UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

IT Risk Management in E-Governance: Case for the Cargo Clearance Process in Kenya

By

KENNEDY KARANJA MUCHIRA

P54/65108/2013

Supervisor

CHRISTOPHER MOTURI

November 2014

A project report submitted in partial fulfillment of the requirements for the award of Masters of Science in Information Technology Management of the University of Nairobi.

ACKNOWLEDGEMENT

I am grateful to my supervisor Mr. Christopher A. Moturi for the guidance, advice and motivation throughout the research process. I thank the staff of the Kenya Revenue Authority who responded to my questionnaires. I specifically acknowledge the efforts of Mrs. Lucy Butichi, Charles Nganga and Eva Msagha, in facilitating collection of data from their respective departments. To my parents, Mr. and Mrs. Muchira, thank you for your constant prayers and support.

DECLARATION

This project is my original work and to the best of my knowledge this research work has not been submitted for any other award in any University

Kennedy Karanja Muchira: _____ Date: _____
(P54/65108/2013)

This project report has been submitted in partial fulfillment of the requirement of the Master of Science Degree in Information Technology Management of the University of Nairobi with my approval as the University supervisor

Christopher A. Moturi: _____ Date: _____
Deputy Director
School of Computing and Informatics

ABSTRACT

Governments all over the world are embracing e-governance by integrating information technology in their operations in an effort to improve quality of services, accountability and efficiency. Traditionally IT risk management has been treated as a technical matter and relegated to technical specialists. The criticality of IT in government operations warrants the management of IT risk by all stakeholders led by organizations' top management. This research builds a case for a process model and tool for the managing IT risk in e-governance. Existing risk management frameworks and standards were evaluated and the Risk IT framework was identified as the most appropriate guiding framework for the process. The framework was customized and used to assemble a process model after which a system prototype developed to guide its implementation. To demonstrate the use of the process model and the tool, an assessment of IT risk was carried out on the cargo clearance process in Kenya. Using the data obtained in the risk assessment, the tool provided an analysis of the IT risk levels in each IT process as well as the overall cargo clearance process. Major sources of risk and quick-wins were also identified and relevant recommendations made. The process model and tool were found to offer very significant benefits to the government and the public and were therefore recommended for adoption.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

COBIT	**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology
IT	**I**nformation **T**echnology
ISACA	**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation
ISO	**I**nternational **O**rganization for **S**tandardization
KPA	**K**enya **P**orts **A**uthority
KRA	**K**enya **R**evenue **A**uthority
OBRiM	**O**ption **B**ased **Ri**sk **M**anagement
ROA	**R**eal **O**ptions **A**nalysis

CHAPTER 1
INTRODUCTION

1.1.Background

E-governance refers to the use of IT to improve the ability of government to address the needs of society (Sharma, Mishra, Mishara, 2011). Governments all over the world are endeavoring to integrate Information Technology (IT) in their operations to transform delivery of services by improving quality of services, accountability and efficiency. Government departments and agencies involved in the cargo clearance process in Kenya have implemented enterprise applications to aid in data processing and information storage. It is now possible for the systems in these organizations to 'co-operate' with each other by sharing data. This allows for cross-verification of data that originates from other organizations and information sharing when reporting. (Moturi, Kinu, Kahonge, 2013) determined that stakeholders in this process have endeavored to integrate their enterprise systems with the aim of Eliminating time wasted on data transmission, Automating the bulk of data validation tasks, Minimizing the duplication of the same datasets in the systems used by different organizations and Improving data integrity by providing a way of checking for the correctness of the same from the base System, i.e. the first system in which the data was created. The all-encompassing use of IT has provided significant benefits, but it also involves risk.

1.2.Problem Statement

IT risk has largely been considered a technical issue and therefore its management is relegated to technical specialists. The criticality of Information Technology in government operations warrants the elevation of IT risk to the level of other key business risks, such as strategic risk or environmental risk since it also affects the organization's ability to achieve strategic objectives. Risk management process models developed for business present a challenge when being translated for use by government mainly because the government's primary objective is promoting the welfare of its citizens as opposed to profit maximization. There is therefore a need for a process model and tool to guide the process of comprehensively defining and treating risks related to the use of IT in government operations.

1.3. Objectives

1. Identify the most appropriate framework for use in the cargo clearance process in Kenya
2. Propose a process model for IT risk management based on the identified framework
3. Develop a tool to guide the implementation of IT risk management using the proposed process model
4. Demonstrate the use of the proposed process model and tool in IT risk management in the cargo clearance process in Kenya.

1.4. Research Questions

1. Which of the existing risk management frameworks is the most appropriate for use in the cargo clearance process in Kenya?
2. What sequence of activities can optimally achieve IT risk management in the cargo clearance process in Kenya?
3. What tool can guide the implementation of IT risk management in the cargo clearance process in Kenya?
4. What IT-related risks exist in the cargo clearance process in Kenya?
5. How are stakeholders in the cargo clearance process addressing IT risk?

1.5. Scope of Research

The principal aim of the research was to propose a process model for IT risk management in e-governance and develop a tool to guide the process, manage the information collected and generate the relevant reports. The Cargo Clearance Process of the Customs Services Department of Kenya Revenue Authority was used to demonstrate the process.

CHAPTER 2
LITERATURE REVIEW

2.1. Key Concepts

Risk is the effect of uncertainty on objectives. Effect in this case refers to deviation from the expected outcome whether positive or negative (ISO guide 73, 2009). Risk is established from the combination of the probability of an event and its consequence (ISACA, 2014).

Vulnerability refers to a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threat events (ISACA, 2014)

Threat is anything that is capable of acting against an asset in a manner that can result in harm (ISACA, 2014). It may also be defined threat as a potential cause of an unwanted incident (ISO/IEC 13335, 2004). A threat is therefore a set of circumstances that has the potential to cause harm.

Exposure refers to the potential loss to an area due to the occurrence of an adverse event (ISACA, 2014). Exposure therefore refers to the extent of loss the organization has to face when a risk materializes.

Risk appetite is the broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (ISACA, 2014).

Risk tolerance is the organization's or stakeholder's readiness to bear the risk after treatment in order to achieve its objectives (ISO guide 73, 2009).

IT Risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT (ISACA (2009), the Risk IT Framework).IT risk is a component of the enterprise risk. All other risk categories have an IT-related component as depicted in Figure 1 e.g. a failed IT system may provide inaccurate information to management leading to an organization filing erroneous tax returns and incurring legal penalties (compliance risk).

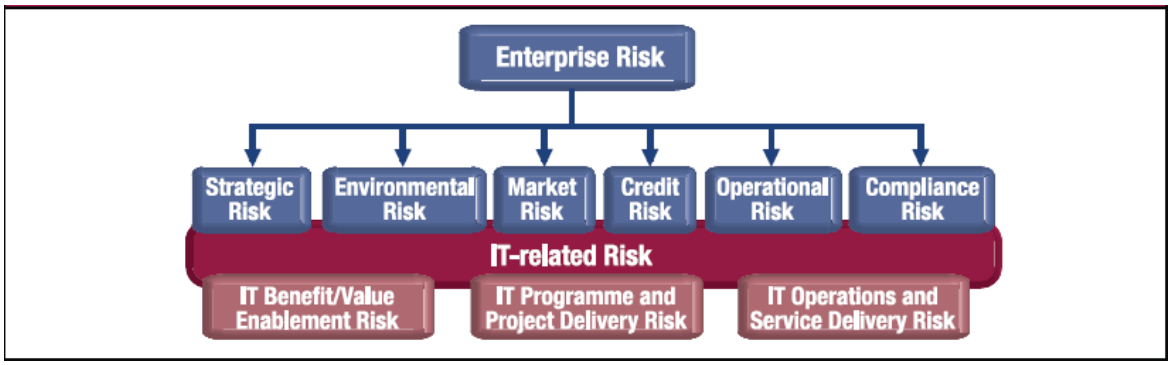


Figure 1: IT Risk in the Risk hierarchy

Source: ISACA (2009), The Risk IT Framework

2.2. Review of Previous Studies

(Institute of risk management, 2010) developed a risk management process based on ISO 31000 with the following components:

Risk assessment - It begins with the identification of the factors that are most critical to the achievement of the organization's objectives. These are defined in terms of opportunities and threats. The risks are then ordered in terms of priority and this is used to determine the resource allocation for risk treatment.

Risk treatment - This involves identifying and implementing controls to reduce the impact or eliminate the risk. Approaches for risk treatment include: risk avoidance and risk transfer. The cost of risk treatment should always be compared to the anticipated benefit to ensure a net gain. Controls with the highest net gain should be given highest priority.

Feedback mechanisms - This involves monitoring and reviewing of the organization's performance as well as that of individual components. It is also important to maintain communication amongst stakeholders on issues affecting their areas of interest.

The thinking and intuition of IT managers correspond well with the logic of option-based risk management as observed by (Benaroch, Lichtenstein, Robinson, 2006) in their empirical study.

For example, for risk related to the size and complexity of an investment some mappings prescribe the use of the stage, prototype, lease and outsource options.

The National Stock Exchange of India Limited implemented IT risk with an aim of risk assessment into IT operational and governance processes as described by (Sunil Bakshi, 2011).
A comparative study of existing standards and frameworks was carried to identify the most suitable guiding framework for the process. The Risk IT framework was selected for the following reasons: It provides granular guidance on risk management processes covering all traditional risk management processes (identification, risk assessment, risk response, risk treatment and risk monitoring);It focuses on linking IT risk with business objectives rather than IT assets; It is the only framework that provides detailed processes for IT risk governance; It is focused on building risk scenarios (also provide list of generic scenarios) that help in directly linking risk management with business processes. The implementation of risk management involved development of risk registers for business functions and defining an aggregation process to arrive at an organization-level risk profile. The Risk IT framework helped NSE in presenting a uniform view of IT risk to stakeholders; encouraging stakeholders to participate in the process by using scenario analysis which is easily understood; defining a monitoring process for continuous updating of changes in the risk profile and promoting acceptance by risk owners. An Excel-based tool was developed for updating the risk profile.

MetLife Inc. leveraged the Risk IT framework to create a MetLife-specific IT Risk Management Framework. They customized it to a framework that used internal terminology to ensure the document could be easily understood and used globally across the enterprise. The customized framework provides for the consistent handling of all IT risk management aspects and integrating them with business operational risk activities. It is not a procedure, but rather a description of what processes and activities management should strive to mature. It maintains the Risk IT domains (risk governance, risk evaluation and risk response) and also provides details on the processes and activities to be carried out (MetLife Inc., 2010).

2.3. Review of Existing Risk Management Frameworks and Standards

To guide the development of the process model, a risk management framework was required to establish connections between observations and facts and to identify key concepts and the relationships among them.

2.3.1. The Risk IT Framework

This framework is aimed of encouraging the inclusion of IT risk management at the highest level of corporate decision making. This is achieved by integrating IT risk Management into the overall ERM. It provides guidelines on how to manage IT-related risk including non-technical aspects. It also provides for the communication of IT-related risks and associated controls to both IT and non-IT personnel. Cost effectiveness of controls is also taken into account to ensure that they deliver measurable value to the enterprise (ISACA, 2009).

Figure 2 : The Risk IT Framework

Source: ISACA (2009), The Risk IT Framework

The framework consists of three domains:

Risk governance: It ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. This is achieved by integrating IT RISK Management with the ERM, establishing and maintaining a common risk view and making risk-aware business decisions

Risk evaluation: This involves identifying IT-related risks and opportunities and presenting them in business terms that can be understood by all stakeholders. Determining the business impact of each risk provides an objective basis for communication and risk response. (Fischer, 2011) identified the identification of relevant risks from a list of things that could go wrong as one of the biggest challenges in IT risk management. Scenario analysis helps in tackling this challenge by providing realism in IT risk Management. Scenario analysis involves developing IT risk scenarios and estimating their likelihood of occurrence as well as business impact. Scenario analysis has been identified as a centerpiece of the Risk IT framework. (ISACA, the Risk IT Practitioner Guide, 2009)

Risk Response: This is aimed at influencing the current scenario to ensure that the risks are maintained within the enterprise's risk appetite. An organization's options include Risk avoidance (steering clear of the conditions that result in the risk), Risk Reduction/Mitigation (reducing the likelihood or impact of the risk), Risk sharing/Transfer (transferring all or part of the risk) and Risk acceptance (taking no action relative to a particular known risk.).

2.3.2. ISO 31000: Risk Management

This is a generic framework developed by (International Organization for Standardization, 2009) for use by organizations in developing, implementing and continuously improving the risk management process. The framework aids the organizations in incorporating risk management into the overall organization management but does not prescribe a risk management system.

It consists of 5 major components:

Mandate and commitment: This is aimed at gaining commitment and endorsement right from top management. This is achieved by aligning the objectives for risk management with the business objectives of the organization. This paves way for allocation of resources and assignment of responsibilities and accountabilities.

Design of framework for managing risk: This begins with the understanding the organization and its context. A risk management policy is then established for the integration of risk management into organizational processes. Resource requirements are determined with keen interest on competence and identification of who is accountable for each aspect of risk management. Plans are also put in place for communication and reporting to stakeholders.

Implementing risk management: The processes defined in the risk management policy are rolled out in all relevant functions and processes of the organization. This should however be preceded by training and information sessions for all affected parties.

