



UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

School of Computing and Informatics

**AN INFORMATION SECURITY RISK MANAGEMENT GAP ANALYSIS TOOL BASED ON
ISO/IEC 27005:2011 COMPLIANCE FOR SMES IN KENYA**

By

ANDREW ELIEZOR OKOTH OBWANDA

P53/73070/2014

Supervisor

DR. ANDREW MWAURA KAHONGE

July 2018

A project report submitted in partial fulfillment of the requirements for the award of the degree of
Masters of Science in Distributed Computing Technology

DECLARATION

This project is my original work and has not been presented for a degree in any other University.

Signature _____ **Date** _____

Andrew Eliezor Okoth Obwanda
Registration No. P53/73070/2014

Supervisor

This research project has been submitted for examination with my approval as University Supervisor.

Signature _____ **Date** _____

Dr. Andrew Mwaura Kahonge
School of Computing and Informatics
University of Nairobi

DEDICATION

To my wife and son for their love, support and constant reminder, to my parents for their never-ending prayers and to myself for being steadfast.

ACKNOWLEDGEMENT

I thank the Almighty God for giving me the strength and wisdom in this project. I am also extremely grateful to Dr. Andrew Kahonge, my project supervisor from the University of Nairobi for his guidance and support during this study. I learned a lot through his guidance and advices.

I also thank Phillip Okello, Donald Chepkwony and Ronald Njagi for tutorials and guidance in Php programming, Apache web hosting and sitting with me late in the evenings when I needed their guidance.

ABSTRACT

While being adopted by large institutions, information security risk management is still an out of range for smaller ones like SMEs, hence the need for a free and easy to use information security risk assessment and management tool.

The main objective of this study was to come up with a software tool for information security risk management based on ISO/IEC 27005:2011 standard to be used by SMEs in Kenya to do a compliance gap analysis.

A detailed literature review of the current works in information security risk management and a descriptive survey using questionnaires targeted to the SMEs with a focus on their understanding of information security risk management, the tools they use and their personnel capacity to conduct an information security risk assessment as per the standard of the study was done.

From the survey response came the non-functional requirements while the functional requirements came from a detailed review and analysis of the ISO/IEC 27005:2011 standard. Development of the software tool followed the Rapid Application Development (RAD) methodology.

We found that even though SMEs were aware of what an information security risk management was, they lacked proper in house skills and tools to do an information security risk assessment and gauge their respective institutions compliance to global risk standards. The software tool was welcomed as a potential in being an effective tool for information security risk assessment and management.

TABLE OF CONTENTS

DECLARATION	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT	iv
ABSTRACT.....	v
TABLE OF FIGURES	viii
ACRONYMS AND ABBREVIATIONS	viii
CHAPTER ONE: INTRODUCTION	1
1.1 Background.....	1
1.2 The Research Problem	2
1.3 Research Objectives.....	3
1.4 Research Questions.....	3
1.5 Significance of the Study	3
CHAPTER TWO: LITERATURE REVIEW	5
2.1 GAP Analysis.....	5
2.2 Understanding SMEs	5
2.3 Information Security Risk Management (ISRM).....	5
2.4 Current Standards in Risk Management	8
2.4.1 AS/NZS 4360:2004 (AS/NZS ISO 3100:2009).....	8
2.4.2 NIST Special Publication 800-39	9
2.4.3 ISO/IEC 27005:2011.....	10
2.5 Current Methods and Frameworks in Information Security Risk Management	13
2.5.1 CRAMM	13
2.5.2 FAIR	13
2.5.3 OCTAVE	14
2.5.4 RISK IT.....	14
2.5.5 EBIOS 2010	15
2.5.6 CORAS	15
2.5.7 MAGERIT v3 2014	16
2.5.8 MEHARI.....	16
2.6 Related works in Information Security Risk Management tools aligned to ISO/IEC 27005.....	17
2.7 Conceptual Model of the study	18
CHAPTER THREE: RESEARCH METHODOLOGY.....	19
3.1 Research Design.....	19
3.2 Study Population.....	19
3.3 Sampling Design	20

