all cadres in the Information Systems (IS) department of a local airline to which questionnaires were administered. However, out of the issued questionnaires, 86 were returned duly filled thus making a response rate of 78%, which was sufficient for statistical reporting.

To guarantee quality of the samples, the reliability of the research instruments was tested and resulted to a reliability of 70 % which is acceptable

4.2 ITIL Framework Implementation Steps in a local Airline

The research sought to ascertain the information that relate to employees and their organizations experience while adopting and implementing ITIL framework. This information points at the respondents' suitability to participate in the research. Details are presented below.

4.2.1 Respondents' Position in the Airline.

The research requested the respondents to state their position in the airline. Table 9 presents the findings.

Table 9: Respondents' Position in the Airline.

Positions	Frequency	Percent
Senior manager	10	11.6
Line managers	18	20.9
Support staff	58	67.5
Total	**86**	**100.0**

Source: Research

From the findings, 11.6% of the respondents were senior managers 20.9% line managers, 67.5% support staff. The findings indicate that majority of the respondents were support staff. This is important because whereas the senior managers would give insight to the research based on their experience, the support staffs are the ones who are actively involved in operationalizing the ITIL framework on a day-to-day basis and therefore their input was key in the research.

4.2.2 Respondents' Stationed Division

The research requested the respondents to state the division in which they were stationed in the airline. Findings are presented in table 10.

Table 10: Respondents' Stationed Division

Divisions	Frequency	Percent
Information Systems	31	36.0
Finance & HR	7	8.1
Ground Operations & Cargo	8	9.3
Flight Operations	16	18.6
Commercial	8	9.3
Technical	16	18.6
Total	**86**	**100.0**

Source: Research

From table 10 above, majority of the respondents (36%) indicated that they were stationed in Information Systems division, 18.6% in flight operations division, 18.6% in technical division, 9.3% in ground operations & cargo division, 9.3% in commercial division and 8.1% in finance and HR division. The findings indicate that most of the employees in the airlines' IS department, were stationed within the information systems division. It is within the IS department that IT related frameworks are adopted and implement and the IS personnel would be best suited to participate in the research to discuss the level of risk integration into the ITIL frame work.

4.2.3 The Airlines Effort to Implement ITIL Framework

The research asked the respondents to state if they were aware of the airlines effort to implement ITIL framework. Findings are presented in Table 11.

Table 11: The Airlines Effort to Implement ITIL Framework

	Frequency	Percent
Yes	86	100.0

Source: Research

From the findings, all the respondents were aware about the airlines effort to implement ITIL framework. This indicates that communication in the airline is effective and since all the employees are aware of the implementation process, implementation was bound to be effective and successful thereby supporting the success of this research.

4.2.4 Employee Involvement in ITIL Implementation.

The research requested the respondents who were aware of the airlines effort to implement ITIL framework. Since all the respondents were aware, all of them responded to this question. Findings are presented in table 12.

Table 12: Employee Involvement in ITIL Implementation

	Frequency	Percent
Yes	86	100.0

Source: Research

From the findings, all the respondents stated that they had been involved in the implementation process. The findings indicate that the airline involved all of its employees in implementing ITIL framework which was key to the success of the implementation and by extension the success of the research.

4.2.5 Respondents' Duration of involvement in ITIL framework Implementation

The research requested the respondents to state the period over which they had been involved in the implementation of ITIL framework. Table 13 presents the findings.

Table 13: Respondents' Duration of ITIL framework Implementation

Duration	Frequency	Percent
1-2 years	31	36.0
3-4 years	16	18.6
More than 4 years	39	45.4
Total	**86**	**100.0**

Source: Research

From the findings, majority of the respondents (45.4%) stated that they had been involved in the implementation of ITIL framework for more than 4 years, 36% for 1 – 2 years and 18.6% for 3 – 4 years. The findings indicate that majority of the employees had been involved in the ITIL framework implementation process for more than 4 years hence they were conversant with the framework meaning that they would give invaluable input into the research..

4.2.6 Ways of Involvement in ITIL Implementation Process

The research requested the respondents to indicate the way(s) in which they were involved in the ITIL implementation process. Table 14 presents the findings.

Table 14: Ways of Involvement in ITIL implementation Process

	Frequency	Percent
Decision making (Management)	16	18.6
Design	23	26.7
Training	31	36.0
Sensitization/Awareness	16	18.6
Total	**86**	**100.0**

Source: Research

From the findings, majority of the respondents (36%) indicated that they had been involved in the training process, 26.7% in the design process, 18.6% in the decision making (management) stage and while other 18.6% in the sensitization/awareness stage. The findings indicate that most of the employees in the airline had been involved in ITIL Framework implementation process at the training level. This was followed closely by 26.7% of the respondents who were involved in the design process. These statistics were key to the research because they confirmed that majority of the respondents were subject matter experts and that the framework was well implemented. The respondents would also give invaluable information in regards to any gaps within ITIL framework.

4.2.7   Level of agreement with ITIL Framework Statements.

The research in this category requested the respondents to rate the degree to which they agreed/disagreed with the various statements concerning ITIL framework. Respondents were given a scale of strongly disagree, disagree, neutral, agree and strongly agree. Findings are presented using means and standard deviations in table 15.

Table 15: Level of Agreement with ITIL Framework Statements

Statement	Mean	Std. Deviation
ITIL led to improved IT services through the use of proven best practice processes at the airline	4.45	0.501
ITIL led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time at the airline	4.36	0.483
ITIL led to improved resource management and usage, improved decision making and optimized risk management at the airline	3.80	0.570
ITIL led to improved productivity as well as improved use of skills and experience at the airline.	3.80	0.838
ITIL adoption led to an improved risk management practice.	2.90	0.882
It is unclear if there is a standard way to treat risk and how to implement risk management framework process in ITIL	3.40	1.151
ITIL risk management should be mapped with other standards and frameworks to build a single, integrated body of work.	3.45	1.155
It is not advisable to adopt multiple frame works as they are costly and complex to implement.	4.09	0.523

Source: Research

From the findings in table 15, majority of the respondents were in agreement that ITIL had led to improved IT services through the use of proven best practice processes at the airline. This had a mean score of 4.45. Respondents were also in agreement with a mean score of 4.36 that ITIL has led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time. Many respondents disagreed with the statement that ITIL adoption has led to an improved risk management practice since this scored the lowest mean of 2.9. Also few respondents agreed that it is unclear if there is a standard way to treat risk and how to implement risk management process in ITIL. This had a mean score of 3.4. The findings indicate that ITIL has led to improved IT services through the use of proven best practice processes at the airline and also ITIL has led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time. The findings also confirmed the initial problem statement that ITIL is weak in risk management.

4.3 Degree of ITIL Framework Implementation at the local airline.

The research in this section sought information about the degree of ITIL framework implementation at the local airline. Respondents were asked to state the degree to which various items had been implemented as part of ITIL implementation process. Respondents were given a scale of 1 to 5 where 1 = Minor, 2 = Moderate, 3 = Don't know, 4 = Large and 5 = Very large. Findings are presented in table 16.

Table 16: Degree of ITIL Framework Implementation at the airline

Item implemented	Mean	Std. Deviation
Service strategy	3.35	0.779
Service Design	2.98	0.854
Service transition	3.07	1.396
Service operation	4.47	0.502
Service continual improvement	4.08	0.800

Source: Research

From the findings, majority of the respondents agreed that service operation had been implemented to a large extent. This had a mean score of 4.47. Those who agreed that service continual improvement had been implemented to a large extent had a mean score of 4.08, service strategy with a mean score of 3.35, service transition with a mean score of 3.07 while service design scored a mean of 2.98. The findings indicate that service operation and service continual improvement had been implemented to a large extent at the airline. In summary the results in table 16 showed that all the ITIL modules had been implemented at least to a moderate degree which would mean increased reliability of the research findings.

4.4 Degree of Integration of Risk Management into ITIL Framework at the local airline

The research in this section sought expert opinion on the degree of integration of risk management into ITIL framework using a scale of 1 to 5 as defined in section 4.3. The question that was asked to the respondents was "To what degree has risk management been integrated in ITIL processes listed in table below?" Findings are presented in table 17.

Table 17: Degree of Integration of Risk Management into ITIL Framework

Process	Mean	Std. Deviation
Strategy Management	2.07	1.064
Service Portfolio management	1.90	1.074
IT financial management	1.90	0.882
Demand management	2.27	1.067
Business Relations Management	2.85	1.070
Service catalogue Management	2.98	1.067
Service level management	4.00	0.434
Capacity management	3.90	0.797
Availability management	4.08	0.800
IT continuity management	3.80	0.838
Supplier management	3.35	0.763
Information management	3.63	0.882
Transition planning and support	3.08	0.800
Change management	4.27	0.873
Knowledge management	3.09	0.523
Service assets and configuration management	3.62	0.883
Release and deployment management	4.00	0.434
Service Testing and deployment	2.45	1.233
Change evaluation	4.08	0.514
Operation Management	4.07	0.801
Event management	4.09	0.523
Incident management	4.44	0.902
Request fulfillment	4.35	0.891
Problem Management	3.09	0.801
Access management	4.09	0.903
7 step improvement service	3.85	1.023
Service measurement	4.53	0.663
Service reporting	4.29	0.944

Source: Research

From the findings, majority of the respondents were in agreement that risk management has been integrated into the service measurement process to a large extent. This is seen with a mean score of 4.53. Respondents who felt that risk management had been integrated into incident management process scored a mean of 4.44 with others on request fulfillment process, service reporting process, change management process, event management process, access management process, availability management process and change evaluation scoring a mean of 4.35, 4.29, 4.27, 4.09, 4.09, 4.08 and 4.08 respectively.