Monitoring and review of the framework: Performance measures for the risk management process are put in place and periodic reviews carried out to determine progress as well as deviation from expected outcomes. Stakeholders should also be consulted to ensure that the risk management framework remains appropriate.

Continual improvement of the framework: Information obtained from performance reviews is used to make adjustments in the process in an effort to help the organization manage risks better.

ISO also developed a process for the management of risk.

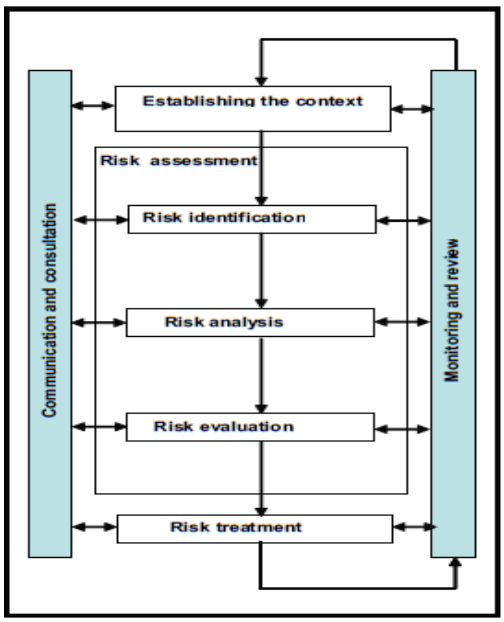


Figure 3 : ISO Risk Management Process

Source: International Organization for Standardization, 2009, Risk Management - Principles and Guidelines

Establishing the context: understanding the internal and external environment. Context includes organizational culture, politics, policies, stakeholder perceptions, legal framework among other aspects.

Risk assessment: This is a broad area that covers identifying sources of risk, areas of impacts, causes and their potential consequences (Risk identification); developing an understanding of the risk and the factors affecting the likelihood and impact of the risk (Risk analysis) and determining if treatment is necessary based on the outcome of risk analysis (Risk evaluation).

Risk treatment: This covers all efforts to reduce the impact or likelihood of risk. It include weighing different options based on anticipated benefits and cost-effectiveness, planning and scheduling of actions, executing the plan , evaluating if the residual risk is within the tolerance limits of the organization as well as the relevant communication to stakeholders. Options for treatment include: transferring/sharing, avoiding the risk and accepting the risk.

Monitoring and review: This is aimed at establishing if the controls that have been put in place are efficient and effective as well as identifying areas of improvement. Changes in the internal and external context may also be detected and emerging risks identified.

Communication and consultation: At each step in the process, stakeholders should be kept informed and their views sought on their perceived performance of the process and proposals for improvement.

2.3.3. COBIT 5 for Risk

COBIT 5 provides a framework to guide enterprises in creating optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. Control Objective PO9.1 provides a framework for managing risk using the following steps: Risk identification; Impact assessment; Probability assessment (likelihood of occurrence); Development of control strategies. It encourages the alignment of the IT risk management objectives with those of the enterprise risk management (ISACA, 2012).

COBIT 5 for Risk, builds on the COBIT 5 framework by focusing on risk and providing more detailed and practical guidance for risk professionals and other interested parties at all levels of the enterprise. It also pays attention to the quantification of risk in order to justify the cost of mitigation COBIT 5 for Risk also offers the benefit of stakeholder (both internal and external)

involvement in risk management since COBIT 5 on which it builds, has stakeholder involvement as one of the major drivers (ISACA COBIT 5 for Risk, 2013)..

Figure 4 summarizes the entire process.

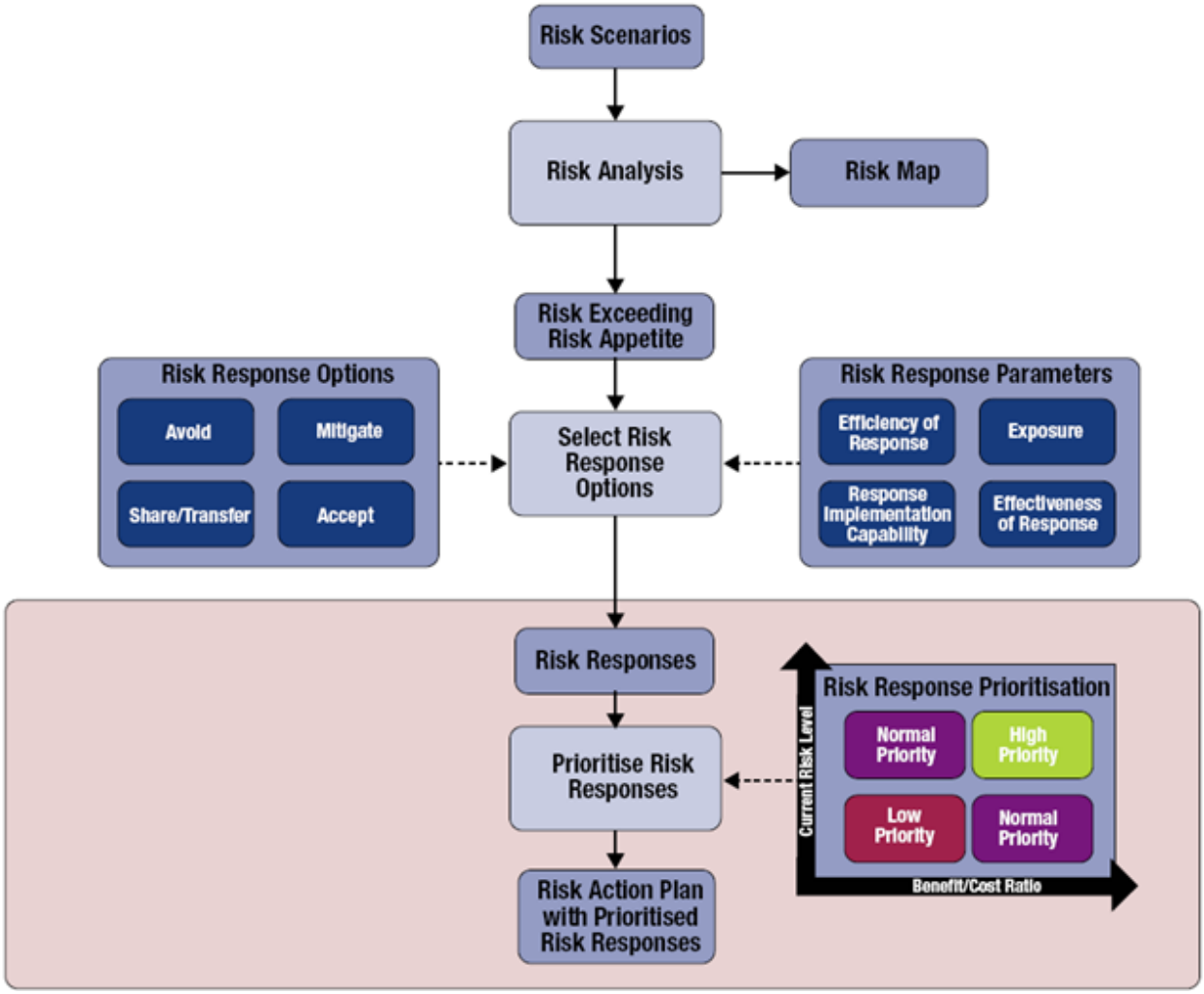


Figure 4: COBIT Risk Management Process

Source: ISACA (2013), COBIT 5 for Risk

Risk scenarios are identified and defined using the top-down (starting from the overall business objectives and performing an analysis of the most relevant and probable IT risk scenarios impacting the business objectives) or bottom-up approach (using a list of generic scenarios to define a set of more concrete and customized scenarios, applicable to the individual enterprise situation).Risk analysis is carried out to establish the impact and likelihood of each risk. The

resulting risk map is used to identify those risks that exceed the organization's risk appetite and therefore require treatment. Risk response options are selected from a list of generic options (Avoid, Mitigate, Accept and Share/Transfer).This takes into account various parameters associated with each of the options (Efficiency, Effectiveness, and Implementation capability) as well as the risk Exposure level. The existing risk level and the expected benefit /cost ratio are used to prioritize the responses. Finally an action plan is generated from the prioritized risk responses for implementation.

2.3.4. Option Based IT Risk Management (OBRiM) Framework

This framework helps managers in to embed various options in IT investments in order to control risks associated with those investments. The framework addresses two major challenges faced in IT risk management; Approaching risk management from an economic perspective and choosing adequate mitigations and combining them to effectively address specific risks (Benaroch, Lichtenstein, Robinson, 2006).

The framework is based on the idea that in an attempt to maximize IT investment value a manager should size up relevant risks, build up flexibility into the investment to an extent that the flexibility is expected to add value and continually evaluate new information and take corrective action within the bounds of the flexibility.

OBRiM formalizes this idea by viewing real options as high-level risk mitigation strategies for building different forms of flexibility necessary to deploy corrective actions when risk occurs. It helps to find a combination of options that adds the most value to the risks specific to an investment. The option types OBRiM considers are: defer, pilot, prototype, stage, alter-scale, abandon, outsource, lease and strategic growth.

(Benaroch, 2002) developed an option based approach to managing IT investment Risk comprising of the following steps: Define the investment and its risks - defining the investment objectives as well as resource requirements of an initial solution identified; Recognize shadow options - determining the options that the investment can embed to control the identified risks .e.g. technological risk can be controlled by the defer, lease and abandon options; Design alternative investment configurations - identifying alternative ways to configure the investment using different subsets of the recognized shadow options and then assessing the risk trade-offs

between the identified configurations; Evaluate Options and Investment Configurations - The most valuable configuration is finally selected.

2.4. Theoretical Framework

2.4.1. Framework Selection

From the literature reviewed, the Risk IT framework was selected due to the following main reasons:

i. It focuses on "ends" by helping in identifying, governing and managing IT risk while COBIT focuses on the "means" by providing a set of controls for managing IT risk.
ii. Like ISO 31000 and COBIT, Risk IT covers identification, assessment and response to risk.
iii. It relates IT risk to business objectives rather than IT assets.
iv. It is the only framework that avails processes for governing IT risk.
v. It identifies risks by generating risk scenarios which are easily understood by stakeholders, therefore encouraging participation.
vi. It provides for the monitoring of risk
vii. It provides for the integration of IT risk management in operations ensuring that it is a continuous process.

2.4.2. Framework Customization

Elements of the framework were customized to clearly define the domain areas and make them easily understood by stakeholders.

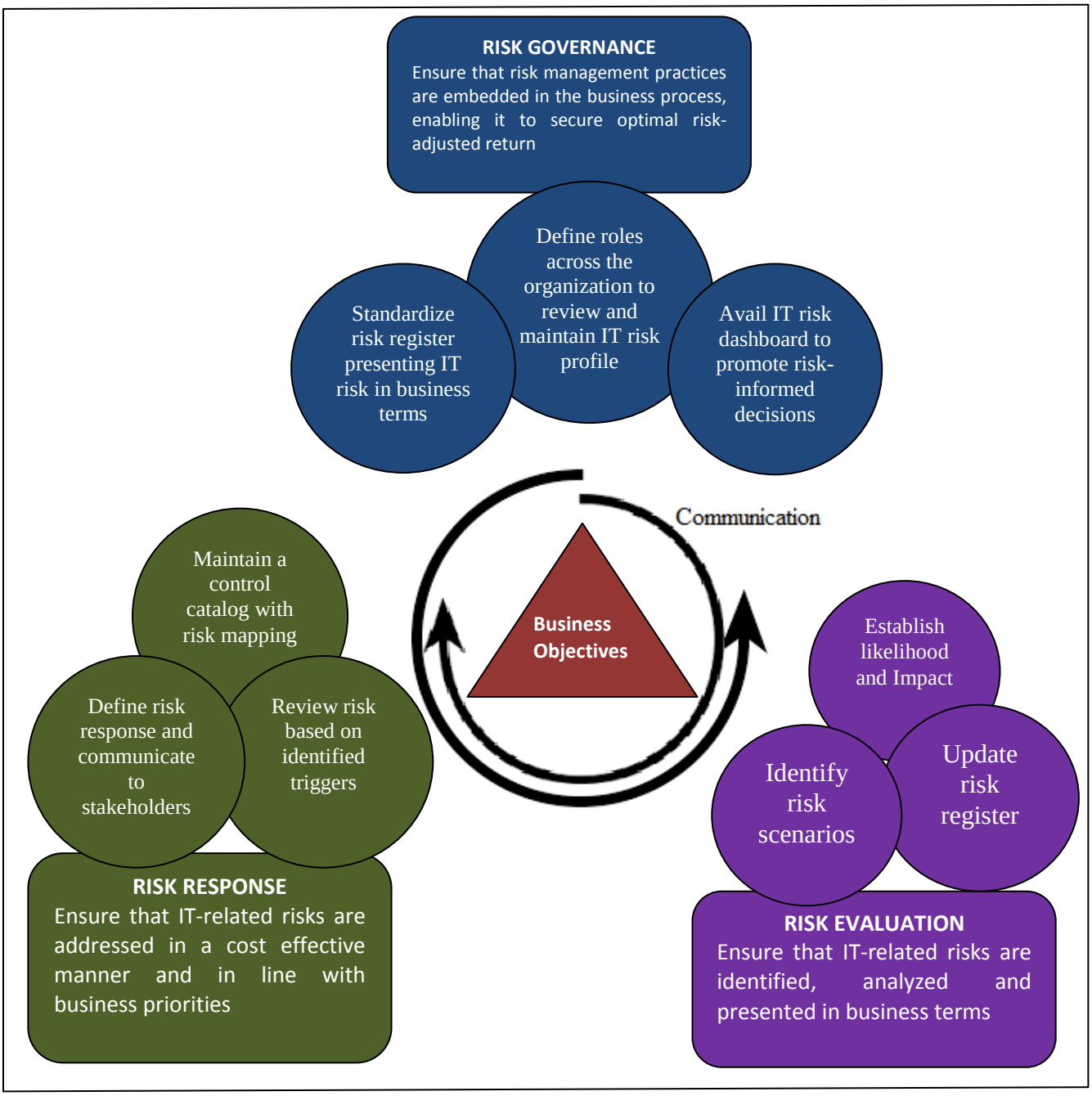


Figure 5 : Customized IT Risk Management Framework

2.5. The IT Risk Management Process Model

Step 1: Defining Risk Universe

The research determined that risks facing the cargo clearance process in Kenya can be broadly be classified as Financial, Infrastructure, Operational or Reputational risk. Drivers for each of the risk are either internal or external to Kenya Revenue Authority. IT being a key enabler of the business process has resulted in there being an IT-related component in each of the risk areas.