3.4	Data Collection	20
3.5	Data Analysis	21
3.6	System Analysis.....	22
3.7	System Design	22
3.8	System Development Tools and Technologies	23
3.9	System Testing.....	24
3.10	Ethical Considerations	24
CHAPTER FOUR: RESULTS AND DISCUSSIONS		25
4.1	Analysis of Survey Results	25
4.1.1	General demographic information of respondents	25
4.1.2	Awareness of Information Security Risk Management	27
4.1.3	The need for an Information Security Risk Assessment Software Tool	30
4.2	Prototype Testing	32
4.2.1	Prototype Usability	32
4.2.2	User Acceptance Test.....	32
4.2.3	Prototype Availability	32
4.3	Discussion	32
CHAPTER FIVE: CONCLUSION & FUTURE WORK.....		34
5.1	Conclusion	34
5.2	Limitations and Challenges.....	34
5.3	Future work.....	35
REFERENCES		36
APPENDIX A: Project Schedule.....		39
APPENDIX B: Letter of Introduction		40
APPENDIX C: Survey Questionnaire		41
APPENDIX D: Why your institution needs a software tool.....		52
APPENDIX E: Probable features		53
APPENDIX F: Application installation requirements		53
APPENDIX G: Application screen shots.....		55
APPENDIX H: Sample code		62

TABLE OF FIGURES

Figure 1- The Risk Management Process. Source ISO 31000.....	6
Figure 2- AS/NZS 4360:2004 Risk Management process. Source (Herpes et al, 2014)	9
Figure 3 - ISO/IEC 27005:2011 Information security risk management process. Source (ISO, 2011).....	11
Figure 4 - Conceptual Model	18
Figure 5 - System Architecture	23

TABLE OF TABLES

Table 1: Role/Titles of respondents	25
Table 2: Category of the Institutions.....	26
Table 3: Institution ages.....	26
Table 4: Information Security incidents within institutions.....	27
Table 5: Information Security Risk Management awareness	27
Table 6: Information Security Risk Management training.....	28
Table 7: Training materials	28
Table 8: Cause and period of training	28
Table 9: Information security Risk Plan	29
Table 10: What necessitates risk assessment	29
Table 11: Respondent aware of global standards, framework or methodology.....	30
Table 12: Global standards, framework or methodologies awareness and adoption	30
Table 13: Familiarity with risk assessment software tool	31
Table 14: Necessity for an information security risk assessment tool	31

ACRONYMS AND ABBREVIATIONS

ISACA	Information Systems Audit and Control Association
IT	Information Technology
COBIT	Control Objectives for Information and Related Technologies
Val IT	Governance framework for creating business value from IT investments
SME	Small and medium-sized enterprises
ISO	International Organization for Standardization
IEC	International Electro-technical Commission
CEO	Chief Executive Officer
MD	Managing Director

CHAPTER ONE: INTRODUCTION

1.1 Background

With the advent and growth of the internet, information technology has made it sure that its presence has been and is felt globally. As technology advances, new opportunities are created. One of these are in business opportunities that have been formed on the backbone of information technology riding on the interconnection that is the internet. This advancement in technology and global interconnection has also created new risks.

Many small and medium enterprises (SME) fall in this category of new businesses or rather organizations that attribute their existence to information technology. A recent National Economic Survey report by the Kenya National Bureau of Statistics (KNBS) indicated that SMEs constituted 98 percent of all businesses in Kenya, they create 30 percent of the jobs annually as well as contribute 3 percent of the GDP to the economy (KNBS, 2017). In the 2017 report by Foresight Africa, one of the top priorities for the African continent was growth of its SMEs and this they said was going to be pegged on technology. Across the continent, new startup digital enterprises are emerging, while existing small and medium enterprises (SMEs) are increasingly leveraging on ICT to expand (Africa, 2017).

While technology dependent SMEs are expanding, they come face to face with new compliance measures they have to meet either due to regulatory requirements or to ensure continuity of business or to meet specific global certification standards. Some of these standards can be in information security, risk management, business continuity, quality assurance and many others.

When it comes to information security and risk management, very few SMEs give much thought to global practices. This according to Tawileh et al (2007) can be attributed to high budgetary constraints which did not allow them to acquire tools to carry out necessary and important security and risk assessment, and this further was compounded with the lack of in house expertise in information security and risk management.

1.2 The Research Problem

A PWC report of 2015 on information security breaches survey, reported that there was a percentage increase in breaches for both large and small organizations in that year. Large organizations suffered 90% and 74% for small organizations, a 10% increase for both from 2014 (Potter et al, 2015).