The processes that had low mean scores indicating that risk integration had not been done to a large extent were IT financial management process, service portfolio management process, demand management process and service catalogue process having scored 1.9, 1.9, 2.27 and 2.45 in that order. The findings supported the initial problem statement and the conceptual framework that indicate that risk management is not sufficiently integrated into ITIL especially on the Service Strategy module that consist of the IT financial management, service portfolio management, demand management processes.

4.4.1 Level of Agreement with Statements concerning ITIL implementation.

The research requested the respondents to indicate their level of agreement with the various statements related to the ITIL implementation. Findings are presented in table 18.

Table 18: Level of Agreement with Statements concerning ITIL implementation.

	Mean	Std. Deviation
Successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actually spent and approved budget.	4.64	0.483
Gaps in disaster preparation and lack of value for money could be mainly as a result of poor service design	4.19	0.847
Increased number of performance measures is an indicator of a well adopted service transition process.	3.19	1.350
High number of successful access attempt is an attribute of a well implemented service operation.	3.83	0.843
A high percentage of new services is a byproduct of a well-structured continual service improvement process.	3.91	0.680

Source: Research

From the findings, majority of the respondents were in agreement that successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actually spent and approved budget. This had a mean score of 4.64. Respondents who agreed on the statement that gaps in disaster preparedness and lack of value for money as a result of poor service design scored a mean of 4.19. A high percentage of new service as a by-product of a well-structured continual service improvement process scored a mean of 3.91, high number of successful access attempt as an attribute of a well implemented service operation scored 3.83 while increased number of performance measures as an indicator of a well adopted service transition process scored 3.19.

The findings indicate that successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actually spent and approved budget.

4.5 Challenges Affecting ITIL Framework Implementation

This section sought information about challenges affecting ITIL framework implementation. The research requested respondents to rate the challenges using a scale of 1 to 5 as defined in section 4.3. The Findings are presented in table 19.

Table 19: Challenges Affecting ITIL Framework Implementation.

	Mean	Std. Deviation
High cost in implementing the framework	3.66	0.978
Organizational Culture - Staff resisting change	4.10	0.908
Lack of support from top management	2.81	0.833
Lack of continuous training in ITIL	3.28	1.059
Lack of planning in the implementation of ITIL	3.06	1.384
Lack of risk management integration	3.63	1.085
Size of the organization	3.49	0.659
Organizational structure	3.79	1.118
Complexity of the processes within the airline	4.19	0.728
Lack of qualified personnel to lead the ITIL process	2.52	1.165
Lack of adequate infrastructure e.g. workspace, equipment	2.53	0.904

Source: Research

From the findings, majority of the respondents indicated that complexity of the processes within the local airline affected ITIL framework implementation to a great extent having scored a mean of 4.19. Organizational Culture (Staff resisting change) also affected ITIL framework implementation at the airline having a mean score of 4.10. Other challenges as rated by the respondents were organizational structure, high cost in implementing the framework, lack of risk management integration, size of the organization, lack of continuous training in ITIL, lack of planning in the implementation of ITIL, lack of support from top management, lack of adequate infrastructure e.g. workspace, equipment and lack of qualified personnel to lead the ITIL process with a mean scores of 3.79, 3.66, 3.63, 3.49, 3.28, 3.06, 2.81, 2.53 and 2.52 respectively.

The findings indicate that complexity of the processes within the local airline and Organizational Culture (Staff resisting change) affected ITIL framework implementation in the airline to a great extent. This finding supports the conceptual framework that took consideration of intervening variables.

4.5.1 Expectation from Effective Risk Management integration into ITIL

The research requested the respondents to indicate their expectations from effective risk management integration into ITIL. Findings are presented in Table 20.

Table 20: Expectation(s) From Effective Risk Management integration into ITIL

	Frequency	Percent
Reduced financial loses	30	34.8
Improve communication with stakeholders	18	20.9
Improved decision making	10	11.6
Improve resource allocation	28	32.5
Total	86	100

Source: Research

Findings show that majority of the respondents (34.8%) stated that they were expecting reduced financial loses, 32.5% expected improved resource allocation, 20.9% expected improved communication with stakeholders while 11.6% expected improved decision making. This shows that majority of the employee at the local airline expected reduced financial loses and improved resource allocation.

4.6 Results from Focus Group Discussions.
4.6.1 Level of ITIL Implementation

The research had asked the respondents to discuss the level of implementation of service strategy, service design, service transition, service operation and service continual improvement ITIL processes in the local airline. Findings are presented in Table 21 to Table 25

Table 21: Level of Service Strategy Implementation at the airline.

Item	Response	Comments
Service strategy	IT strategy had been defined for 1, 2 and 3 years against the business strategy of 1, 5 and 10 years. IT financial management and Service portfolio management had also been implemented though on the initial stages due to lack of resources to own and drive them. Demand management had come as a by-product of capacity management. A deliberate effort had been made to implement business relationship management as this lies in the heart of customer satisfaction. Service strategy had been largely adopted and implemented. Successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actually spent and approved budget. The customer satisfaction index dropped anytime a new service was introduced. The airline needed to define and document, important input from clients and external service providers in a strategic plan.	From the responses, it shows that some work had been done in the implementation of service strategy processes. It also shows that Successful service strategy implementation would eliminate the risk of customer dissatisfaction and budget over-runs.

Source: Research

Table 22: Level of Service Design Implementation at the airline.

Item	Response	Comments
Service Design	All processes had been implemented apart from information management. Service design had been well adopted and was a normal way of work. Service design had provided guidance for the design, development of services and service management processes.	The responses show that there was a deliberate effort to implement service design, however not all processes had been implemented.

Source: Research

Table 23: Level of Service Transition Implementation at the airline.

Item	Response	Comments
Service transition	Service transition processes had been adopted although not all of the underlying processes had proper ownership. Successful Service transition process implementation had been affected by staff turnover and the long training cycles. Service transition had been largely campaigned for and the focus was on adoption and proper implementation. There was need to create change evaluation reports that would be used at different points in a change lifecycle. Potential risk lay in developing standard measures across projects and suppliers. Service transition had provided guidance for the development and improvement of capabilities for transitioning new and changed services into operations. In transitioning services from service design to service operation, Service transition had some elements of controlling the risks of failure and disruption of services to the customer. The airline staff had managed the complexity related to changes in services and service Management processes hence preventing undesired consequences while allowing for innovation.	The respondents were of the view that there was some risk elements in service transition. However the risk elements were lacking in defining process ownership and specific metrics which are integral to proper risk management process.

Source: Research

Table 24: Level of Service Operation Implementation at the airline.

Item	Response	Comments
Service operation	Service operation processes were fully implemented and fully owned. Service operation processes had been embedded in the culture and had become a way of life. Service operation had been largely adopted and implemented.	The respondents were of the view that service operation process had matured and was already embedded in the culture of the organization.

Source: Research

Table 25: Level of Service Continual Improvement Implementation at the airline.

Item	Response	Comments
Service continual improvement	Service measurement and reporting as well as 7 – step service improvement had matured and stabilized. Work was being done to fine tune and optimize Service measurement and reporting processes. Continual improvement had largely been adopted and implemented. Keeping updated database was the bedrock to continual service improvement process.	The respondents were of the opinion that Service continual improvement process had been implemented to a large degree although there was still room for improvement. It was also seen that there were some challenges in up-to-date record keeping.

Source: Research

4.6.2 Risk management gaps within the ITIL framework

The Risk gaps identified within ITIL framework were as follows:-

i) Lack of defined accountabilities and responsibilities in managing the risks identified.

ii) Lack of metrics to measure compliance to defined risk mitigations.

iii) Alienation of some key support and operations staff in decisions making.

iv) Budget over-runs to address inadequate risk mitigations during services transition.

v) Resistance to change and circumvention of the processes due to perceived bureaucracy.

vi) Excessive costs to the business caused by overly risk-averse Service Transition practices and plans.

vii) Undefined standards in Knowledge sharing which may result to unauthorized people having access to information

viii) Lack of integration of systems and tools resulting in people 'blaming' technology for their shortcomings.

ix) Poor integration between the processes – which can cause process isolation and a silo approach to delivering IT services.

x) Loss of productive hours, higher costs, loss of revenue or perhaps even business failure as a result of poor service transition processes.

xi) Decrease in customer satisfaction hence reduced customer count as a result of creation of services that are not aligned with the organization's strategy and/or customer needs.

xii) Poor customer satisfaction as a result of definition of unstructured or un-competitive strategy.

xiii) Gaps in disaster preparedness and lack of continuity plans as results of lack of appropriate information on future plans and strategies.

xiv) Failed goals as a result of inadequate reporting on progress thus failing to take corrective actions in good time.