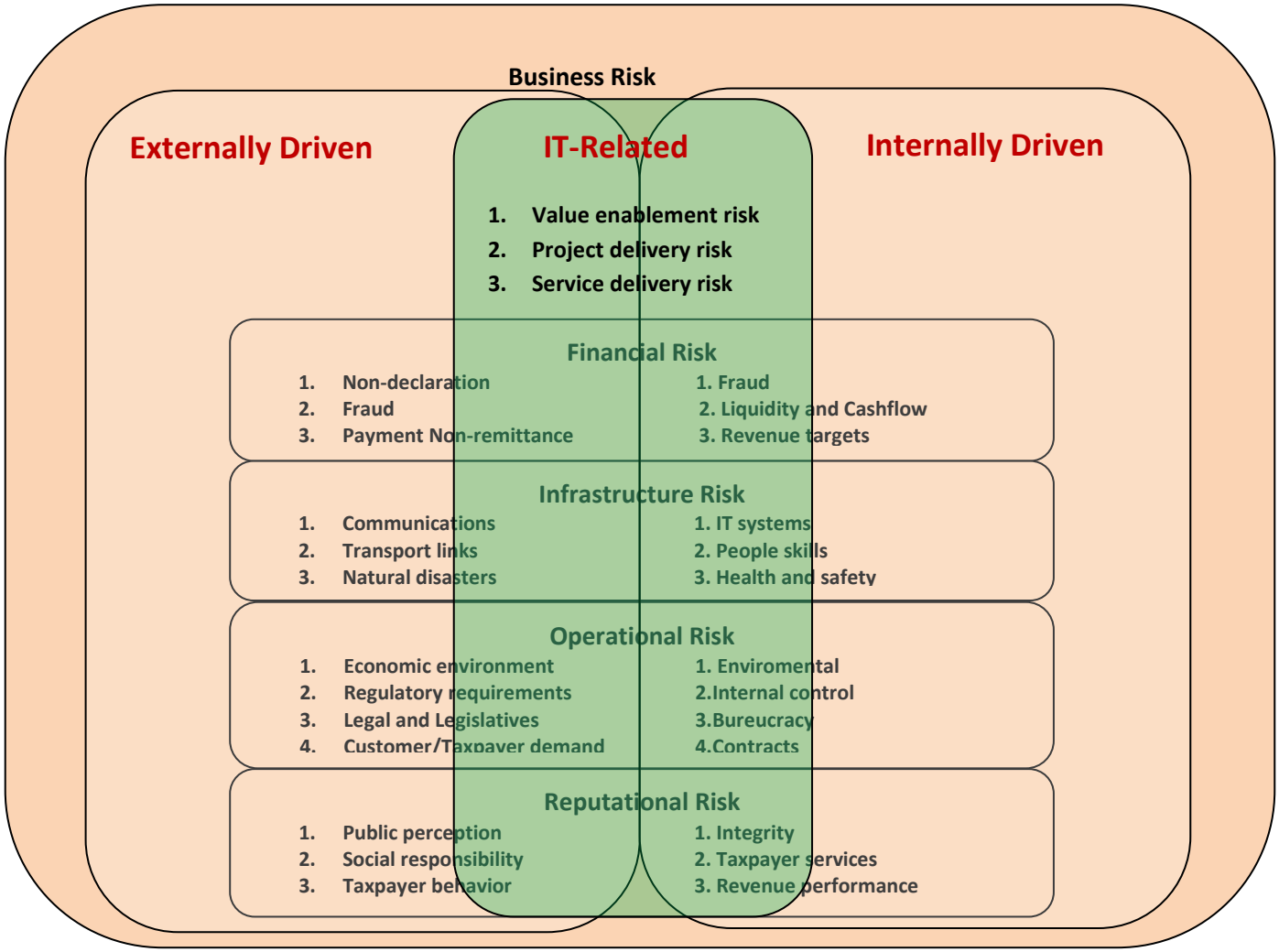


Figure 6 : Risk Universe

Step 2: Mapping IT Risk Management Process

The IT risk management process covers preparation of masters (risk scenario catalogue, control catalogue, risk and controls mapping) based on the risk management framework, updating the masters based on the business processes and their interactions with IT and presenting the risk profile for each IT process.

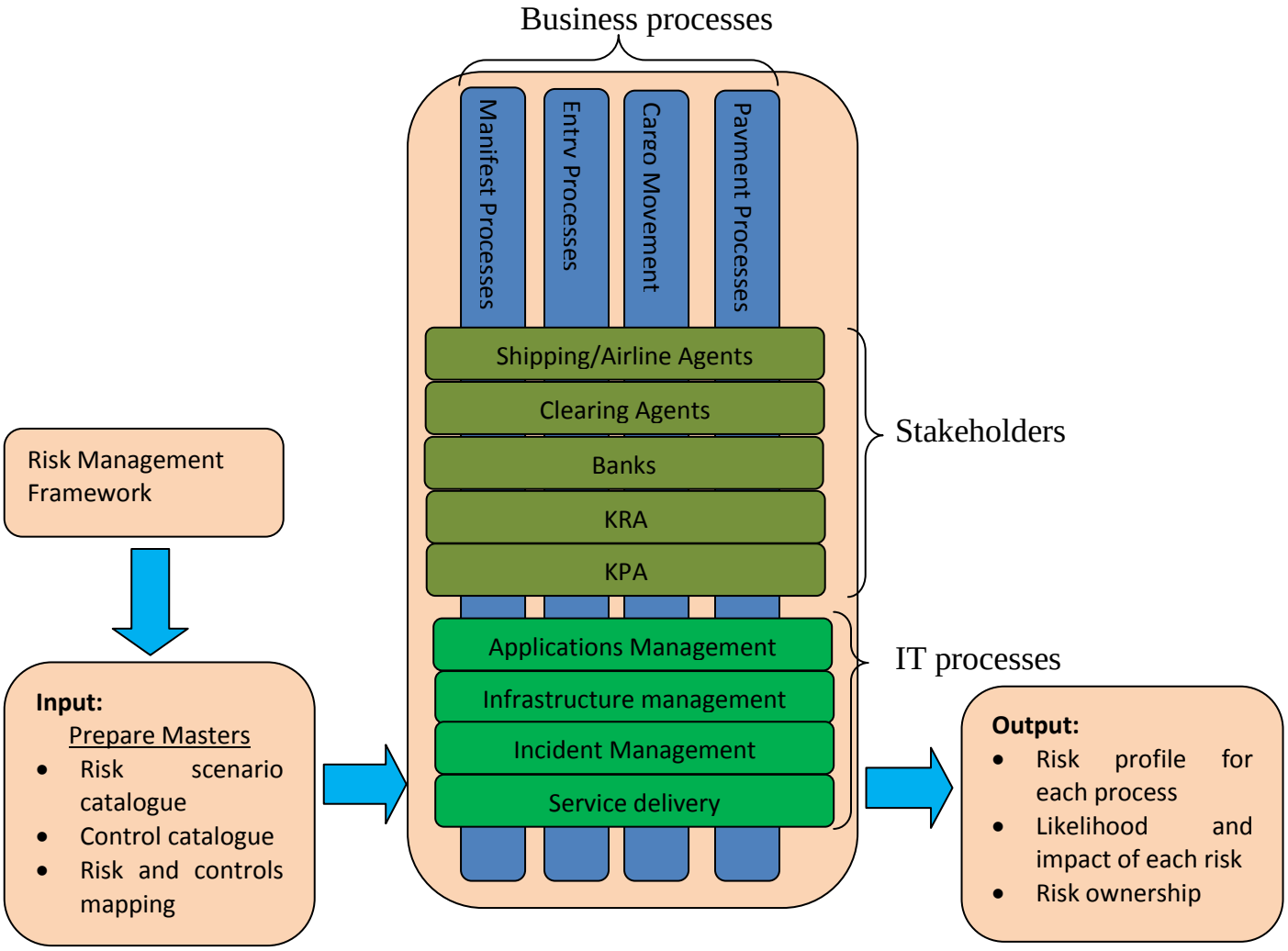


Figure 7 : Risk management process mapping

Step 3: Defining Risk Appetite and Tolerance

Risk appetite and tolerance are defined as a factor of risk likelihood and consequence as shown in Table 1.

Table 1: Likelihood Scale

Likelihood					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Consequence				

KEY:

- Further action required with top level escalation and urgency
- Further action required with medium escalation and urgency
- No further action required(only monitoring)

Step 4: Selecting Applicable Risk Scenarios

Scenario analysis is used to identify IT-related risk scenarios applicable to the cargo clearance process. The Risk IT framework provides two approaches: the Top-Down approach which involves starting with business objectives and identifying and analyzing IT risk scenarios that would hinder their achievement; and the Bottom-Up approach where a list of generic scenarios is used as a basis for defining customized IT risk scenarios for an organization or business process. The top down approach was selected to ensure that the focus of risk management is to maximize the ability to achieve business objectives.

Each risk is assigned a risk owner and the key risk indicator is defined.

Step 5: Estimating the Business Impact

The financial impact of identified risks is estimated in terms of Cost amount and/or revenue implication. Non-financial impact is estimated in terms of reputation, regulatory/legal consequences, customer satisfaction, staff satisfaction, IT efficiency and/or quality of service delivery. The consequence scale described in Table 2 is used to assign the business impact level.

Table 2 : Consequence Scale

Level	Description	Amount (Cost)	Amount (Revenue)	Reputation	Regulatory /Legal	Customer satisfaction	Staff satisfaction	IT efficiency	Quality of service delivery
5	Fundamental	Losses exceeding 100Million:All fraud Cases:	>1% of revenue per day/annual /transaction: All fraud Cases	Prominence by media = All Mainstream media houses: Coverage of media = front/headline news: Length of time on media = 1week:	Breach laws resulting in loss of over 10Millon; Prohibited goods clearing	Critical impact to customers, service time +60mins, Grievances > 500 per week	resignations over 50% of staff; Staff complaint over 100; staff grievances over 50% ;	Critical service unavailability >24hours, Non-critical service unavailability < 5days	clearing days>10days; Transfer over 5days;
4	Major	Losses between 50 – 100Million; Cost of collection greater than	0.5% - 1% of revenue per day/annual/transaction	Prominence by media = 75% of Mainstream media houses; Coverage of media = not on front or not on headline news; Length of time on media = 5days;	Breach laws resulting in loss of 5 - 10Million; Clearing unlicensed goods.	Substantial customer disruption, grievances > 300 per week; service time +45mins	resignations 30-50% of staff; Staff complaint 50-100; staff grievances 25-50%	Critical service unavailability between 6-24hours, Non-critical service unavailability < 4days	clearing days 8-10days; Transfer 4days;
3	Moderate	Losses between 25 – 50Million;	0.1% - 0.5% of revenue per day/annual/transaction	Prominence by media = 50% Mainstream media houses; Coverage of media = not on front or not on headline news; Length of time on media = 3days;	Breach laws resulting in loss of 2 - 5Million	Conspicuous customer disruption; grievances > 200 per week; service time +30mins.	resignations 15-30% of staff; Staff complaint 30-50; staff grievances 15-25%	Critical service unavailability between 2-6hrs; Non-critical service unavailability < 3days	clearing days less than 5-8 days; Transfer 3days;
2	Minor	Losses between 5 – 25Million;	0.01% - 0.1% of revenue per day/annual/transaction	Prominence by media = 25% Mainstream media houses or magazines; Coverage of media = Opinions/letters/cutting edge/small articles/watchman;	Breach laws resulting in loss of below 2Million	Minimal customer disruption, grievances > 100 per week; service time +20mins	resignations 5-15% of staff; Staff complaint 20-30; staff grievances 5-15%	Critical service unavailability < 30mins-2hrs; Non-critical service unavailability < 2days	clearing days less than 5days; Transfer 2days;
1	Insignificant	Losses below 1millon;	< 0.01% of revenue per day/annual/transaction	Negative news on non-official media; Street-talk, rumors	No regulatory breach	No customer disruption, grievances < 100 per week, service time 10-20mins	resignations <5% of staff; Staff complaint <20; staff grievances <5%	Critical service unavailability < 30mins; Non-critical service unavailability < 1day	clearing days less than 2days;Transfer 1day;

Step 6: Establishing the Likelihood

The likelihood of the identified risks is estimated and expressed in terms of the indicative frequency or probability. The likelihood scale described in Table 3 is used to assign the likelihood level based on the estimates.