The report further stated that the risk profiles for SMEs and large institutions did not differ significantly, they both use technology in many of their business processes and both would face serious consequences in the event of a disaster, irrespective of the source of the threat. This called for a proactive risk management to at least nip the threats and vulnerabilities before a disaster or even control them to an acceptable level.

Information security risk management is one of the key areas of a company's management process, whether big or small, that deals with the identification, analysis, treatment, communication and acceptance of information security related risks. It involves the selection and implementation of countermeasures justified by the identified information security risks and the reduction of those risks to acceptable levels (ENISA, 2006).

For large organizations, information security risk management is not an issue. This is because of their large budget towards asset protection and acquisition of expert human resources. But this is not so for SMEs. Due to resource restrictions and insufficient maturity of information security and risk management knowledge (Tawileh et al, 2007), they face difficulties in setting up an effective and efficient information security risk management system.

To help with the issue of information security risk management, the International Standardization Organization (ISO) published in 2008 the ISO/IEC 27005 standard followed by its revision in 2011, giving guidelines on how to establish an information security risk management system. It is designed to assist the satisfactory implementation of information security based on a risk management approach (ISO, 2011).

Implementing this standard by organizations mostly starts by doing a gap analysis between the current status of information security risk management process and what the standard dictates. This is necessary to estimate the resources required and to give an overview of what could be reused within the current setup. For most organizations especially for special ones like the SMEs, it is usually an arduous task.

The focus of this research was to analyze the needs of the SMEs vis-a-vis information security risk management and to come up with an efficient gap analysis software tool to assist with this venture.

1.3 Research Objectives

The primary objective of this research was to design a software tool for information security risk management based on ISO/IEC 27005:2011 standard to be used by SMEs in Kenya to do a compliance gap analysis.

Sub-objectives of this study were;

- i. To analyze the information security risk management system models employed by SMEs in Kenya.
- ii. To investigate whether there exist other similar information security risk management standards, frameworks and methodologies in use.
- iii. How to quickly and successfully assess the compliance of an SME to ISO/IEC 27005:2011 standard.

1.4 Research Questions

The following research questions came out;

- i. Have SMEs in Kenya employed any information security risk management systems within their organizations?
- ii. Were there other similar information security risk management standards, frameworks or methodologies in use globally?
- iii. How could SMEs in Kenya go about implementing an information security risk assessment and management systems within their organizations?

1.5 Significance of the Study

At the time of this study, little attention was given to research work focusing on information security risk management by SMEs in Kenya. Further to this, we knew little about the standards if any, that SMEs were using at the time to bench mark their information security risk management processes. This was the case despite increased use of information technology by SMEs either as a core business operator or as a complement to business operations.

This study has brought many benefits to different stakeholders. A few of these benefits are;

- i. Scholars can now use the references and the outcome of this study to do further research in this area.
- ii. SMEs in Kenya can now leverage on the software tool that came from this study to do their own information security risk assessments that will help them in identifying gaps in information security.

- iii. For experts in risk, information security and information systems auditors, they can and should use the tool to carry out audits and/or evaluation of an institutions readiness for ISO/IEC 27005:2011 standard certification.

CHAPTER TWO: LITERATURE REVIEW

2.1 GAP Analysis

A way to compare current conditions and practices in order to identify gaps and areas in need of improvement with regards to compliance to the relevant standards or regulatory requirements is known as gap analysis (Lindsay, 2014). Compliance is the process of comparing the applied controls of an organization with those in ISO/IEC 27005:2011 in this case.

Gap analysis is different from risk assessment in the fact that it compares the object against some target, whereas risk assessment is not measured against a target. But for both, they try to bring us to terms with where we are. But gap analysis on the other hand is geared towards where we want to be (Al-Mayahi & Mansoor, 2012).

Gaps can occur in knowledge, skills or business practices and gap analysis is not something done often but when need arises. This need can be to be in compliance with government regulation, as a step towards implementing a global standard towards certification or for business growth.

2.2 Understanding SMEs

The acronym SME stands for Small and Medium-sized Enterprise. According to OECD (2000), these are non-subsidary, independent firms which employ less than a given number of employees, which varies between countries.