4.6.3 Benefits of ITIL Implementation

The research had asked the respondents to discuss what ITIL framework had led to and also give their view on risk management statements within the ITIL context. The findings are presented in Table 26

Table 26: What ITIL Framework has led to.

Statement	Response	Comments
ITIL has led to improved IT services through the use of proven best practice processes at the local airline	Systems availability levels had improved from 97 % to 98% and 99.9 % in progressive years (Data from operating reports).	There was factual data to support the statement that ITIL had led to improved IT services.
ITIL has led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time at the local airline	Customer satisfaction had improved from 60% to 95 % as a result of reliable services (Data from Customer satisfaction surveys). Reduced staff and efficient workforce (all problems are resolved in a structured way hence no re-work)	The improved IT Services as a result of ITIL had led to reliability of services hence improved customer satisfaction. The respondents' statement shows that ITIL had improved efficiency which had translated to financial savings.
ITIL has led to improved resource management and usage, improved decision making and optimized risk management at the local airline.	Standardization of processes and services had led to resource sharing (both human and technology). Decisions were supported by actual data from the ITSM tool. Risk management was focused on the day-to-day services operation (risks as a result of unplanned change) but lacking on strategic level (future planning).	The respondents' were of the opinion that ITIL had led to improved strategic planning and short term risk management practices. ITIL had also led to optimal utilization of resources.

Statement	Response	Comments
	Process improvement and adoption of new technologies had led to resource optimization. Management decisions were based on facts from data collected.	
ITIL had led to improved productivity as well as improved use of skills and experience at the local airline.	Higher systems availability translated to improved staff productivity. There was also time for innovation and specialization. Standardization of services had also led to improved service availability and employee productivity.	The respondents' stated that ITIL had led to standardization of services. Standardization leads to repeatability hence improved employee productivity.
ITIL adoption had led to an improved risk management practice.	IITL had led to day-to-day systems availability risk management but no clear long term risk mitigation strategy. ISMS framework had been implemented to manage risk despite having implemented the ITIL framework.	The statements would mean that although it has some risk management elements, ITIL does not address all risk aspects.
It is unclear if there is a standard way to treat risk and how to implement risk management process in ITIL .	There was no known standard that was in ITIL on how to implement risk. ITIL only talked on the importance of risk mitigation. In many processes, the risk element was mentioned and emphasis put on mitigation, however, there was no process defined, with roles and responsibilities highlighted on how to manage risk.	The statement is clear that ITIL is lacking in terms of risk management hence the need to revamp the framework.

Statement	Response	Comments
ITIL risk management should be mapped with other standards and frameworks to build a single, integrated body of work	Risk management could not be implemented in isolation or ad-hoc. It was important to integrate it to the day to day processes to become part of the culture in the organization and to build a strong foundation of delivering services to the customers end – to – end. There is no harm in borrowing from strengths of other frameworks to supplement the existing frameworks.	In principle, the respondents supported the statement that ITIL risk management should be mapped with other standards and frameworks to build a single, integrated body of work as the benefits out-weigh the challenges.
It is not advisable to adopt multiple frame works as they are costly and complex to implement.	Multiple frameworks would be complex and costly to implement. There is a challenge on how the frameworks would interface hence the risk of silos of knowledge and expertise. These silos would frustrate standardization of processes and services which would affect the service delivery.	The respondents supported the statement that It is not advisable to adopt multiple frame works citing the complexity, cost, interface and standardization challenges.

Source: Research

4.7 Discussion on Risk Indicators

The researcher asked the respondents to discuss the extent of the risk indicators on the respective ITIL components at the airline. The findings are presented in Table 27

Table 27: Discussion on Risk Indicators

Risk Indicator	ITIL Component	Response	Comments
Decrease/ Increase of customer's satisfaction.	Strategic management.	The IT strategy was defined for 1, 3 and 5 years against the business strategy of 1, 5 and 10 years. Customer satisfaction index dropped every time a new service was implemented. It was hard to predict customer satisfaction level for timeline of more than one (1) month.	It was found that definition of unstructured or un-competitive strategy would lead to poor customer satisfaction.
Decrease/Increase of customer satisfaction. Decrease /Increase of customers.	Service portfolio management	Customer satisfaction index dropped every time a new service was implemented. There was always resistance to accept new systems / services. There was duplicate functionality in systems hence user dissatisfaction (due to re-work).	It was found that creation of a service that is not aligned with the organization's strategy or customer needs would lead to decrease in customer satisfaction hence reduced customer count.
Number of agreed UCs. Number of contract reviews. Number of suppliers and the information about them.	Supplier management	All suppliers were registered in the system / database and they (Suppliers) had their information updated regularly. Each service had a signed contract with explicit SLA's. Contract reviews were not systematic but dependent on the service contracted, supplier and time.	The discussions revealed that expensive but poor services and no value for money would be a likely result of poor supplier management,

Risk Indicator	ITIL Component	Response	Comments
Gaps in Disaster Preparedness. Time lapse from identification of risk to the implementation of a suitable continuity mechanism.	Information Management	Gaps in Disaster preparedness only came to the light once disaster stroke. Once a risk was identified, mitigation was put in place urgently. Disaster recovery was not fully implemented and also there was quick implementation of continuity mechanisms but there was no post implementation reviews. There were huge gaps in disaster preparation and huge time laps in risk identification and implementation of continuity structures.	Lack of appropriate information on future plans and strategies would lead to Gaps in disaster preparedness and lack of continuity plans.
Number of performance measures created. Number of performance measures documented.	Evaluation Management	Performance metrics were set for all projects / initiatives. Performance tracked and documented. Standardized performance measures were important to be put in place.	It came out clear that developing standard performance measures and measurement methods across projects and suppliers would improve performance evaluation.
Number of access attempts. Number of authorized access attempts. Number of unauthorized access attempts.	Access management	All users were given the access levels depending on their roles and with management authorization. Systems were put in place to track any illegal access attempts and audit reports produced. Access was given on need basis and illegal access attempts audited and necessary measures taken.	Proper access management would reduce the risk of unauthorized access.

Risk Indicator	ITIL Component	Response	Comments
Percentage of new services.	7-Step service Improvement.	New performance metrics were set each year, tracked and reported on (to ensure improvements to services). New services were implemented in line with business requirements. The introduction of new services was dictated by the business requirements.	From the findings, the adoption of 7-Step service Improvement. Process would ensure that the IT is properly aligned with the business needs and also eliminate the risk of static services throughout time.
Percentage of organization goals tracked/reported.	Service Reporting	All goals were tracked and reviewed quarterly. All set targets tracked and reported on each quarter and corrective actions taken in case of deviation.	From the discussions, it was revealed that sustaining continuous reporting would ensure that that all organizational goals are tracked and corrective measures taken in good time to mitigate the risk of failed goals.

Source: Research

4.8 Actions Recommended for Effective Risk Management

From the findings, the known risks were mitigated very fast and effectively but in an ad-hoc manner. There was still a gap in identifying these risks as many of them were identified once a catastrophic event occurred. There was therefore need to revamp the process to continuously and consistently do risk identification, define roles and responsibilities to deal with the identified risks, set auditable metrics, and track them on the short, medium and long term. Apart from driving change through continual improvement, the organization must be prepared for rapid transitions and transformations driven by changes in the organizational environment or internal situation while managing potential risks. Changes may be driven by, sourcing decisions, actions of competitors, technology innovations and shifts in customer preferences hence Service management should respond effectively and efficiently.

Other actions that were recommended include:-

i) Creation of a Service Measurement Framework.
ii) Encouraging the organization to continuously improve services.
iii) Adequate customer-oriented and technically trained support staff that should have the correct skill level at all stages of the process.
iv) Building a thorough understanding of risks that have caused an impact or may impact successful Transition of services and releases.
v) Encouraging a risk management culture where people share information and take a pragmatic and measured approach to risk.
vi) Keeping abreast of current and future technologies.