Table 3 : Likelihood Scale

		Options for determining the Likelihood	
Level	**Description**	**Option 1: Indicative Frequency**	**Option 2: Indicative Probability**
5	Almost Certain	Likely to arise within the next 0 - 3 months	Strong probability (>90%) that the risk event will occur
4	Likely	Likely to arise within the next 3 - 6 months	Probable that the risk event will occur (55 – 89%)
3	Possible	Possible to occur within the next 6 months - 1 year	Risk event could potentially take place (25 – 54%)
2	Unlikely	Possible to occur within the next 1 - 5 years	Risk event not expected to happen, however an outside chance exists (5 -24%)
1	Rare	Not likely to happen within the next 5 -10 years or only in exceptional circumstances.	Not likely to happen within the next 5 -10 years or only in exceptional circumstances (0-4%)

Step 7: Establishing Inherent Risk Level

For each of the identified risk, business impact as well as likelihood of occurrence is estimated on the assumption that no controls have been implemented in response to this risk. The impact and likelihood levels are then derived from the consequence and likelihood scales respectively based on these estimates. The inherent risk level is the product of the resulting impact and likelihood levels

Step 8: Identifying Existing Controls

This involves identifying measures that have been implemented in an effort to reduce the likelihood of the risk (Risk Avoidance) , reduce the business impact of the risk (Risk Reduction/Mitigation) or transfer all or part of the consequences of the risk to a third party.

Step 9: Current Risk Analysis

Where risk avoidance controls exist, the likelihood is expected to have reduced while where risk transfer and/or mitigation controls exist; the expected business impact is expected to have reduced. The product of the risk likelihood and impact after considering the existing controls represents the current residual risk.

Step 10: Identifying Improvement Actions

Where the current risk level exceeds the organization's risk tolerance level, improvement actions in form of additional controls are identified and prioritized.

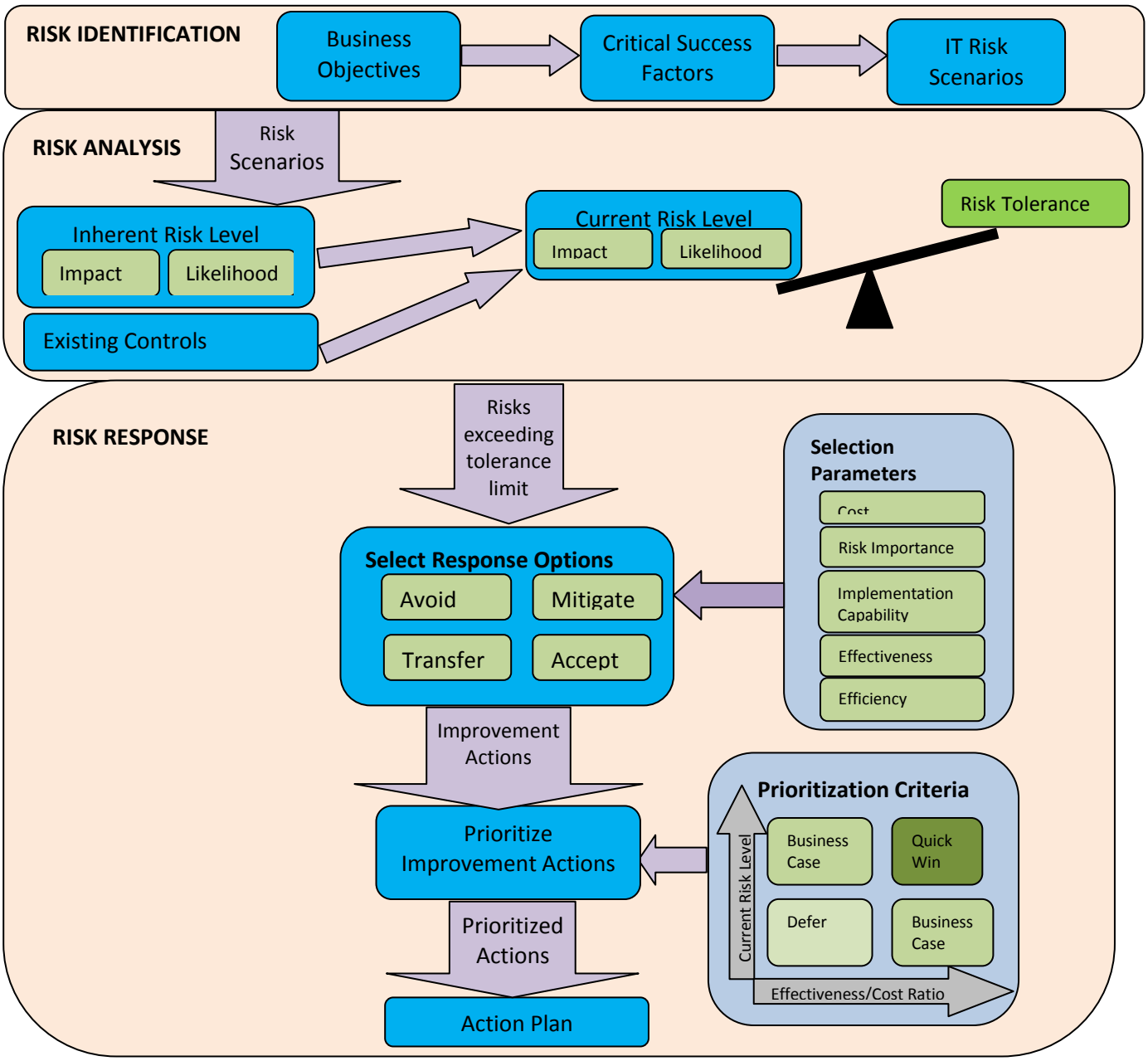


Figure 8 : Risk Identification, Analysis and Response Process (steps 4-10)

Step 11: Continuous Monitoring and Updating

Incidents; changes in IT and business environment; and scheduled assessments were identified as triggers having an impact on risk status and should therefore be continuously monitored

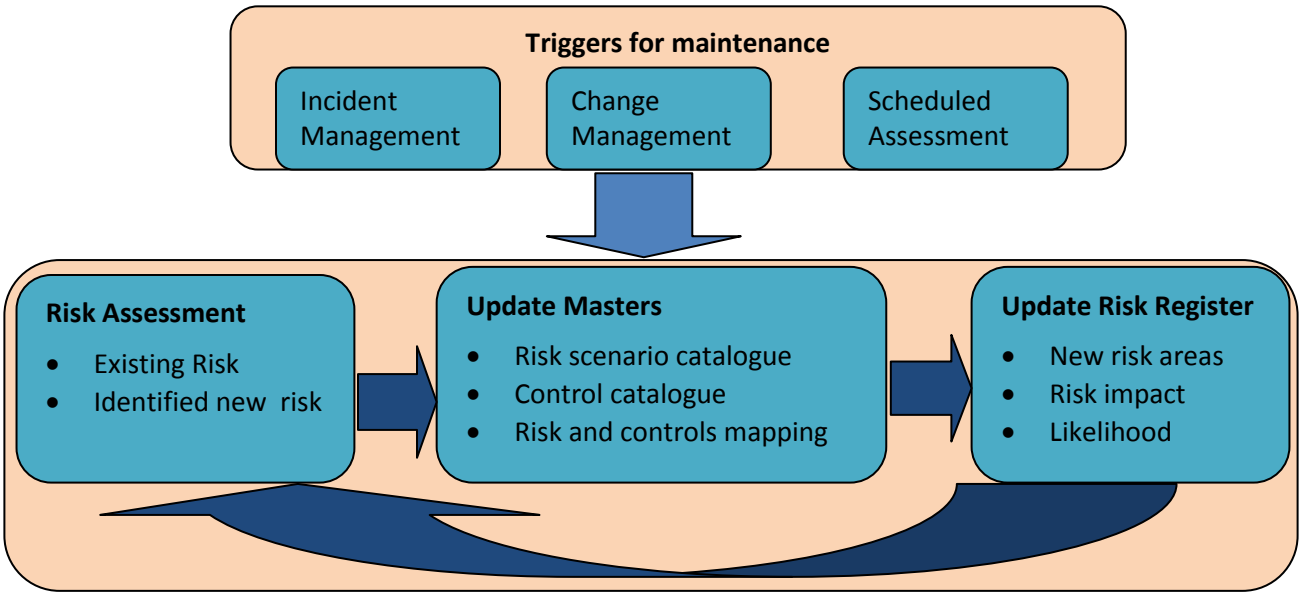


Figure 9 : Continuous Monitoring and Updating Process

CHAPTER 3
RESEARCH METHODOLOGY

3.1. Research Design

Existing risk management frameworks and standards were studied and the Risk IT framework was identified as the most appropriate framework to guide the IT risk management process due to the reasons stated in 2.4.1. Elements of the framework were customized to clearly define the domain areas and make them easily understood by stakeholders.

Fragments of the risk management process were obtained from the literature on the Risk IT framework. These combined with the operational realities of the cargo clearance process resulting in the process model described in 2.5. A web-based application prototype was developed to guide the implementation of the process, manage the IT risk management data and generate relevant reports. IT risk assessment on the cargo clearance process was carried out to demonstrate the use of the proposed process model and the developed tool.

3.2. Study Area

The cargo clearance process of Kenya Revenue Authority was used as the study area. This is the process concerned with facilitation of clearance of imported cargo and generally covers manifest management and import declaration of both sea and air cargo. The process was selected due to the involvement of multiple government departments and organizations; the all-encompassing use of IT in daily operations; and the interaction between IT systems in different organizations

3.3. Data Collection

The aim of this activity was to gather data necessary to establish the level of IT-related risks in the cargo clearance process as well as the controls targeting them by gathering information from staff in the IT and Business departments involved in the cargo clearance process.

The key methods of data collection was questionnaires and interviews; both formal and informal. The excel-based template in Appendix 13 was used to collect data. Once the data entry module of the prototype was completed, some respondents entered the data directly into the application.

Respondents were required to provide the information in Table 4.

Table 4: IT Risk Management Information

Information	**Type of Question**	**Values**
IT process objectives	Open-ended question	Respondents were required to provide a list of objectives
Critical success factors in meeting each objective	Open-ended question	Respondents were required to provide a list of factors
Risks under each critical success factor	Open-ended question	Respondents were encouraged to give as many responses as they can based on their own knowledge
Controls directed at each risk	Open-ended question	Respondents were encouraged to give as many responses as they can based on their own knowledge
Improvement actions directed at each risk	Open-ended question	Respondents were encouraged to give as many responses as they can based on their own knowledge
Inherent risk likelihood	Closed – Multiple choice questions	1=Rare,2=Unlikely,3=Possible,4=Likely,5=Almost Certain
Current risk likelihood	Closed – Multiple choice questions	1=Rare,2=Unlikely,3=Possible,4=Likely,5=Almost Certain
Residual risk likelihood	Closed – Multiple choice questions	1=Rare,2=Unlikely,3=Possible,4=Likely,5=Almost Certain
Inherent risk impact	Closed – Multiple choice questions	1=Insignificant,2=Minor,3=Moderate,4=Major,5=Fundamental
Current risk impact	Closed – Multiple choice questions	1=Insignificant,2=Minor,3=Moderate,4=Major,5=Fundamental
Residual risk impact	Closed – Multiple choice questions	1=Insignificant,2=Minor,3=Moderate,4=Major,5=Fundamental
Risk owner	Open-ended question	Respondents were required to provide the person/persons responsible for the risk
Key risk indicator	Open-ended question	Respondents were required to provide the criteria for establishing the existence and level of risk.

Sampling

Stratified random sampling was used since the target population consisted of sub-groups of interest. The research required input from respondents at various levels involved in the cargo clearance process e.g. top management, supervisors and junior staff; as well employees in different areas of specialization e.g. IT, revenue administration, systems audit, financial audit. From each of these stratums, simple random sampling was used to select respondents from whom information was obtained.

Table 5 : Sample Frame

Department	**Function**	**No. of questionnaires issued/Officers interviewed**
ICT	Infrastructure management	8
ICT	Service delivery	8
ICT	Applications management	8
ICT	Incident management	8
Internal audit	Risk management	8
Internal audit	Systems audit	8
Customs	Post clearance audit	8
Customs	Business automation office	8
Customs	Document processing centre	8
TOTAL		**72**

3.4. Data Analysis

Current risk data was analyzed based on the defined risk appetite parameters and aggregated for each IT process. The results were presented in a graphical format providing a generalized view of risk as well as the contribution of each IT process to the overall risk.

Quantitative data analysis was then carried out by computing and interpreting proportions of each level of risk in the processes as well as measures of dispersion and central tendency.

Qualitative data analysis was also carried out to identify major sources of risk, quick-wins and make relevant recommendations.