In Kenya under the Micro and Small Enterprises Act of 2002, this formed businesses with an annual turnover of USD 5,000 to USD 8 million, employing 10 to 99 employees (ARBT, 2017). The referenced report further stated that the importance of the SME in economic growth could not be understated since 80% of the jobs that were created in Kenya in 2014 were in the small and medium-sized enterprises and the number was expected to grow in the coming years. That clearly showed how SMEs were a major contributor to the country's socioeconomic development.

Even with its huge contribution to the economy, SMEs were faced with major challenges that affected their growth and hindered their access to global markets. Some of these were inadequate capital, poor infrastructure, inadequate knowledge and skills and rapid changes in technology (Deloitte, 2016). These challenges posed a risk factor especially for SMEs in the technology sector.

2.3 Information Security Risk Management (ISRM)

ENISA technical report of 2006 defined risk management as a process aimed at balancing between realizing opportunities for gains and growth and at the same time minimizing vulnerabilities and

losses (ENISA, 2006). The report further stated that it was a core part of management practice and an essential element of good corporate governance.

Risk management is a continuous cyclic process consisting of many activities. These activities in order of steps are context establishment, risk assessment; identification, analysis and evaluation of risk, treatment of risk which is followed by continuous monitoring. This cyclic process focuses on achieving a coordinated and economical application of resources to control the probability of an unfortunate event and/or minimize its impact (Hubbard, 2009).

The figure below shows a high level overview of the risk management process as specified in ISO 31000.

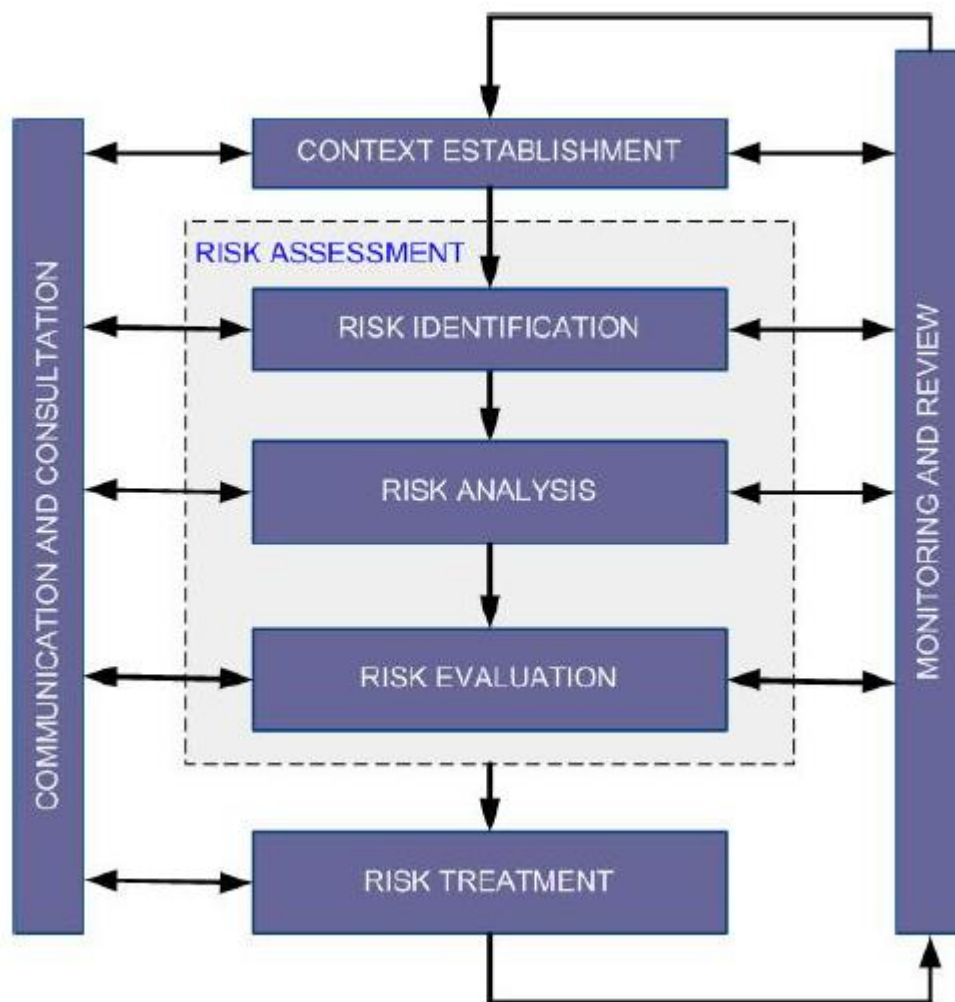


Figure 1- The Risk Management Process. Source ISO 31000

Prior to dealing with any risk, it is prudent to understand the context in which it exists as this sets the boundaries for dealing with the latter. Context can be set by understanding the environment within which the organization operates in, its objectives, core activities and its operations.