4.9 Qualitative and Quantitative Research Results

Table 28: Qualitative and Quantitative Results Comparison

Risk Factor	Outcome (Qualitative)	Corresponding Quantitative outcome
Percentage Decrease/Increase in customer's satisfaction levels.	Most of the respondents were in agreement that successful service strategy implementation would lead to increased customer satisfaction. However some were of the view that the customer satisfaction index dropped anytime a new service was introduced. They said that the airline needed to define and document, important input from clients and external service providers in a strategic plan.	Majority of the respondents were in agreement that successful service strategy implementation would lead to increased customer satisfaction. This had a mean score of 4.64 with a standard deviation of 0.483.
Degree of Variance between actual spent and approved budget.	Most of the respondents were in agreement that successful service strategy implementation would lead to a small variance between actual spent and approved budget.	Those in agreement that successful service strategy implementation would lead to a small variance between actual spent and approved budget scored a mean of 4.64 with a standard deviation of 0.483.
Gaps in Disaster Plan(s).	There were Gaps in Disaster preparedness and they only came to the light once disaster stroke. It was also noted that once a risk was identified, mitigation was put in place urgently but there was no post implementation reviews. There were huge gaps in disaster preparedness and huge time laps in risk identification and implementation of continuity structures.	The statement that gaps in disaster preparation and lack of value for money could mainly be as a result of poor service design scored a mean of 4.19 with a standard deviation of 0.847. This supported the statement that Service Design was not implemented to a large extend which had scored mean of 2.98 with a standard deviation of 0.854
Number of performance measures created. Number of performance measures documented	Performance metrics were set for all projects / initiatives and performance tracked and documented. The respondents were also of the opinion that standardized performance measures were important to be put in place.	Increased number of performance measures as an indicator of a well adopted service transition process scored 3.19.

Risk Factor	Outcome (Qualitative)	Corresponding Quantitative outcome
Number of access attempts. Number of authorized access attempts. Number of unauthorized access attempts.	Responses from the respondents confirmed the significance of keeping updated access database. They said it was advisable for organizations to keep a flexible system linked to the ability to manage changes to user access rights according to the roles in the organization.	High number of successful access attempt is an attribute of a well implemented service operation scored 3.83
Time lapse from identification of risk to the implementation of a suitable continuity mechanism.	About the statement that ITIL adoption had led to an improved risk management practice, it was seen that ITL had led to day-to-day systems availability risk management but no clear long term risk mitigation strategy. ISMS framework had been implemented to manage risk despite having implemented the ITIL framework. This would mean that ITIL does not address all risk aspects.	The statement ITIL adoption led to an improved risk management practice scored a mean of 2.90 with a standard deviation of 0.882.

Source: Research

4.10 Causal relationship between research variables

The research ascertained that the research variables in one way or the other affected ITIL implementation. There were three categories of variables considered namely; intervening, dependent and independent variables. Results showed that the size and complexity of the organization influence service strategy implementation and ultimately affected ITIL implementation. Level of risk management integration further complicated the relationship.

In order to measure the degree to which the independent variables contributed to the dependent variable, each construct was measured using respondent's comments.

Figure 9 and table 29 summarizes the causal relationship, between the variables.

Table 29: Respondents Comments

Service Strategy
Increase in customer satisfaction levels was as a result of good strategy definition.
Increase in customer count would be as a result of creation of services aligned to the customer needs.
Decrease in variance between actual spent and budget in successive years would mean successful implementation of financial management process
Service Design
Gaps in disaster preparedness and lack of value for money could be mainly as a result of poor service design
Increase in the number if Underpinning contracts (UC's) was a result of good supplier management
Increase in the number of properly registered suppliers was as a result of good supplier management
Increase of gaps in disaster preparedness was as a result of poor information management
Service Transition
Increased number of performance measures is an indicator of a well adopted service transition process
Increase in number of performance measures documented would be as a result of good performance evaluation process
Service Operation
Increase in number of successful access attempts is an attribute of a well implemented service operation
Increase in number of un-authorized access attempts indicate poorly implemented access management.
Service Continual Improvement
A high percentage of new services is a byproduct of a well structured continual service improvement process
Percentage increment of organizations goals tracked and reported is an indicator of good Service measurement and reporting
Level of Maturity of ITIL implementation
Performance measures were set for all projects/ initiatives and tracked on a quarterly basis
Customer service index had increased from 60% to 95% in 2 years
Systems availability levels had improved from 97% to 98% and then to 99 % in progressive years
Standardization of processes and services had led to resource sharing (both human and technology)
Decisions were based on facts from data from the ITSM tool
There were huge gaps in disaster preparedness and only came to light once disaster stroke.

Figure 9: Causal relationship between the variables
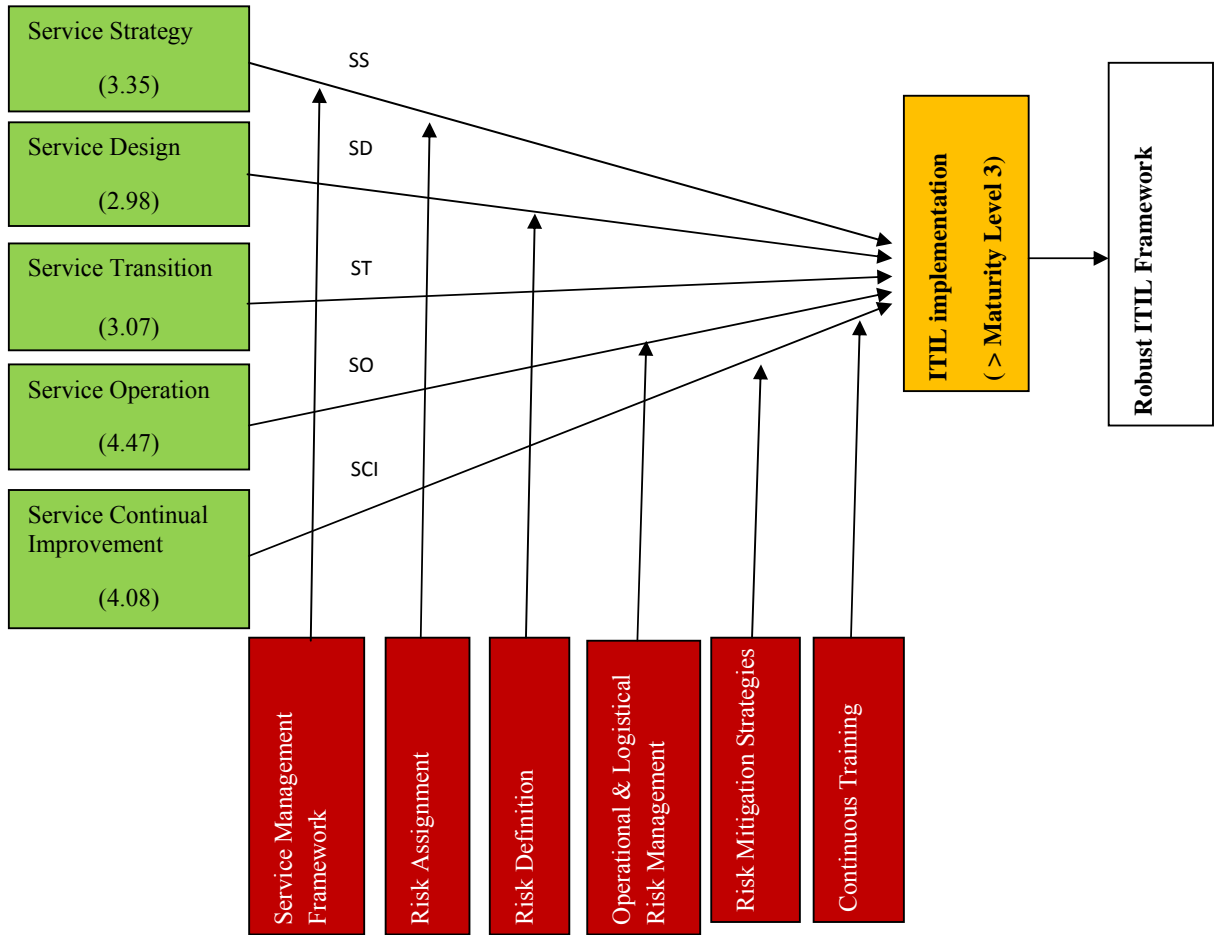
Source: Research

Table 30: Explanation on Causal relationship between the variables

| Element	Description
Service Strategy (SS)	The increase in risk management in Service Strategy processes by the introduction of service measurement framework and risk assignment processes would improve the ITIL implementation by mitigating against the definition of substandard or mis-aligned strategies that do not meet customer needs. It would also positively impact smooth transition of services.
Service design (SD)	The increase in risk management in Service Strategy processes by the introduction of risk definition process would positively impact on ITIL implementation by ensuring that the designed services meet customer needs, have disaster recovery measures factored and have the requisite underpinning contracts with well defined performance metrics.
Service Transition (ST)	Service transition makes sure that changes to services and Service operation processes are carried out in a coordinated way while controlling the risks of failure and disruption. The research found this element to have risk management integrated in most of its processes and therefore is not likely to have a significant impact on the maturity level of ITIL implementation.
Service Operation (SO)	The risk management on this module is around organizations' routine and focuses on delivering and supporting all services at the same time. The introduction of operational and Logistical risk process would have a positive impact on the ITIL framework implementation in that it would assist to control and manage all risk aspects associated with day-to-day operations especially around information systems security management In addition, operation managers should work closely with Service Design and Service Transition to provide the operations perspective, thus ensuring that design and transition outcomes support the overall ITIL implementation.
Service Continual Improvement (SCI)	While Risk Management in design and transition stages must organize concepts and mainly identify risks of the service lifecycle, a good Continuous Service Improvement program will assess the results of Risk Management activities to identify service improvements. Processes within this module lacked risk management components and consequently compromised the ability significantly improve the rest. The introduction of risk mitigation strategies as well as continuous training would therefore positively improve ITIL framework because it would ensure continuous improvement on risk management amongst all the other lifecycle modules.