CHAPTER 4
RESULTS AND DISCUSSION

4.1. Prototype Development

The application prototype was developed based on the system use cases in Appendix 1 and the application architecture and data model in Appendix 2. The application consists of a web-based front end developed using Java Server Faces (JSF); application logic implemented using Java object oriented programming language; a persistence layer implemented using hibernate object-relational mapping library; and a MySQL database.

The application was tested and found to be working as described in the user manual in Appendix 4.

4.2. Analysis of Survey Data

4.2.1. Response Rate

A total of 59 officers responded to the questionnaires/interviews giving a response rate of 81.9%.

126 unique risks were identified with 118 controls targeting them and 51 proposed improvement actions.

Table 6: Response Rate

Department	**Function**	**No. of questionnaires issued/Officers interviewed**	**Responsive Officers**
ICT	Infrastructure management	8	8
ICT	Service delivery	8	8
ICT	Applications management	8	8
ICT	Incident management	8	8
Internal audit	Risk management	8	4
Internal audit	Systems audit	8	5
Customs	Post clearance audit	8	4
Customs	Business automation office	8	8
Customs	Document processing centre	8	6
TOTAL		**72**	**59**

4.2.2. Data Analysis

The IT risk related data was analyzed using the IT risk management tool and the results obtained are shown on Figure 10.

	Overall	Applications Mgt	Service Delivery	Infrastructure Mgt	Incident Mgt
High Risk(%)	10.32	11.11	12.5	13.64	7.55
Medium Risk(%)	67.46	70.37	41.67	81.82	71.7
Low Risk(%)	22.22	18.52	45.83	4.55	20.75
Total(%)	**100**	**100**	**100**	**100**	**100**

	Overall	Applications Mgt	Service Delivery	Infrastructure Mgt	Incident Mgt
Mean	8.41	8.07	7.54	11.27	7.0
Max	20.0	16.0	20.0	16.0	20.0
Min	2.0	2.0	2.0	4.0	3.0
Range	18.0	14.0	18.0	12.0	17.0
Standard Deviation	3.94	3.68	4.94	2.47	3.58

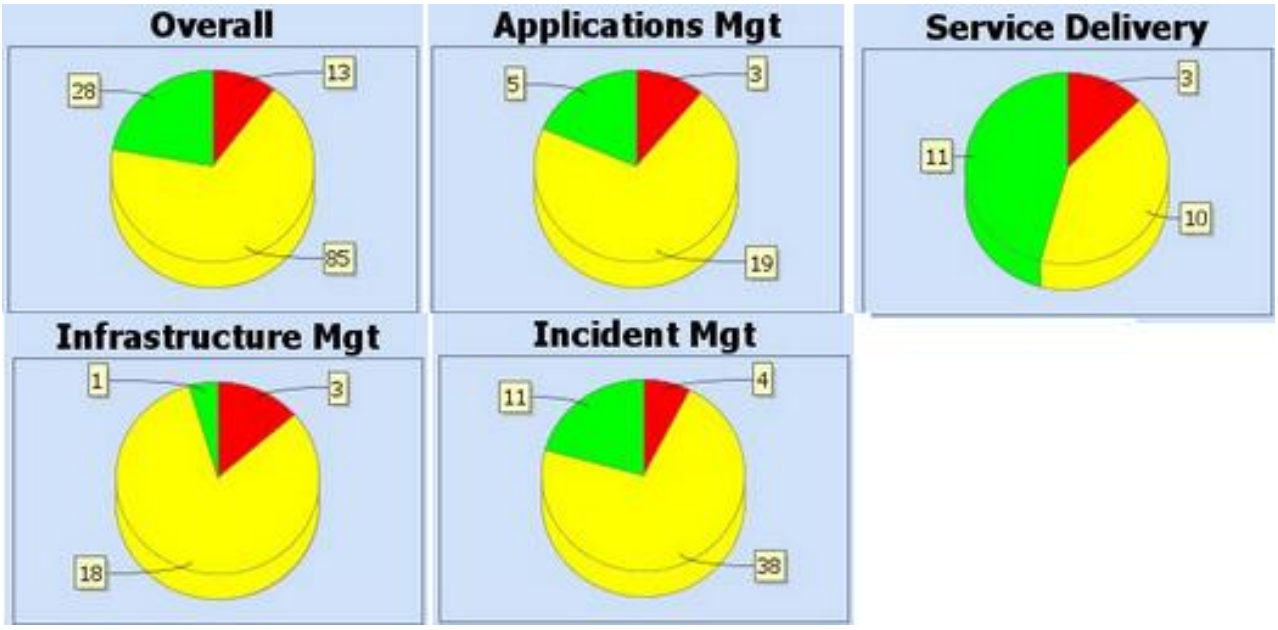


Figure 10 : Risk Data Analysis

4.3. Discussion

Infrastructure management has the highest percentage of risks requiring immediate action as well as those requiring action with medium urgency. This was attributed to the high cost of implementation of controls. It would be prudent to identify compensating controls that can be implemented immediately while resources are sought for more permanent solutions.

The mean overall risk level is 8.41.This implies that on average the controls implementation should be stepped up with a medium level of urgency.

All processes have a wide range in current risk level indicating that some risks have been controlled to a very low level while others have been left at a very high level.

The standard deviation for the overall IT risk is 3.94 indicates that the on average the level of the risks lies within the "requiring action with medium level of urgency" level of risk appetite since 8.41 +3.94 = 12.35 and 8.41 + 3.94 = 4.47.

Some controls such as a well organized training and capacity building program were found to be mitigating multiple risks. These controls if implemented will significantly improve the IT risk status of the process.

Many proposed improvement actions such as segregation of duties and banning of shared user accounts can be implemented at no significant cost. Management should ensure that they are implemented and enforced.

Reliability of external service providers was also noted as a source of many risks identified. The procedures for engaging them need to be reviewed and better ways of enforcing SLAs explored.

Obsolete equipment and inflexible technologies were also found to be causing a lot of challenges. Procurement and product development procedures need to cater for the rapid change in technology as well as the changes in the nature of business.

Staff related issues such as competence, working conditions, motivation and cooperation between IT units were identified as significant contributors towards mitigation of many risks. These should be actively promoted.

While best practice in product development is promoted, there is need for enforcement to ensure that IT products perform as expected and possess all desirable qualities such as scalability and ease of integration with other technologies.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.1. Achievements

All stated objectives of the research were achieved as shown in table 7.

Table 7 : Achievement of Objectives

	Objective	**How objective was achieved**
1	Identify the most appropriate framework for use in the cargo clearance process in Kenya	Four major Risk management frameworks and standards were studied and the Risk IT framework was identified as the most appropriate.
2	Propose a process model for IT risk management based on the identified framework	The process model defined in 2.5 was assembled from literature on the Risk IT framework as well as information specific to the area of study.
3	Develop a tool to guide the implementation of IT risk management using the proposed process model	A web-based application prototype was developed to guide the implementation of the process, manage the IT risk management data and generate relevant reports.
4	Demonstrate the use of the proposed process model and tool in IT risk management in the cargo clearance process in Kenya.	IT risk assessment on the cargo clearance process was carried out using the proposed process model and the developed prototype.

5.2. Conclusion

The framework customization process was similar to the one carried out by (MetLife Inc., 2010); maintaining the three Risk IT domains (risk governance, risk evaluation and risk response) and had a similar effect of making it easily understood by the stakeholders. This coupled with the use of scenario analysis will help the organization in encouraging stakeholder participation by making IT risk management more relevant to the business. Maintaining an updated risk profile and providing a risk dashboard to aid decision making is also significant benefit to the organization. These organizational benefits are similar to those observed by (Sunil Bakshi, 2011). Improved IT risk management will aid the government in improving revenue collection by sealing IT-related avenues for revenue leakage as well as reducing the costs of recovery from undesirable events. The Public will also benefit from better trade facilitation through availability and efficiency of IT-enabled services as well as security of personal and proprietary information.

It is therefore recommended that Kenya Revenue Authority adopts the proposed IT risk management process.

Other government Institutions can also adopt the process model. They will however need to change the likelihood scales, consequence scales and risk appetite parameters to fit their specific circumstances.

Since the Risk IT framework covers all the traditional risk management processes (identification, risk assessment, risk response, risk treatment and risk monitoring), the tool can be customized for use by organizations using risk management frameworks or standards that cover similar processes such as COBIT 5 developed by (ISACA, 2012) and the ISO 31000 risk management process developed by (International Organization for Standardization, 2009).

5.3. Recommendations for Further Research

The process model and tool may be extended to include predictive modeling. Over time, the tool will accumulate data that can be analyzed over a timeline and the impact of changes in various aspects of risk management can be predicted.

REFFERENCES

1. ISACA (2009). *The Risk IT Framework.* Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx [Accessed: 27 August 2014]
2. ISACA (2009). *The Risk IT Practitioner Guide*. Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx [Accessed: 27 August 2014]
3. ISACA (2013).*COBIT 5 for Risk.* Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-5-for-Risk.aspx [Accessed: 14 September 2014]
4. ISACA (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* Available from: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx [Accessed: 03 August 2014]
5. ISACA (2014).*Certified Information Systems Audit Glossary.* Available from: http://www.isaca.org/Knowledge-Center/Documents/Glossary/cisa_glossary.pdf [Accessed: 07 August 2014]
6. International Organization for Standardization (2009). *ISO 31000 Risk Management - Principles and Guidelines.* Available from: http://www.iso.org/iso/catalogue_detail?csnumber=43170 [Accessed: 10 August 2014]
7. International Organization for Standardization (2009). *ISO Guide 73: Risk Management Vocabulary.* Available from: http://www.iso.org/iso/catalogue_detail?csnumber=44651 [Accessed: 12 August 2014]
8. Moturi, C. A., Kinu, G. G., Kahonge, A. M. (2013). *Process Model for Enterprise Application Integration: Case for a Customs Department*. International Journal of Applied Information Systems, Vol. 6, No. 2, pp 1-16
9. Sunil Bakshi (2011)**.** *Risk IT Framework for IT Risk Management: A Case Study of National Stock Exchange of India Limited.* Available from: www.isaca.org/Knowledge-Center/cobit/Pages/Risk-IT-Case-Study-Risk-IT-Framework-for-IT-Risk-Management-A-Case-Study-of-National-Stock-Exchange-of-India-Limited.aspx [Accessed: 15 August 2014]

10. MetLife Inc (2010). *Risk IT Case Study: MetLife Enhances Risk Management.* Available from: http://www.isaca.org/Knowledge-Center/cobit/Pages/Met-Life.aspx [Accessed: 15 August 2014]

11. Benaroch M, Lichtenstein Y, Robinson K (2006).*Real Options in Information Technology Risk Management: An Empirical Validation of Risk-Option Relationships,* Management Information Systems Research Center, University of Minnesota, MIS Quarterly, Vol. 30, No. 4

12. Michel Benaroch (2002).*Managing Information Technology Investment Risk,* Journal of Management Information Systems,2002,Vol. 19,No. 2

13. Institute of Risk Management (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* Available from: *www.theirm.org/media/886062/ISO3100_doc.pdf* [Accessed: 12 August 2014]

14. Urs Fischer (2011).*IT Scenario Analysis in Enterprise Risk Management,* ISACA Journal , Vol. 2,No. 3

15. Sharma, P., Mishra, A., Mishara, P. (2011). *E-Governance in India is the Effectual and Challenging Approach to Governance,* International Journal of Business Management & Economic Research, Vol. 3,No. 5

APPENDICES

Appendix 1 : System Use Cases

Figure 1 summarizes the interactions between the user and the risk management tool.