A key step in risk management process is risk assessment. This step consists of risk identification, risk analysis and risk evaluation. It is worth noting that even though risk assessment is a step within risk management, it is not continuous and repetitive as it is only initiated when required (Ionita, 2013).

Ionita (2013) described the three steps within risk assessment as follows; risk identification employs available data to identify possible attack vectors and vulnerabilities of the system. That is, what could go wrong and what is the consequence of it occurring. Risk analysis on the other hand deals with understanding the probabilities, impacts and other related parameters associated with the identified risks. The final step, risk evaluation, entails ranking and prioritizing risk. That is analyzing the likelihood and consequences of each identified risk and deciding which risk factors will have the greatest effect and should be given priority in management.

The final step in risk management process is risk treatment. This is putting in controls on the identified risks. Treatment options can be mitigation, avoidance, sharing or acceptance (Berg, 2010). SANS publication of 2007 elaborated on these treatment options by defining risk mitigation as involving fixing the flaws or providing some type of compensatory control to reduce the likelihood or impact of the flaws. An example is installing a patch from the vendor to fix a security flaw.

Risk sharing is the process of allowing another party to accept the risk on your behalf. An example is having insurance cover your I.T infrastructure together with the systems. It is worth noting that this does not fix the flaw or even reduce it, but rather reduce the financial impact on the organization (Elky, 2006). Acceptance is the practice of simply allowing the system to operate with a known risk. This includes low risks and those that are highly costly to mitigate. Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself (Elky, 2006).

Monitoring and reviewing is an ongoing part and parcel of risk management that is very important to every step of the process. With this comes communication to organizational management in a language easy to understand (Elky, 2006). Communication involves updating the management with where the organization stands as far as risk management is concerned.

2.4 Current Standards in Risk Management

2.4.1 AS/NZS 4360:2004 (AS/NZS ISO 3100:2009)

Introduced in 1995 followed by a revision in 2004 by the joint committee of the Australian and New Zealand International Standards (AS/NZS, 2004). It was and still is a generic framework for managing risk which divides the elements of the risk assessment process into several sub-processes. That is establishing the risk context, identifying the risks, analyzing the risks, treating the risks and two other concurrent processes; monitoring and review, and communication and consultations. The process is graphically depicted in figure two below.

This standard was superseded by AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines also by the same committee. The new edition set eleven risk management principles an organization should comply with, and a management framework for the effective implementation and integration of these principles into an organization’s management system (Lenin et al, 2014).

Its strength was on considering risk in terms of the effect of uncertainty on objectives, rather than the risk incident. The principles as was summarized by Knight (2010) are;

- i. create and protect value by contributing to the achievement of objectives and improved performance
- ii. be an integral part of organizational processes; from the setting of organizational objectives to strategic planning, project management and operational activities
- iii. be an integral part of the decision-making process, so that decisions are the right ones and can be managed to a successful outcome
- iv. explicitly address ‘uncertainty’
- v. be systematic, structured and timely
- vi. be based on the best available information, and acknowledge any data limitations
- vii. be based on the organization’s risk profile, and risk appetite for given situations
- viii. recognize the impact of the human, cultural and environmental paradigms of the organization on the achievement of objectives
- ix. address the perceptions of stakeholders, not just company management
- x. be dynamic and responsive to change and take account of new or emerging risks and
- xi. be continually improving as the organization matures.

Harpers et al (2014) pinpointed that because of its broad applicability, it offered almost no practical guidelines for its implementation, leaving that to the actual assessor. For non-experts this could lead to ambiguities regarding certain sub-processes and their correct implementation.