Source: Research

Table 31: New Elements into ITIL Framework

New Element	Underlying Lifecycle Module
Service Measurement framework	Service Strategy
Risk Assignment	Service Strategy
Risk Definition	Service Design
Operational and Logistical Risk Management	Service Operation
Risk Mitigation Strategies	Continual Service Improvement
Continuous Training	Continual Service Improvement
Change Management (Organizational)	Intervening Variable

Source: Research

4.11 Resultant Framework

Figure 10: Resultant Framework
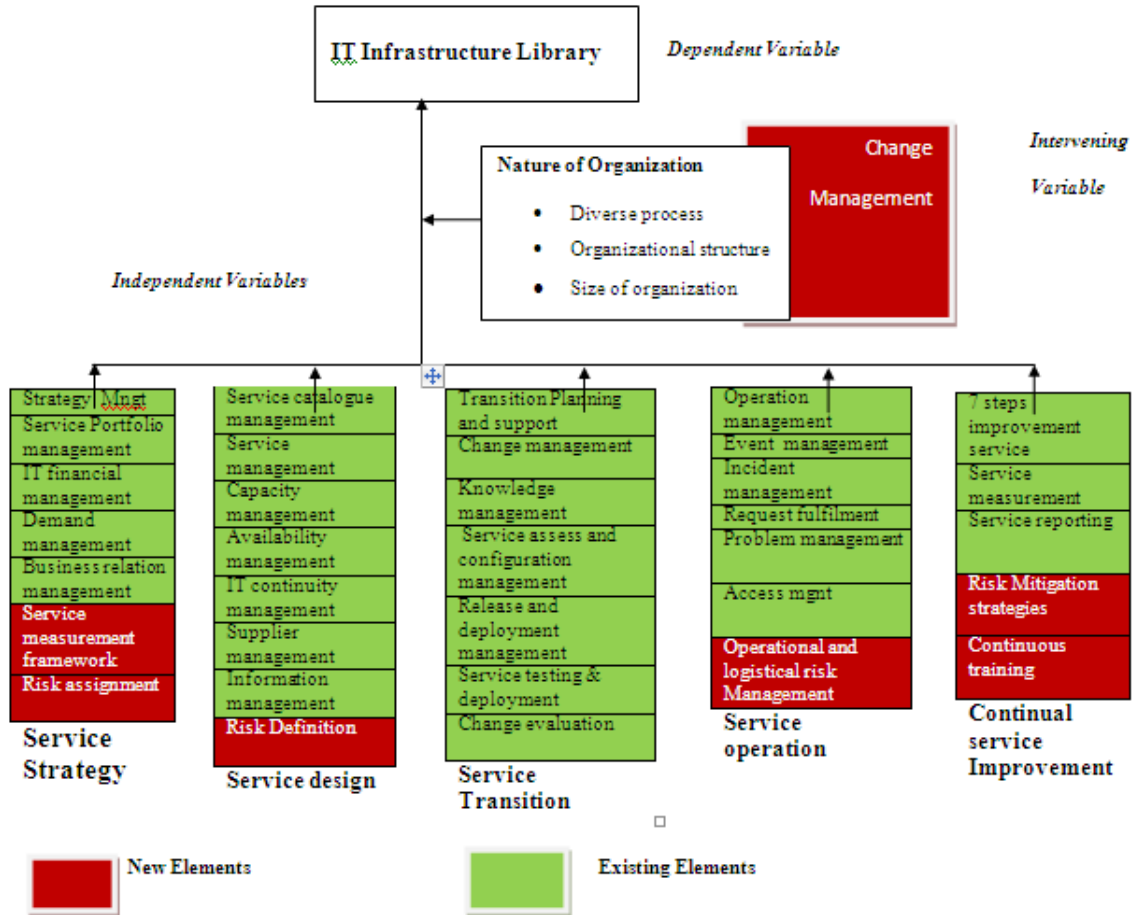
Source: Research

The main intention of this research was to introduce new risk elements where they are not specified and reinforcing of ITIL risk management concepts on areas with deficiency. It was expected that the resultant framework would ensure risk elements are integrated at all levels in addition to borrowing from the strengths of other related frameworks such as COBIT and M_O_R. Result of the research confirmed that some of the independent variables had risk management partially integrated or completely lacking. Finding of the research formed a strong base upon which the resultant framework was formulated. Results also revealed that there was need to manage the effects of the intervening variables such as size of organization, complexity of the processes and organizational structure. This could be achieved by developing measures of the main constructs of interest to enhance the employees working towards the same goals popularly referred to as change management. Organizations have an option of adopting the behavior system leverage points to drive and sustain change during and after the ITIL implementation.

4.12 Chapter Summary

The chapter gave a summary of both qualitative and quantitative results. The results agreed with the initial problem statement that there existed gaps in risk management in view of the ITIL framework. Respondents confirmed that risk management in ITIL was focused on the short term and not the long term. This supports the conceptual framework which had outlined risk as insufficient on the service strategy lifecycle module which is concerned with strategic planning but relatively sufficient on the Service operation module that is concerned with the day-to- day support of systems. A comparison between the qualitative and quantitative results was presented, causal table developed and a new improved resultant framework derived with a proposal on how to handle the effects of the intervening variables.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter evaluates the attainment of research objectives, outlines the recommendations and carries out a self-assessment of the research. It also highlights areas that could be explored in the future.

5.2 Evaluation of Research Objectives

The broad objective of this research was to come up with a framework of ICT service management that improves the current ITIL service delivery framework to incorporate risk management. The research began by identifying risk management attributes that could be applicable to ICT services and further made use of existing literature in addition to information from subject matter expert to determine risk management gaps in ITIL framework. Subsequently a conceptual ITIL Service management framework was developed articulating respective components in which risk management had not been factored.

Objective 1: Identify Risk management attributes that could be applicable to ICT services.

The matching question for this objective was: *What are the Risk management attributes that could be applicable to ICT services?*

The research came up with the attributes namely usability (Customer Satisfaction), Availability, Capacity, Security and Continuity.

Usability means that the service needs to fulfill the customer needs. The measure to this is the degree to which the customer is satisfied with the services and can be expressed as a percentage. It was established that successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actual spent and approved budget. There is a likelihood of having IT services that are not usable and this can pause a great risk to the business hence the need for mitigation.

Availability means the IT services are available to the end users as and when needed. Availability management defines, analyzes, plans, measures and improves all aspects of the IT services' availability. Availability Management is responsible for ensuring that the level of service availability delivered in all services is matched to or exceeds the current and future agreed business needs, in a cost-effective manner. IT services availability is measured as a percentage. One of the greatest risks to IT services is "unavailability" and deliberate effort must be put to counter any threat to systems continued availability.

Capacity refers to "width and breadth" of IT infrastructure to "carry and deliver" the IT services to the end users. The Capacity management process is responsible for ensuring that the capacity of the IT services and IT infrastructure are able to deliver the agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service, and plans for short, medium and long term business requirements. Discussions showed that standardization of processes and services had led to resource sharing (both human and technology) thus reducing the cost. Also process improvement and adoption of new technologies had led to resource optimization. Effectiveness of capacity management is measured by the percentage incidents as a result of capacity constraints or the percentage budget that is attributed to excess capacity. Lack of sound capacity plans can pose a great risk to the availability and /or usability of the IT services.

Security of IT resources important to ensure integrity and confidentiality of the information. Security breaches can be classified as:-

- Operational - where human resources access unauthorized information or perform human errors
- Technical- where the ICT infrastructure does not have sufficient controls and
- Strategic - where weak conceptual designs (strategic level) translates to poor processes and methods of work (logical level) and deficient operational plan (physical structure level).

Security effectiveness can be measured by the number of successful unauthorized access attempts in a given period or number of security breaches in a period. Security is regarded as the greatest risk factor to any IT service and organizations have invested heavily to secure their systems.

IT Service Continuity was found to support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities can be resumed within required, and agreed on, business timescales. As technology is a core component of most business processes, the continued or high availability of IT services is critical to the survival of the business as a whole. This can be measured by the mean time to recover (MTTR) or mean time between failures (MTBF). Lack of continuity plans is regarded as the second highest risk factor to IT services after security.

The success of the provision of ICT services end-to-end will depend on the effectiveness of the IT service management framework implemented. There is therefore need to mitigate the potential risks factors around the aforementioned IT services attributes. The risk management components will thus provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organizations ITSM processes, determine the nature of risks which are acceptable and not acceptable to the organization; and provide the detailed structure and mechanisms through which the organization manages risk at varying levels and also ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all times.