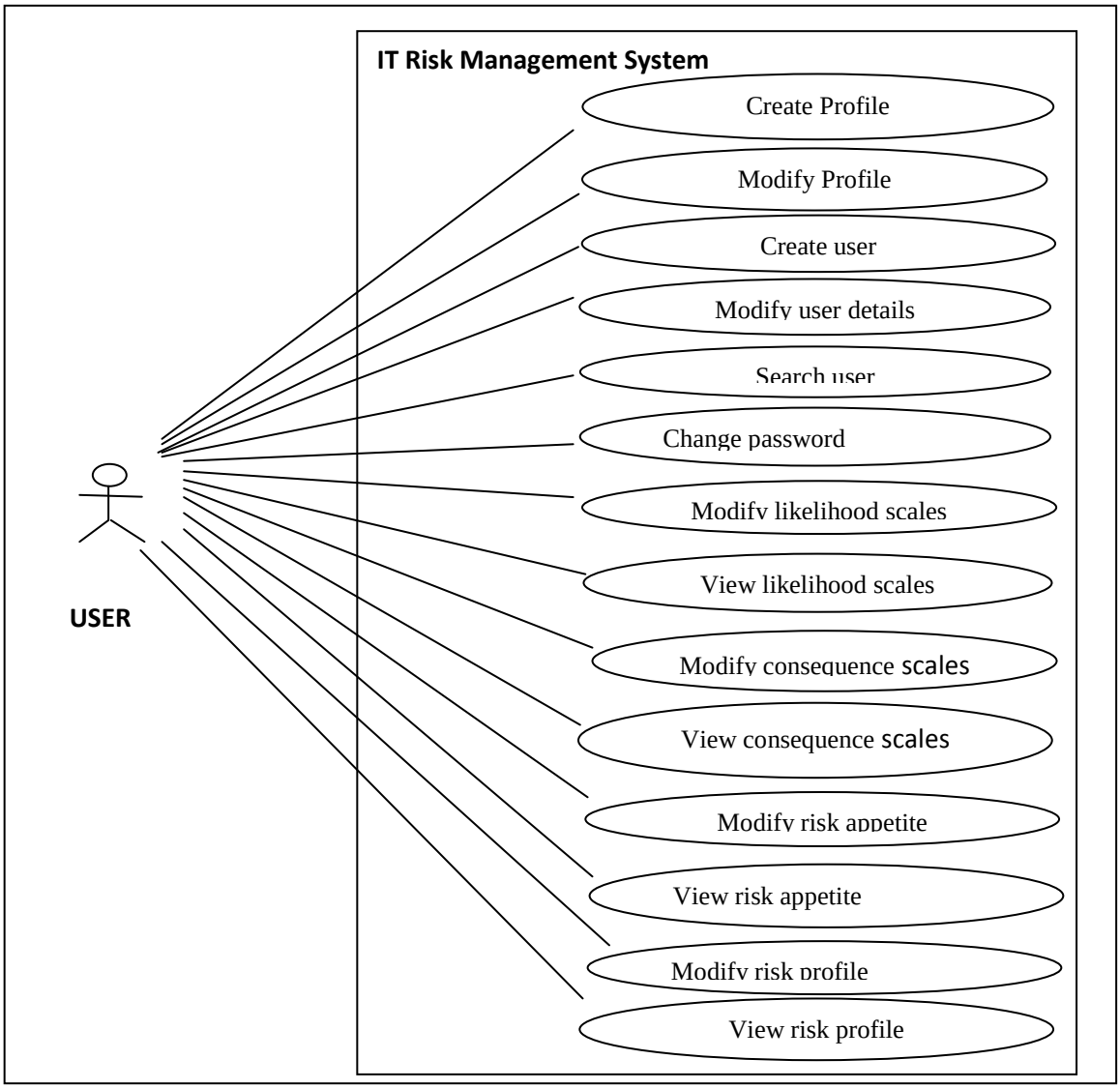


Figure 1: Use case Model

Login

Use Case ID:	UC-001				
Use Case Name:	Login				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality authenticates users and allows access to assigned functions				
Preconditions:	1. User's account exists in the database				
Post conditions:	1. Application log entry made for the successful or failed login attempt 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User enters the address of the application on a web browser 2. System displays the authentication interface 3. User types in the username and password in the relevant fields and clicks on the 'Submit' button. 4. System authenticates the credentials using **UC-001-BR1** 5. If the credentials are valid, the system avails the functions assigned to the user's profile. 6. If this is the User's first login attempt, **AP1** 7. If credentials are invalid, **EP1, EP2** 8. End of use case				
Alternative Paths:	1. System displays "change password" interface **UI6**				
Exception Paths:	**EP1:** If username or password is incorrect i. System displays message "Wrong username or password" **EP2:** If user account status is suspended i. System displays message "Account is suspended. Please contact administrator"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-001-BR1:** User Authentication i. User account must exist in the application database ii. Password entered must be the same as password stored when both are encrypted iii. Account status must be active				
Process Owner:	IT Risk Management Manager				

Create profile

Use Case ID:	UC-002				
Use Case Name:	Create Profile				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality creates user roles in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Create Profile" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Create profile" function from the menu 2. System displays the profile creation interface 3. User enters the profile name and code and clicks on the "save" button 4. System validates the profile name and code using **UC-002-BR1** 5. If code and name are valid, System displays the message "Profile saved successfully" and allows for the addition of functions to the profile 6. User selects the functions to be added to the profile and clicks on the "Add functions" button. 7. System displays the message "Functions added successfully" 8. End of use case				
Alternative Paths:					
Exception Paths:	**EP1:** If profile code is invalid i. System displays message "Invalid code" **EP2:** If profile name is invalid i. System displays message "Invalid code"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-002-BR1:** User Authentication i. Profile code must be alphanumeric and 3 characters long ii. Profile name must not be blank iii. Profile name must be alphanumeric				
Process Owner:	IT Risk Management Manager				

Modify profile

Use Case ID:	UC-003				
Use Case Name:	Modify Profile				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality amends user roles in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Modify Profile" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify profile" function from the menu 2. System displays the profile search interface 3. User enters part or full profile name and/or code and clicks on the "search" button 4. System displays a list of profiles retrieved based on the specified criteria. 5. User may modify profile name and/or code and click on the "Save" button 9. System validates the profile name and code using **UC-003-BR1** 6. If code and name are valid, System displays the message "Profile updated successfully". 7. User may select the functions to be added to the profile and clicks on the "Add functions" button. 8. System displays the message "Functions added successfully" 9. End of use case				
Alternative Paths:					
Exception Paths:	**EP1:** If profile code is invalid i. System displays message "Invalid code" **EP2:** If profile name is invalid i. System displays message "Invalid code"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-003-BR1:** User Authentication i. Profile code must be alphanumeric and 3 characters long ii. Profile name must not be blank iii. Profile name must be alphanumeric				
Process Owner:	IT Risk Management Manager				

Create user

Use Case ID:	UC-004				
Use Case Name:	Create User				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality creates a user account in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Create user" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Create user" function from the menu 2. System displays the user creation interface 3. User enters the user details specified in **UC-004-BR1** and clicks on the "save" button 4. System validates the details using **UC-004-BR2** 5. If details are valid, System displays the message "User saved successfully". 6. End of use case				
Alternative Paths:					
Exception Paths:	**EP1:** If details are invalid i. System displays message "Invalid information"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-004-BR1:** User Details i. Staff No. ii. Name iii. Profile iv. Physical address v. Postal Code vi. P.O. box vii. Telephone viii. Email address **UC-004-BR2:** Details Validation i. Staff No. must be alphanumeric ii. Staff No. and Name must not be blank iii. Profile must be selected				
Process Owner:	IT Risk Management Manager				

Modify user details

Use Case ID:	UC-004				
Use Case Name:	Modify User Details				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality amends user details in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Modify user details" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify user details" function from the menu 2. System displays the user search interface 3. User enters the search criteria and clicks on the "search" button 4. System displays all user records displayed using the criteria specified 5. User modifies the user details specified in **UC-005-BR1** and clicks on the "save" button 6. System validates the details using **UC-005-BR2** 7. If details are valid, System displays the message "User details updated successfully". 8. End of use case				
Alternative Paths:					
Exception Paths:	**EP1:** If details are invalid i. System displays message "Invalid information"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-005-BR1:** User Details i. Staff No. ii. Name iii. Profile iv. Physical address v. Postal Code vi. Telephone vii. Email address **UC-005-BR2:** Details Validation iv. Staff No. must be alphanumeric v. Staff No. and Name must not be blank vi. Profile must be selected				
Process Owner:	IT Risk Management Manager				

Search user

Use Case ID:	UC-004				
Use Case Name:	Search User				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality searches user details in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Search user" function				
Post conditions:	1. Application log entry made for the operation				
Basic Course:	1. Use Case begins when a User selects the "Search user" function from the menu 2. System displays the user search interface 3. User enters the search criteria and clicks on the "search" button 4. System displays all user records displayed using the criteria specified 5. End of use case				
Business Rules:					
Process Owner:	IT Risk Management Manager				

Modify likelihood scales

Use Case ID:	UC-004				
Use Case Name:	Modify likelihood scales				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality modifies likelihood scales				
Preconditions:	1. User is logged in. 2. User profile has the "Modify likelihood scales" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify likelihood scales" function from the menu 2. System displays the Likelihood scales modification interface 3. User modifies the likelihood scale details and clicks on the "save" button 4. System displays the message "Likelihood scales saved successfully". 5. End of use case				
Process Owner:	IT Risk Management Manager				

Change password

Use Case ID:	UC-004				
Use Case Name:	Change Password				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality changes the password of the logged in user				
Preconditions:	1. User is logged in.				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify user details" function from the menu 2. System displays the password change interface 3. User enters the current password, new password and confirmation of new password and clicks on the "Change Password" button 4. System validates the entered password using **UC-006-BR1** 5. If entered details are valid, System displays the message "Password changed successfully". 6. If entered values are invalid, **EP1, EP2, EP3, EP or EP5** 7. End of use case				
Alternative Paths:					
Exception Paths:	**EP1:** If Old Password is blank System displays message "Please enter Old Password" **EP2:** If New Password is blank System displays message "Please enter New Password" **EP3:** If Confirmation Password is blank System displays message "Please enter Confirmation Password" **EP4:** If New Password is less than 8 characters System displays message "New Password must be at least 8 characters"				
Priority:	High				
Frequency of Use:	High				
Business Rules:	**UC-006-BR1:** Password Validation i. Old, New and Confirmation passwords must not be null ii. New password must be the same as Confirmation password iii. New password must be at least 8 characters long iv. New password must have at least one letter and one number				
Process Owner:	IT Risk Management Manager				

View likelihood scales

Use Case ID:	UC-004				
Use Case Name:	View likelihood scales				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality displays likelihood scales				
Preconditions:	1. User is logged in. 2. User profile has the "View likelihood scales" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "View likelihood scales" function from the menu 2. System displays the Likelihood scales view interface 3. End of use case				
Process Owner:	IT Risk Management Manager				

Modify consequence scales

Use Case ID:	UC-004				
Use Case Name:	Modify consequence scales				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality modifies consequence scales				
Preconditions:	1. User is logged in. 2. User profile has the "Modify consequence scales" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify consequence scales" function from the menu 2. System displays the consequence scales modification interface 3. User modifies the consequence scale details and clicks on the "save" button 4. System displays the message "Consequence scales updated successfully". 5. End of use case				
Process Owner:	IT Risk Management Manager				

View consequence scales

Use Case ID:	UC-004				
Use Case Name:	View consequence scales				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality displays consequence scales				
Preconditions:	1. User is logged in. 2. User profile has the "View consequence scales" function				
Post conditions:	1. Application log entry made for the operation				
Basic Course:	1. Use Case begins when a User selects the "View consequence scales" function from the menu 2. System displays the consequence scales view interface 3. End of use case				
Business Rules:					
Process Owner:	IT Risk Management Manager				

Modify risk appetite

Use Case ID:	UC-004				
Use Case Name:	Modify risk appetite				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality modifies risk appetite details in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Modify risk appetite" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify risk appetite" function from the menu 2. System displays the risk appetite modification interface 3. User modifies the risk appetite details and clicks on the "save" button 4. System displays the message "Risk appetite details updated successfully". 5. End of use case				
Process Owner:	IT Risk Management Manager				

View risk appetite

Use Case ID:	UC-004				
Use Case Name:	View risk appetite				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality displays risk appetite details				
Preconditions:	1. User is logged in. 2. User profile has the "View risk appetite" function				
Post conditions:	1. Application log entry made for the operation				
Basic Course:	1. Use Case begins when a User selects the "View risk appetite" function from the menu 2. System displays the risk appetite view interface 3. End of use case				
Process Owner:	IT Risk Management Manager				

Modify risk profile

Use Case ID:	UC-004				
Use Case Name:	Modify risk profile				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality modifies risk profile details in the system				
Preconditions:	1. User is logged in. 2. User profile has the "Modify risk profile" function				
Post conditions:	1. Application log entry made for the operation 2. Database trigger fires to store before and after images of the affected database records				
Basic Course:	1. Use Case begins when a User selects the "Modify risk profile" function from the menu 2. System displays the risk profile modification interface 3. User modifies the risk profile details and clicks on the "save" button 4. System displays the message "Risk profile details updated successfully". 5. End of use case				
Process Owner:	IT Risk Management Manager				

View risk profile

Use Case ID:	UC-004				
Use Case Name:	View risk profile				
Version:	**Version No.:**	**Created By:**	**Date Created:**	**Last Updated By:**	**Date Last Updated:**
	1.0	K. Karanja	12/11/2014	K. Karanja	12/11/2014
Actors:	System User, IT Risk management system				
Description:	This functionality displays risk profile details				
Preconditions:	1. User is logged in. 2. User profile has the "View risk profile" function				
Post conditions:	1. Application log entry made for the operation				
Basic Course:	1. Use Case begins when a User selects the "View risk profile" function from the menu 2. System displays the risk profile view interface 3. End of use case				
Alternative Paths:					
Exception Paths:					
Priority:	High				
Frequency of Use:	High				
Business Rules:					
Process Owner:	IT Risk Management Manager				

:

Appendix 2 : Application Design Diagrams

Architectural Overview

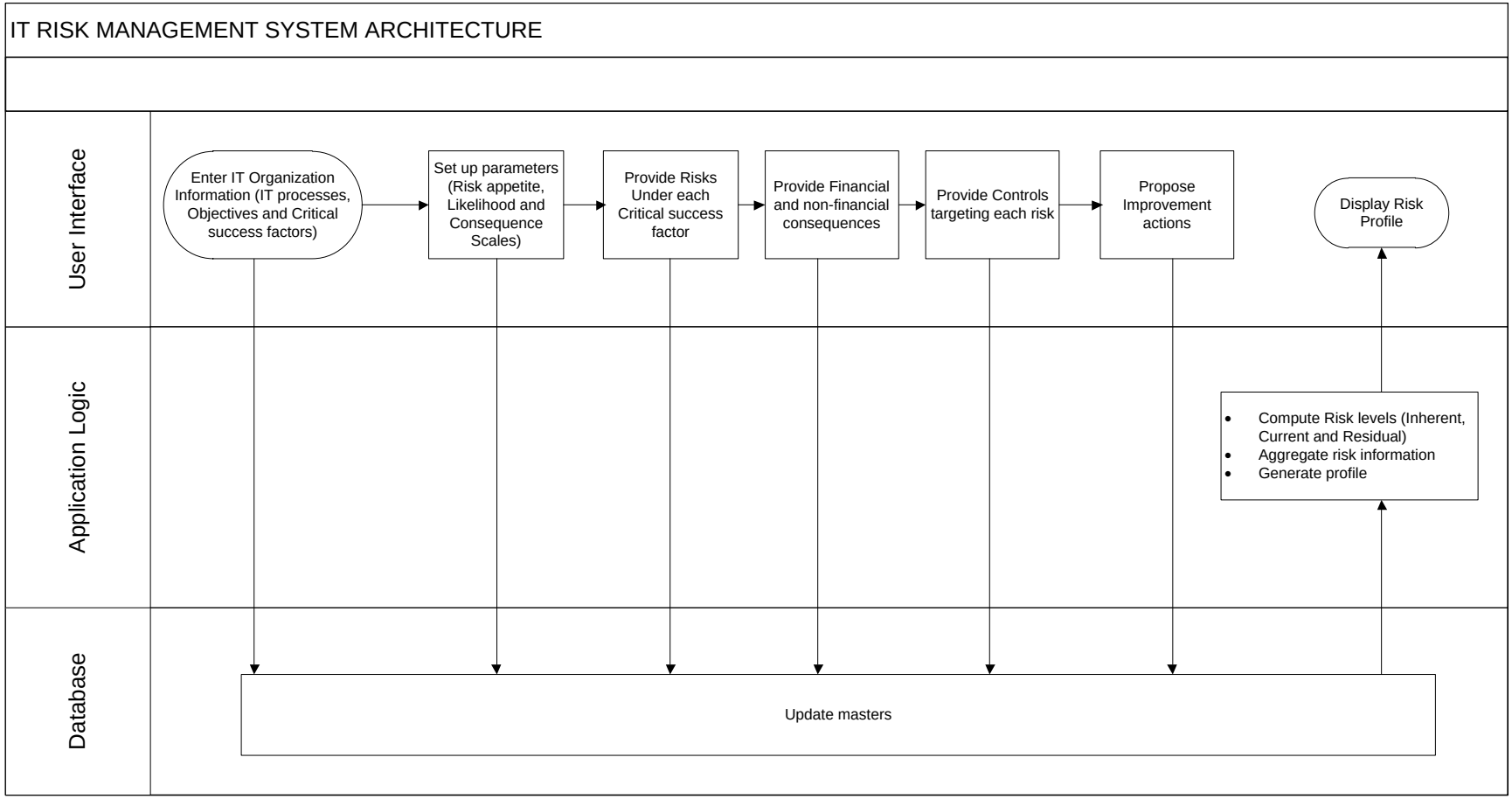


Figure 2: Architectural overview

Data Model

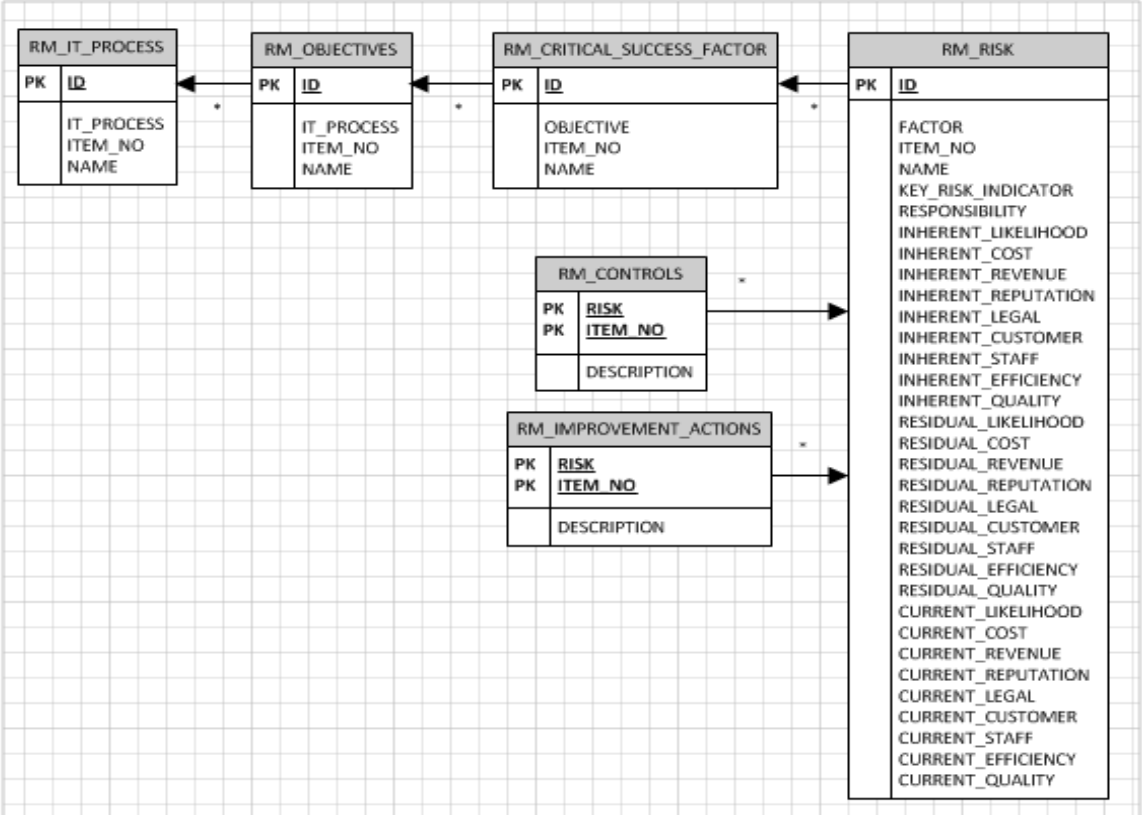


Figure 3: Risk Management Data Model

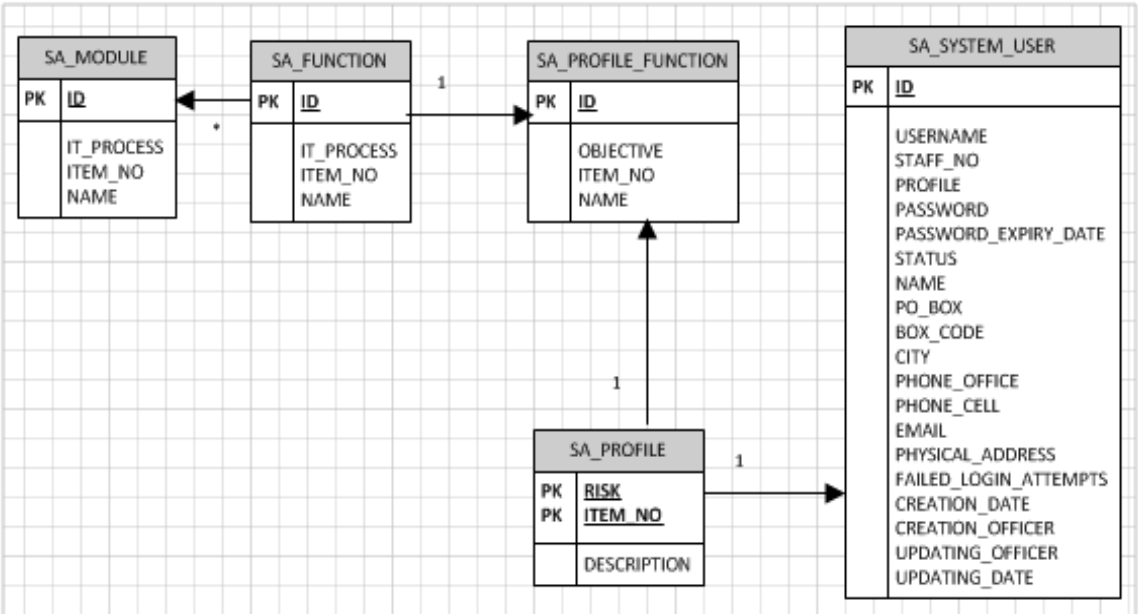


Figure 4: System Administration Data Model

Appendix 3 : Data Collection Template

This appendix presents the template used in data collection.

General Information

IT Process	Objectives	Critical success factors	RISKS	Key Risk Indicator	Owner

Inherent Risk (for each risk)

Likelihood	Impact							
	Amount (Cost)	Amount (Revenue)	Reputation	Regulatory /Legal	Customer satisfaction	Staff satisfaction	IT efficiency	Quality of service

Existing Controls (for each risk)

Existing Controls

Current Risk (for each risk considering the existing controls)

Likelihood	Impact							
	Amount (Cost)	Amount (Revenue)	Reputation	Regulatory /Legal	Customer satisfaction	Staff satisfaction	IT efficiency	Quality of service

Proposed improvement actions (for each risk)

Proposed improvement actions

Expected Residual Risk (for each risk considering the improvement controls)

Likelihood	Impact							
	Amount (Cost)	Amount (Revenue)	Reputation	Regulatory /Legal	Customer satisfaction	Staff satisfaction	IT efficiency	Quality of service delivery

Appendix 4 : Application Prototype User Manual

Contents

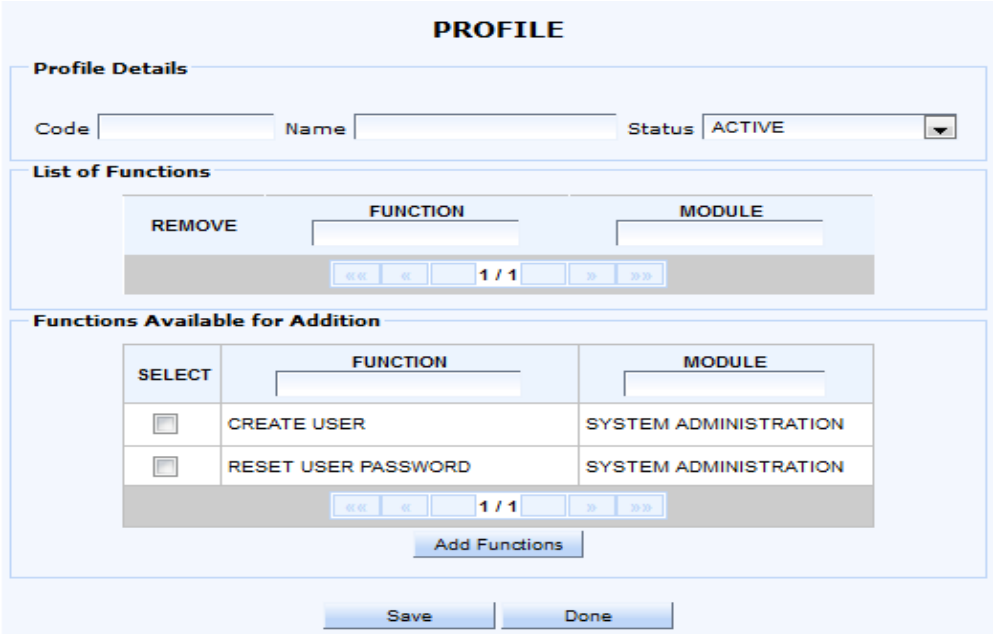
Login

1. Enter the address of the application on a web browser
2. System displays the login interface (UI1)
3. Type in the username and password in the relevant fields and click on the 'Submit' button.

UI1: User login interface

Create Profile

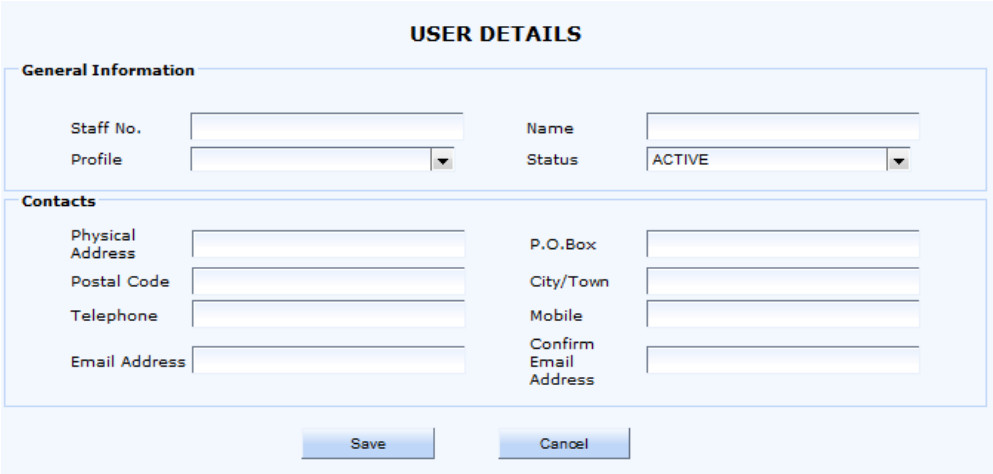
1. Select the "Create profile" function from the menu
2. System displays the profile creation/Modification interface (UI2).
3. Enter the profile name and code and click on the "save" button
4. If code and name are valid, System displays the message "Profile saved successfully"
5. Select the functions to be added to the profile and click on the "Add functions" button.
6. System displays the message "Functions added successfully"



UI2: Profile creation interface

Create user

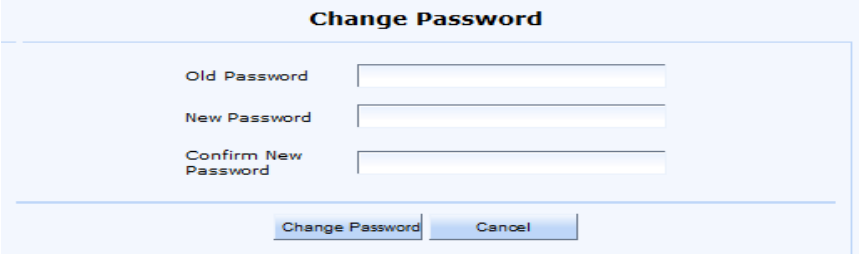
1. Select the “Create user” function from the menu
2. System displays the user creation interface (UI3)
3. Enter the user details and click on the “save” button
4. System validates the details
5. If details are valid, System displays the message “User saved successfully”.