Objective 2: Determine what needs to be incorporated in the ITIL service management framework to address the risk management gaps.
The matching question for this objective was: *What needs to be incorporated in the ITIL Service management framework to address risk management?*

Among the components that had not integrated risk management include change management, knowledge management, transition management, planning and support, strategic management, service portfolio, IT financial management, demand management; supplier management, service measurement management and 7 step improvements. Results of the research were consistent with conceptual framework. The components that were rate lowest include IT financial management process, service portfolio management process, demand management process and service catalogue process having scored a mean of 1.9, 1.9, 2.27 and 2.45 in that order

Those that were rated highly by the respondents include incident management process, request fulfillment process, service reporting process, change management process, event management process, access management process, availability management process and change evaluation scoring a mean of 4.44, 4.35, 4.29, 4.27, 4.09, 4.09, 4.08 and 4.08 respectively.

From the research findings the researcher was able to establish the measures that needed to be put in place to ensure that risk management was incorporated in all ITIL components. Among the measures proposed were such as:-

i)   Effective service strategy implementation as it would lead to increased customer satisfaction.

ii)   Need to define and document, important input from clients and external service providers in a strategic plan.

iii)   Closure of huge gaps in disaster preparedness and huge time laps in risk identification and implementation of continuity structures.

iv)   Performance metrics to be set for all projects / initiatives and performance results tracked and documented.

v)   Implementation of standard performance measures.

vi)   Keeping an up-to-date access database.

vii)   Development of a clear long term risk mitigation strategy.

viii)   Describing the organizations understanding of risk in the context of its operations, legislation and strategies.

ix)   Describing organizations overall approach, intention and procedures used to identify, analyse, evaluate and treat risks.

x)   Describing clearly the roles and responsibilities in relation to managing risk.

xi)   Broadly describing the boundaries which define acceptable and unacceptable levels of risk.

Objective 3: Develop a conceptual ITIL Service management framework that incorporates Risk management.

The finding of the research formed a strong base upon which the resultant framework was formulated as presented in Figure 10 of Chapter 4. Results also revealed that there was need to manage the effects of the intervening variables such as size of organization, complexity of the processes and organizational structure. This could be achieved by developing measures of the main constructs of interest to enhance the employees working towards the same goals popularly referred to as change management.

According to research findings the new framework would benefit the organization in the following ways;

i)   Improve IT services through the use of proven best practice processes.

ii)   Improve user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time, reduced staff and efficient workforce (all problems are resolved in a structured way hence no re-work).

iii)   Improve decision making and optimize resource utilization. Discussions showed that standardization of processes and services would lead to resource sharing (both human and technology). Also process improvement and adoption of new technologies would lead to resource optimization. Management decisions would be based on facts from data collected.

iv)   Higher systems availability would translate to improved staff productivity. There would also be time for innovation and specialization. Standardization of services would lead to improved service availability and employee productivity.

v)   Clear long term risk mitigation strategy.

vi)   Well defined processes, with roles and responsibilities highlighted on how to manage risk and metrics to measure compliance.

vii)   Integrate risk management to the day to day processes to become part of the culture in the organization thus building a strong foundation of delivering services to the customers end – to – end.

viii)   Explicitly addresses uncertainty – takes account of the nature of the uncertainty and how it can be addressed.

ix)   Create and protect value – helps to achieve the objectives and improve performance of the organization.

x)   Enable tailoring – alignment with the organization's operating environment and risk profile.

xi)   Take human and cultural factors into account – recognizing the human capabilities and limitations.

5.3   Research Assessment

The researcher adopted the whetten (1989)'s seven question model to assess whether the work constitutes a theoretical contribution. Though the questions originally apply to the organizational science field, they provide a background through which this study can be reflected.

1.   What's new? Does this work make a significant, value-added contribution to current thinking?

The conceptual framework has its foundation on the related work (examples include ITIL and Corporate Risk Management by Michael Faber and Rubina Faber, March 2010; Risk Management Model in ITIL by Sarah Villa – Real Vilarinho, June 2012), the experience of experts in this field and the researchers experience with ITIL framework. Its main approach is introducing new risk elements where they are not specified and reinforcing of ITIL risk management concepts on areas with deficiency. The new elements introduced into the framework are listed in Table 31 of chapter 4. The research has also pointed out the need to manage intervening variables such as size of organization, complexity of the processes and organizational structure by adopting the behavior system leverage points to drive and sustain change during and after the ITIL implementation.

2.   So What? Will the research change ITIL service management framework?

The main intention of this research was to introduce new risk elements where they are not specified and reinforcing of ITIL risk management concepts on areas with deficiency. It was expected that the resultant framework would ensure risk elements are integrated at all levels in addition to borrowing from the strengths of other related frameworks such as COBIT and M_O_R. Result of the research confirmed that some of the independent variables had risk management partially integrated or completely lacking. Finding of the research formed a strong base upon which the resultant framework was formulated. Results also revealed that there was need to manage the effects of the intervening variables such as size of organization, complexity of the processes and organizational structure. This could be achieved by developing measures of the main constructs of interest to enhance the employees working towards the same goals popularly referred to as change management. Organizations have an option of adopting the behavior system leverage points to drive and sustain change during and after the ITIL implementation

From the findings, 11.6% of the respondents were senior managers, 20.9% line managers, 67.5% support staff. The findings indicate that majority of the respondents were support staff. This is important because whereas the senior managers would give insight to the research based on their experience, the support staffs are the ones who are actively involved in operationalizing the ITIL framework on a day-to-day basis. In addition, results of the research confirmed that some of the independent variables had risk management partially integrated or completely lacking. Finding of the research formed a strong base upon which the resultant framework was formulated. Results also revealed that there was need to manage the effects of the intervening variables such as size of organization, complexity of the processes and organizational structure.

3. *Why so? Are the underlying logic and supportive evidence compelling?*

The research was based on sound methodological approach and well tested research design and conforms to acceptable levels of measurement. Identification of gaps within the ITIL framework entailed reference to other related studies; seeking opinion from subject expert as well banking on the researchers experience on the ITIL implementation process at a local airline. The Experts' opinion was gathered through research articles/publications, questionnaires and results of focus groups. The focus groups were chosen depending on their ability to articulate their opinion on the subject, work experience and availability. ITIL experts Information obtained helped the researcher formulate the conceptual framework in which the various variables were determined and a questionnaire developed accordingly. Data collected was analyzed and shared with the subject matter expert for validation purposes before conclusion and recommendations were drawn. The subject matter experts were drawn from a local airline employees holding ITIL Expert Certification and are practicing ITIL in their day-to-day work. The results were adopted in selected sections of the organizations in order to test the robustness of the risk integrated framework.

4. *Is the research well done?*

The research was based on a tested framework and data was collected being cognizant of research best practices. An exploratory research method was adopted in this research. This method allows a researcher to explore a particular phenomenon or circumstance (such as ICT risk management in an organization) in order to provide sufficient information to design, develop and execute the next research steps. In addition, a mixed mode approach was adopted as there were multiple objectives to this research. Quantitative and qualitative research approaches supplement each other to produce a mixed mode research approach. The qualitative research provided in-depth explanations, respondent's experiences, opinion and knowledge while the quantitative research approach provided statistical data. Both techniques were used to draw from their strengths and minimize the weaknesses of quantitative and qualitative research approaches hence increase validity and reliability of the data collected.

5. *Is the report well written?*

The report follows guidelines set by the School of Computing and Informatics of the University of Nairobi. The structure of the report starts with introduction where the objectives are set and the background, justification of the study provided. The researcher then explored the theoretical background of the study where other frameworks such as COBIT and M_o_R were reviewed and then concluded by proposing a conceptual ITIL model that incorporates risk management. The research methodology was then presented where the data collection instruments were described as well as data analysis and validation techniques. The results were presented, discussed and conclusion

and recommendations drawn. This reports format is therefore consistent with the standards expected for academic writing.

6. Why now? Is this topic of contemporary interest to the scholars in this area?

The ITIL framework was developed in the UK and has been adopted by local companies to manage their IT Services. However, no research, to the best of the researchers' knowledge has been done to evaluate improvements that can be incorporated into the framework to suite to the local setting. This is therefore a research that can interest information systems researchers who have an interest in the African setting.

7. Who cares? Who is interested in this topic?

The finding of this research would benefit IS Managers by introducing a "one-stop-shop" improved service delivery framework that addresses all the variables of ICT service management namely Usability (Customer Satisfaction), Availability, Capacity, Security, Continuity and Risk Management. This would eliminate multiple frameworks thus reducing operating costs and management complexity.

The research finding would also be of interest to the academic fraternity and other researchers by helping them to understand Risk Management within the context of a service industry and by having come up with an improved service delivery framework that incorporate Risk Management hence adding to the body of knowledge.

5.4 Conclusion

Based on the above findings, the following conclusions were drawn:

i) The findings of this thesis should be used as a guideline for organizations implementing this type of a framework. The information provided in this research project is useful for people who are looking forward to adopt and implement a versatile ITIL framework as new ITSM guideline for their organization. This research highlights the deficiencies in ITIL regarding risk management and suggests measures that must be kept in mind when implementing the framework to reap the most benefit.

ii) Risk management is essential to all organizations. The need of predicting and preparing organizations to face the unexpected with flexibility and agility is real in today's business environment.

iii) ITIL service management framework does not provide a clear concept on how to treat risk and there is need for a guideline in ITIL about how to manage risk.

iv) In organizations nowadays, risk is a completely separate process that includes not only IT but all organizational aspects.

v) For organizations implementing ITIL, It is important to ensure that they Integrate or adapt a risk management framework, embedded it into ITIL, document the methodology, processes and create key risk indicators, link them to strategic responses and develop metrics to measure compliance.

vi) Multiple frameworks are costly and complex to implement, however there is no harm in borrowing from strengths of other framework to supplement the existing frameworks. It is also worth noting that multiple frameworks are complicated and need multi-skilling or duplicated human resources.

vii) The value of ITIL is undeniable as it helps reducing IT costs, increase IT performance and, at the same time, improve business performance through IT-business alignment. These qualities are vital for any organization.

viii) There is need to communicate the organizations outlook towards risk and effectively define an approach to risk management. In addition it would be of essence to encourage a risk management culture in which people share information.

ix) Advantages to the using the enhanced framework (risk integrated) include having the roles and responsibilities for risk management clearly defined and assigned and also having consistent process audit metrics.

5.5 Recommendations

To enhance the ITIL framework the research recommends that;

i) ITIL framework should be mapped with other standards and frameworks to build a single integrated body of work.

ii) Organizations should define and document their goals, important input from clients and external service providers in their strategic plan to ensure a structured or competitive strategy.

iii) It would also be advisable to keep users database updated as well as keep a flexible system linked to the ability to manage changes to user's access requirements and give multiple access rights according to the roles in the organization. This would effectively mitigate the risk that may result from the inability to restrict access rights to unauthorized users.

iv) There is need to revamp the ITIL process to continuously and consistently do risk identification, define roles and responsibilities to deal with the identified risks, set auditable metrics, and track them on the short, medium and long term.

v) A service portfolio review report, a document containing the results and findings from a service portfolio audit should be created frequently to ensure all updates are captured.

vi) In order to obtain value for money, a Supplier and Contract Management System should be created. This could be in the form of a database or structured document that would enable the organization to manage suppliers and contracts throughout their life cycle. It would also contain the key attributes of all the contracts with the suppliers and should be part of the service knowledge management system.

vii) To enhance understanding of how to manage risk and/or take risk as it affects the overall strategy of the organization and service delivery, organizations should build a thorough understanding of risks that have impacted or may have impacted successful transition of services and releases.

5.6 Future Work

This research was conducted in a local airline in Kenya and an independent observation of processes made on a regional carrier with local presence. The findings represent a unique context to which the conclusions may not be

generalized. Therefore, there is need to extend similar studies exploring risk management in the context of ITIL framework to other sectors like government departments, non-governmental organizations and academic institutions.

Due to the nature of the research and a limited number of participants, this is a subjective and limited view of the market and the tools. To obtain a more thorough view of the market, a much larger research with more participants would be required. Nevertheless, this research project has managed to cover the important aspects relating to risk management within the ITIL framework.

REFERENCES

Audit Commission. (2005). ICT fraud and abuse 2004. The Audit Commission for authorities and the National Health Service in England and Wales, England

Bandyopadhyay, K, Mykytyn, PP & Mykytyn, K. (1999). A framework for integrated risk management in information technology. Management Decision. 37 (5), 437-445.

Cartlidge & Alison (2007). An Introductory Overview of ITIL® V3. LONDON: ITSMF.

Cater-Steel, Aileen, Tan, Wui-Gee and Toleman. (2006). Challenge of adopting multiple process. Proceedings of 14th European Conference on Information Systems. ECIS 2006 (1), 1375-1386

Center for Technology in government 2007. (2007). Making smart IT choices. Understanding value and risk in government IT investment.

Crouhy, Michel, Galai, Dan and Mark (2005). The Essentials of Risk Management. USA: McGraw-Hill. 85-90

Dhillon, G & Backhouse, J . (1996). Risks in the use of information technology within organizations. International Journal of Information Management. 16 (1), 65-74

Douwe Brolsma & Mark Kouwenhoven (2010). *M_o_R (Management of Risk)*. 3nd ed. Amsterdam: Van Haren Publishing. 43-65.

ENISA. (Nov 29, 2010). The European Network and Information Security Agency (ENISA). *How to raise information security awareness (EN)*. 2 (1), 37-38.

Gerke, L & Ridley, G. (2006). Towards an abbreviated COBIT framework for use in an Australian State Public Sector. Available: http://aisel.aisnet.org/acis2006/83. Last accessed 4 August 2013

Haeri, A. G. (2005). Total quality management in an Iranian Auto Part Manufacture: the case of 'RAFA' Master of Art dissertation. 1-68.

IT Governance Institute (ITGI) & The Office of Government Commerce (OGC) (2005). Aligning COBIT, ITIL, and ISO/IEC 17799 for business benefit: Management summary, A management briefing from ITGI and OGC, ITGI & OGC, England

James P. Womack & Daniel T. Jones (2010). Lean Thinking: Banish Waste and Create Wealth in Your Corporation. 2nd ed. New York: Simon & Schuster, Inc. p29.

Khan, K. (2006). How IT governance is changing. Journal of Corporate Accounting & Finance. 17, (5), 21-5.

Kouns, Jake, Minoli and Daniel (2010). Information Technology Risk Management in Enterprise Environments. Canada: John Wiley & Sons

Lainhart IV, JW.(2001). COBIT: A methodology for managing and controlling information and
Information technology risks and vulnerabilities.Journal of Information Systems. 14, 21-5.

Massingham, P. (2010). Knowledge risk management: a framework. Journal of knowledge Management. 14, (3), 464-485.

McAdams AC. (2004). Security and risk management: A fundamental business issue.Information Management Journal. 38, (4), 36-45.

Nascimento Luís. (2010). Methodologies of Support to the Execution of Risk Management.
2nd International Conference on Software Technology and Engineering. I, 176-180.

OGC SS, 2007: Office of Government Commerce (2007). ITIL Service Strategy. 2nd ed. UK: TSO.

OGC SD, 2007: Office of Government Commerce (2007). ITIL Service Design. 2nd ed. UK: TSO.

OGC ST, 2007: Office of Government Commerce (2007). ITIL Service Transition. 2nd ed. UK: TSO

OGC ST, 2007: Office of Government Commerce (2007). ITIL Service Operation. 2nd ed. UK: TSO

OGC M P, 2007: Office of Government Commerce **(2007)** Management of Risk Pocketbook. UK: TSO.

Segars, AH & Grover. (1996). Designing company-wide information systems: Risk factors and
coping strategies. Long Range Planning. 29 (3), 381-92.

Sharifi, Mohammad. (2008) Lessons Learned in ITIL Implementation Failure. ITSM 2008. International Symposium Malaysia 1-4.

Smith, E & Eloff, JHP (2002).A prototype for assessing information technology risks in health
Care. Computers& Security. 21, (3), 266-84.

Smith, HA & McKeen, JD. (2006). Developments in practice XXI: IT in the new world of corporate governance reforms. Communications of the Association for Information Systems. 17 (1), 32.

Viator, RE & Curtis, MB (1998). Computer auditor reliance on automated and non-automated
Controls as a function of training and experience. Journal of Information Systems. 12, (1), 19-30.

Willcocks, L, Feeny, D & Olson, N.(2006). Implementing core IS capabilities: Feeny–Willcocks
IT governance and management framework revisited. European Management Journal. 24, (1), 28-37.

Wim Van Grembergen and Steven De Haes. (2005). COBIT's Management Guidelines Revisited:. Information systems control journal *L*. 6 (1), 1-3.

APPENDIX 1: QUESTIONNAIRE

Dear Colleagues,

My name is Titus Kitavi. This questionnaire is intended to gather research data as part of an academic investigation for my MSC – Information Systems at the University of Nairobi. This Questionnaire is divided into 5 sections.

Section (A) – ITIL framework implementation steps in the local Airline Industry, Section (B) – Degree of ITIL framework implementation in the local Airline Industry, Section (C) – Degree of Risk Management integration into ITIL framework in the local Airline Industry, Section (D) – Challenges facing ITIL implementation in the local Airline Industry.

The information obtained will not be used for any other purpose other than to enhance the body of knowledge in the Academic Research area of IT service management. I kindly request you to take your time and answer the questions below to the best of your knowledge and thereafter send the same back to me. Your participation is highly appreciated. Thank you

SECTION A: ITIL FRAMEWORK IMPLEMENTATION STEPS IN THE LOCAL AIRLINE INDUSTRY

The following questions relate to you and your organizations experience while adopting and implementing ITIL framework. Answer the questions below about the steps taken in the implementation of ITIL by placing a tick (✓) below the appropriate item.