UI3: User creation/modification interface

Change Password

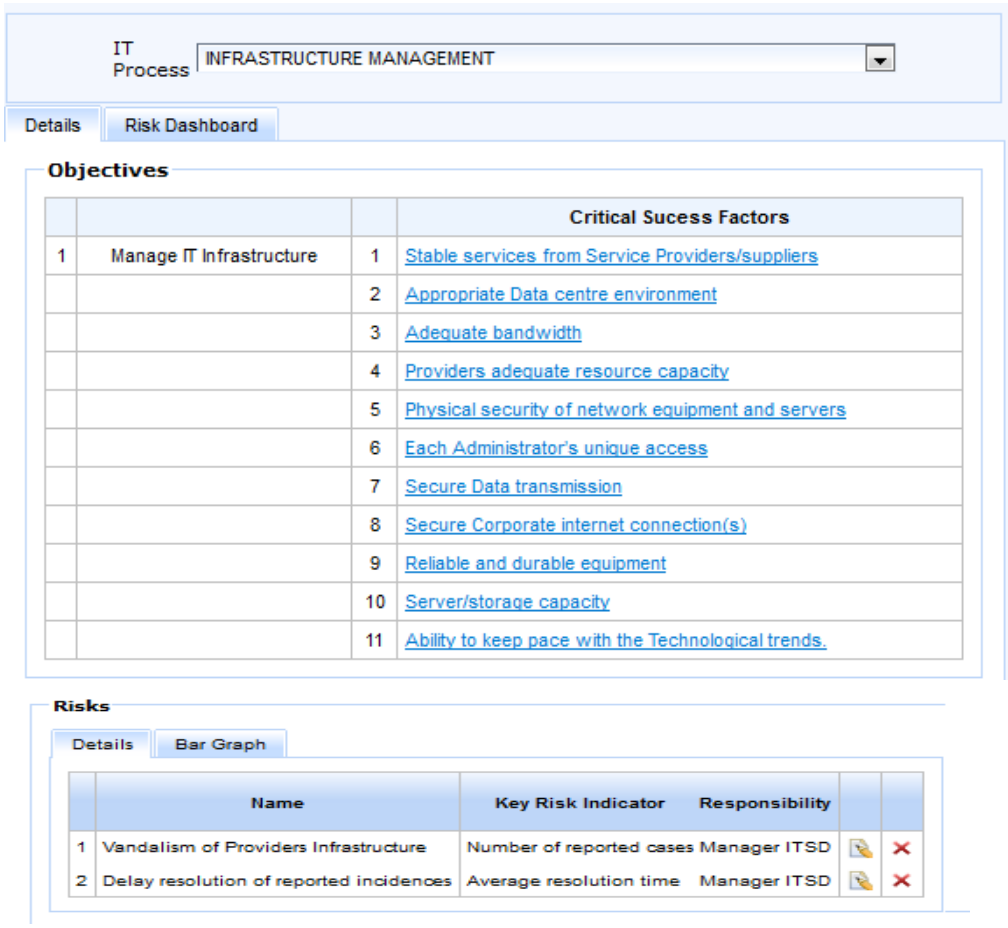
1. Select the “Modify user details” function from the menu
2. System displays the password change interface (UI4)
3. Enter the current, new and confirmation password and click the “Change Password” button
4. System validates the entered details
5. If entered details are valid, System displays the message “Password changed successfully”.



UI4: password change interface

Modify Risk Profile

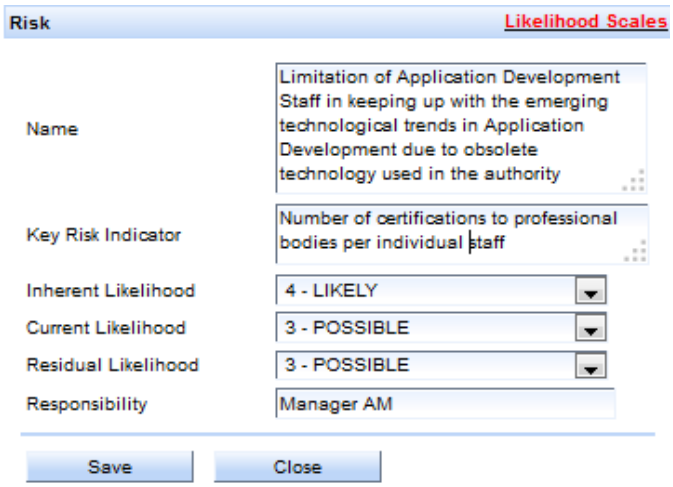
1. Select the “MODIFY RISK PROFILE” function on the menu.
2. The System displays the risk information classification interface (UI5).
3. Select the appropriate IT process.
4. Add/Edit/Delete risks as appropriate



UI5: IT risk management information classification interface

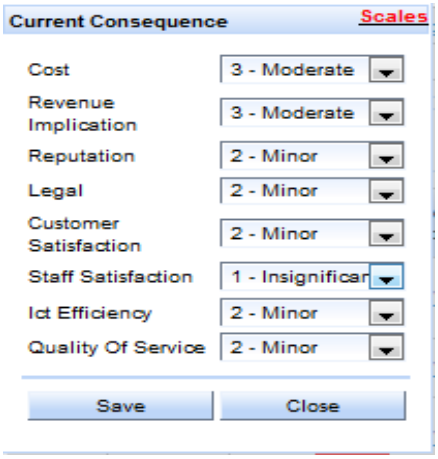
Capture Modify/risk

1. Click on the “New Risk” Button if capturing a new risk or select the “edit” link.
2. The System will display the risk input interface (UI6)
3. Enter the Risk name, Key risk indicator, ownership and likelihood information
4. Click on the save button



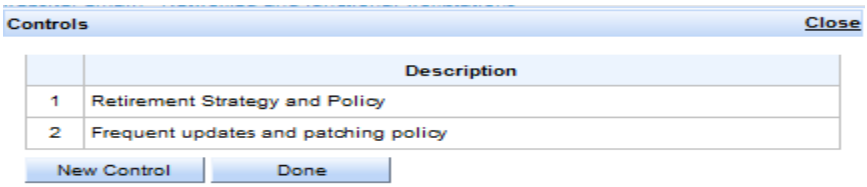
UI6: Profile creation interface

5. Select the Consequence information for the risk using (UI7).



UI7: Consequence input interface

6. Enter the existing controls targeted at the risk using (UI8).



UI8: Existing controls input interface

View Risk Details

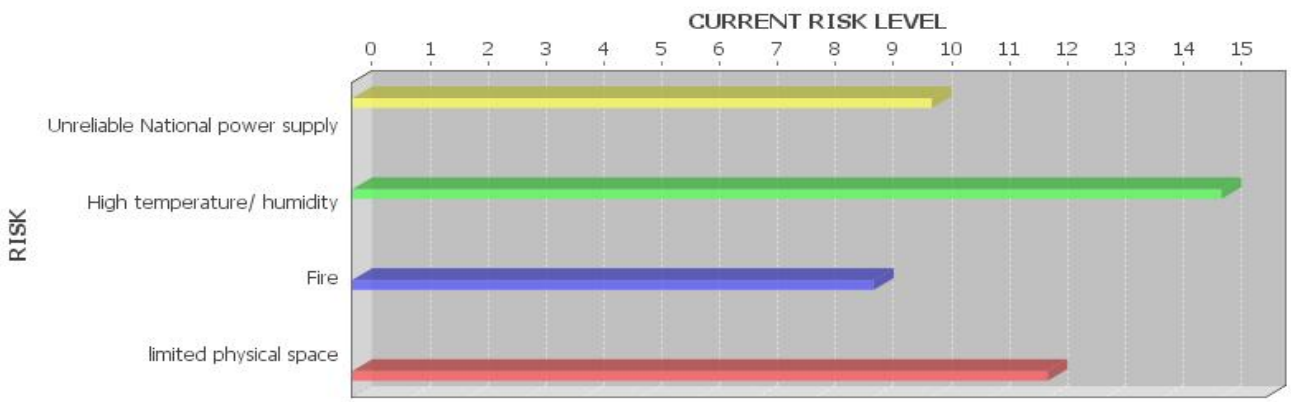
The application generates tabular and graphical reports on demand.

Details | Bar Graph

	Name	Key Risk Indicator	Inherent Risk			Existing Controls	Current Risk			Improvement Actions	Residual Risk			Responsibility		
			Likelihood	Impact	Level		Likelihood	Impact	Level		Likelihood	Impact	Level			
1	Unreliable National power supply	Frequency and duration of power outages and unstable power supply	5 - Almost Certain	5	25	View	5 - Almost Certain	2	10	View	5 - Almost Certain	2	10	Manager IM		
2	High temperature/ humidity	frequency of high levels of recorded temperatue and humidity	3 - Possible	5	15	View	3 - Possible	5	15	View	3 - Possible	5	15	Manager IM		
3	Fire	Number of potential causes	3 - Possible	5	15	View	3 - Possible	3	9	View	3 - Possible	3	9	Manager IM		
4	limited physical space	related audit issues	4 - Likely	3	12	View	4 - Likely	3	12	View	4 - Likely	3	12	Manager IM		

UI9: Tabular risk report

Details | Bar Graph

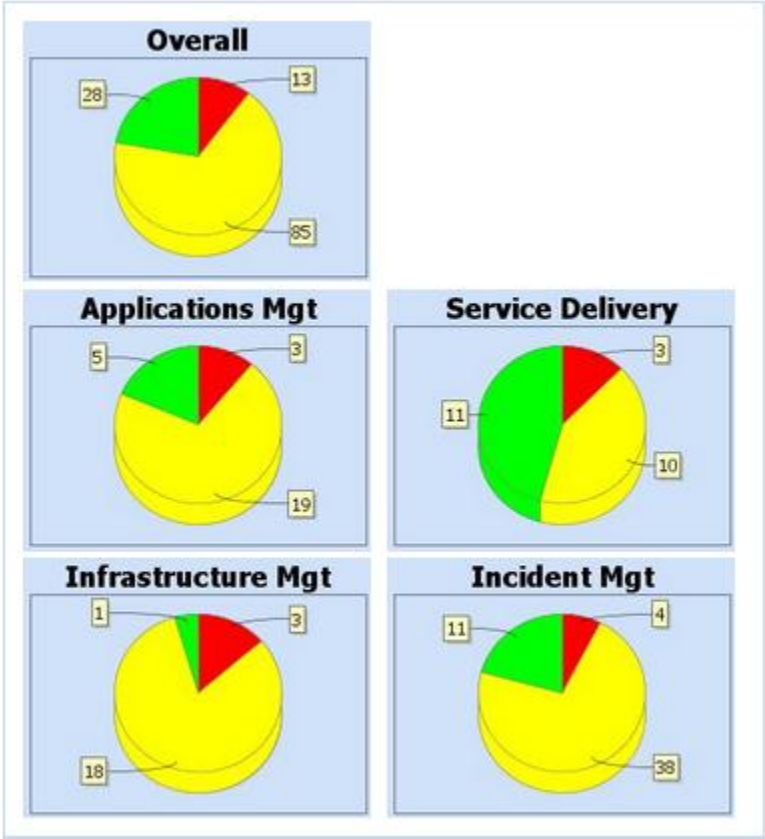


Risk	
Unreliable National power supply	10
High temperature/ humidity	15
Fire	9
limited physical space	12

UI10: Graphical risk report

Risk dashboard

The application provides a summarized view of the IT risk status of the organization at a glance.



	Overall	Applications Mgt	Service Delivery	Infrastructure Mgt	Incident Mgt
High Risk(%)	10.32	11.11	12.5	13.64	7.55
Medium Risk(%)	67.46	70.37	41.67	81.82	71.7
Low Risk(%)	22.22	18.52	45.83	4.55	20.75
Total(%)	**100**	**100**	**100**	**100**	**100**

	Overall	Applications Mgt	Service Delivery	Infrastructure Mgt	Incident Mgt
Mean	8.41	8.07	7.54	11.27	7.0
Max	20.0	16.0	20.0	16.0	20.0
Min	2.0	2.0	2.0	4.0	3.0
Range	18.0	14.0	18.0	12.0	17.0
Standard Deviation	3.94	3.68	4.94	2.47	3.58

UI11: Risk Dashboard