1) Which of the following best describes your position in the Airline?

Senior manager ☐   Line managers ☐   Support staff ☐

2) In Which Division are you stationed?

Information Systems ☐   Finance & HR ☐

Ground Operations & Cargo ☐   Flight Operations ☐

Commercial ☐   Technical ☐

3) Are you aware of your airlines effort to implement ITIL frame work?
Yes ☐   No ☐

4) If your answer in the question above is "Yes", have you been involved in ITIL implementation? Yes   No
☐   ☐

5) If your answer in question 2 is "Yes", for how long have you been involved in the process?
Less than 1 Year ☐   1-2 years ☐

3-4 years ⬜　　　　More than 4 years ⬜

6) In which way(s) have you been involved in the ITIL implementation process?

Decision making (Management) ⬜	Sensitization/Awareness	⬜
Design ⬜	Coordination	⬜
Training ⬜		

Others,(Specify)_____

7) Please rate the degree to which you agree/disagree with the following statements and give comments for your answer.

Description	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Justification
ITIL led to improved IT services through the use of proven best practice processes at the airline	○	○	○	○	○	
ITIL led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time at the airline	○	○	○	○	○	
ITIL led to improved resource management and usage, improved decision making and optimized risk management at the airline	○	○	○	○	○	
ITIL led to improved productivity as well as improved use of skills and experience at the airline.	○	○	○	○	○	
ITIL adoption led to an improved risk management practice.	○	○	○	○	○	
It is unclear if there is a standard way to treat risk and how to implement risk management process in ITIL	○	○	○	○	○	
ITIL risk management should be mapped with other standards and frameworks to build a single, integrated body of work.	○	○	○	○	○	
It is not advisable to adopt multiple frame works as they are costly and complex to implement	○	○	○	○	○	

SECTION B. DEGREE OF ITIL FRAMEWORK IMPLEMENTATION IN THE LOCAL AIRLINE INDUSTRY

(a) To what degree was the following items implemented as part ITIL implementation process? Please tick (✓) (with the guidance of the key below) in column that best describes your implementation experience.

1 = Minor   **2** = Moderate   **3** = Don't know

4 = Large   **5** = Very large

Item implemented	Degree of Implementation of ITIL				
	1	**2**	**3**	**4**	**5**
i). Service strategy					
ii). Service Design					
iii). Service transition					
iv). Service operation					
v). Service continual improvement					

SECTION C: DEGREE OF INTEGRATION OF RISK MANAGEMENT INTO ITIL FRAMEWORK IN THE LOCAL AIRLINE INDUSTRY

(a) To what degree has risk management been integrated in ITIL processes listed in table below? Please tick (✓) (with the guidance of the key below) in column that best describes your implementation experience.

1 = Minor   **2** = Moderate   **3** = Neutral

4 = Large   **5** = Very large

Process	Degree of integration				
	1	2	3	4	5
Strategy Management					
Service Portfolio management					
IT financial management					
Demand management					
Business Relations Management					
Service catalogue Management					
Service level management					
Capacity management					
Availability management					
IT continuity management					
Supplier management					
Information management					
Transition planning and support					
Change management					
Knowledge management					
Service assets and configuration management					
Release and deployment management					
Service Testing and deployment					
Change evaluation					
Operation Management					
Event management					
Incident management					
Request fulfillment					
Problem Management					
Access management					
7 step improvement service					
Service measurement					
Service reporting					

b). Please rate the degree to which you agree/disagree with the following statements

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
Successful service strategy implementation would lead to increased customer satisfaction as well as a small variance between actually spent and approved budget .	◯	◯	◯	◯	◯
Gaps in disaster preparation and lack of value for money could are mainly as a result of poor service design	◯	◯	◯	◯	◯
Increased number of performance measures is an indicator of a well of a well adopted a well adopted service transition process	◯	◯	◯	◯	◯
High number of access attempt is an attribute of a well implemented service operation.	◯	◯	◯	◯	◯
A high percentage of new service is a byproduct of a well structured continual service improvement	◯	◯	◯	◯	◯

SECTION D: CHALLENGES AFFECTING ITIL FRAMEWORK IMPLEMENTATION IN THE LOCAL AIRLINE INDUSTRY

(a) Please indicate by ticking in the appropriate column (with the guidance of the key below) the extent to which ITIL has been affected by the following:-

1 = Minor   **2** = Moderate   **3** = Neutral   **4** = Large

5 = Very large

Description	Extent of effect				
	1	2	3	4	5
High cost in implementing the framework					
Organizational Culture - Staff resisting change					
Lack of support from top management					
Lack of continuous training in ITIL					
Lack of support from top management					
Lack of planning in the implementation of ITIL					
Lack of risk management integration					
Size of the organization					
Organizational structure					
Complexity of the processes within the airline					
Lack of qualified personnel to lead the ITIL process					
Lack of adequate infrastructure e.g. workspace, equipment					

b) What actions would you recommend for effective risk management in view of ITIL at the airline?

………………………………………………………………………………………………

………………………………………………………………………………………………

c) What is your expectation(s) from effective risk management in ITIL at the airline?

Reduce financial loses   Improve communication with stakeholders

Improved decision making   improve resource allocation

Others (please Specify.

_____

_____

Thank you for sparing your valuable time to answer the above questions.

APPENDIX 2: FOCUS GROUP GUIDE

1. Discuss the level of implementation of the following ITIL lifecycle modules at the airline.
    a) Service Strategy
    b) Service Design
    c) Service Transition
    d) Service Operation
    e) Service Continual Improvement

2. Rate the degree to which you agree/disagree to the following statements (give a justification to each response)

Description	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Justification
ITIL led to improved IT services through the use of proven best practice processes at the airline	◯	◯	◯	◯	◯	
ITIL led to improved user and customer satisfaction with IT Services, financial savings from reduced re-work or lost time at the airline	◯	◯	◯	◯	◯	
ITIL led to improved resource management and usage, improved decision making and optimized risk management at the airline	◯	◯	◯	◯	◯	
ITIL led to improved productivity as well as improved use of skills and experience at the airline.	◯	◯	◯	◯	◯	
ITIL adoption led to an improved risk management practice.	◯	◯	◯	◯	◯	
It is unclear if there is a standard way to treat risk and how to implement risk management process in ITIL	◯	◯	◯	◯	◯	
ITIL risk management should be mapped with other standards and frameworks to build a single, integrated body of work.	◯	◯	◯	◯	◯	
It is not advisable to adopt multiple frame works as they are costly and complex to implement	◯	◯	◯	◯	◯	

3. Discuss the extent of the following risk indicators on the respective ITIL components at the airline

process	Potential Risk	Key Risk Indicator
Strategic management	Definition of unstructured or un-competitive strategy.	• Decrease/ Increase of customer's satisfaction.
Service portfolio management	Creation of a service that is not aligned with the organization's strategy or customer needs.	• Decrease/Increase of customer's satisfaction. • Decrease /Increase of customers.
Supplier management	Expensive but poor services No value for money	• Number of agreed UCs. • Number of contract reviews. • Number of suppliers and the information about them.
Information Management	Lack of appropriate information on future plans and strategies.	• Gaps in Disaster Preparedness. • Time lapse from identification of risk to the implementation of a suitable continuity mechanism.
Evaluation Management	Developing standard performance measures and measurement methods across projects and suppliers.	• Number of performance measures created. • Number of performance measures documented.
Access management	Unable to restrict access rights to unauthorized users.	• Number of access attempts. • Number of authorized access attempts. • Number of unauthorized access attempts.
7-Step Improvement service	Services became static throughout time.	• Percentage of new services.
Service Reporting	Inability to sustain continuous reporting.	• Percentage of organization goals tracked/reported.

What actions would you recommend for effective risk management in view of ITIL at the airline?

APPENDIX 3: GLOSSARY OF TERMS

Mpesa: This refers to the mobile money transfer platform provided by Safaricom (a public listed telecommunications company in Kenya)

Yu – cash: This refers to the mobile money transfer platform provided by YU - Telecoms (a public listed telecommunications company in Kenya)

Airtel Money: This refers to the mobile money transfer platform provided by Airtel (a public listed telecommunications company in Kenya)

UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

Telephone: 4447870/4444919/4446544   P. O. Box 30197
Telefax: 4447870   Nairobi
Email: moturi@uonbi.ac.ke   Kenya

          22-Jul-13

TO WHOM IT MAY CONCERN

TITUS KITAVI P56/P/7277/2005
MSC RESEARCH PROJECT

The above named is bona fide student in the MSc in Information Systems of this University. As part of the requirement for the programme, the student is carrying out a final project entitled: **Integrating Risk Management in the ICT Service Management Frameworks: The Case of ITIL Service Management Framework in the Local Airline Industry.** This project involves gathering relevant information from your organization. We are therefore requesting that your accord the student the necessary assistance. Your assistance will be highly appreciated.

Yours faithfully,

Christopher A Moturi
Deputy Director
School of Computing & Informatics