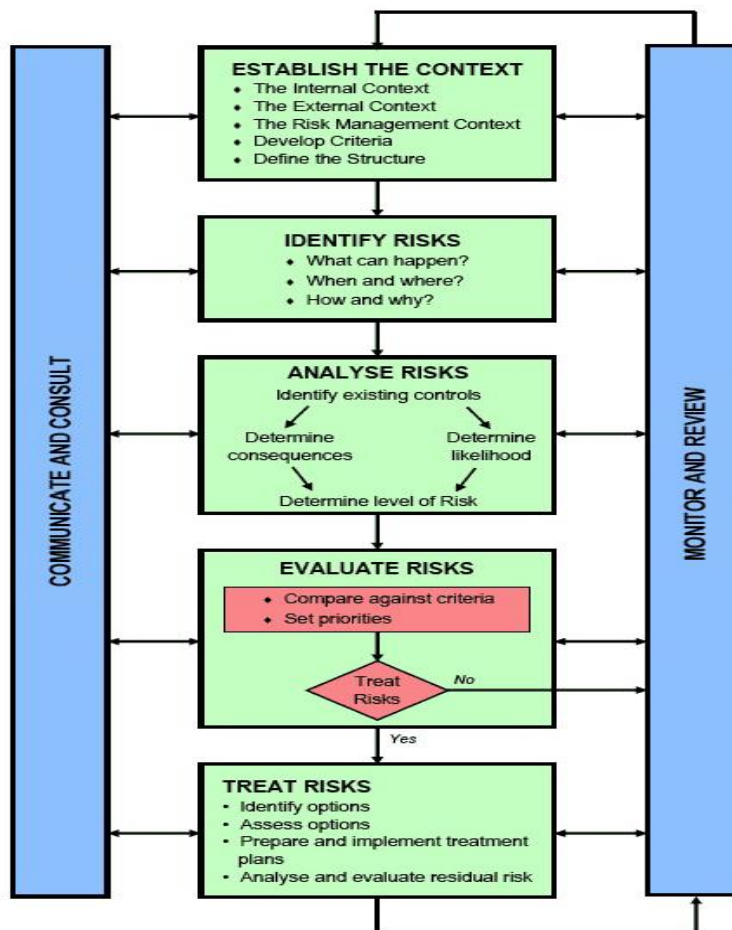


Figure 2- AS/NZS 4360:2004 Risk Management process. Source (Herpes et al, 2014)

2.4.2 NIST Special Publication 800-39

The NIST - National Institute for Standards and Technology publication 800-39 was created in 2011 by the U.S Department of Commerce in response to Federal Information Security Management Act (FISMA). The publication was and still is a generic standard providing guidance for managing information security risk within the U.S government federal information systems (NIST, 2011).

It provided a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines (NIST, 2011).

Haythorn (2014) stated that the standard defined risk as a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization. The standard proposed a risk management process consisting of several

steps which had inputs and preconditions, activities with associated tasks and outputs with post conditions.

The steps according to Harpes et al (2014) are Risk framing consisting of Risk assumptions, Risk constraints, Risk tolerance, Priorities and Trade-offs. Risk assessment consisting of threat and vulnerability identification and risk determination. Risk response having risk response identification, evaluation of alternatives, risk response decision and risk response implementation. Risk monitoring consisting of risk monitoring strategy and risk monitoring event.

2.4.3 ISO/IEC 27005:2011

ISO/IEC 27005:2011: Information technology - Security techniques - Information security risk management was and still is a publication of the International Organization for Standardization (ISO) and the International Electro-Technical Commission (IEC), hosted in Geneva Switzerland (ISO, 2011). First publication was in 2008 followed by a revision in 2011 hence the name 27005:2011.

The standard provided and still provides guidance for information security risk management within an organization supporting the requirements of information security management according to ISO/IEC 27001. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization (ISO, 2013).

The ISO/IEC 27005 Standard assists organizations, whether big or small, whether in government or private sector, in implementing information security based on a risk management approach. The process outlined by the standard is to identify the information assets that are at risk, the potential threats or threat sources, the potential vulnerabilities and the potential consequences if the risks materialize (Haythorn, 2014).

ISO/IEC 27005 (2011) however gives a caveat that the standard does not provide any specific method for information security risk management, this is up to the organization to define their approach to risk management basing on the scope of the information security, context of risk management or industry sector.

The Standard, as shown in figure three below provides an iterative process for information security risk management consisting of seven stages or clauses; context establishment, risk assessment within which we have risk identification, risk analysis and risk evaluation, risk treatment, risk communication and consultation, monitoring and review.

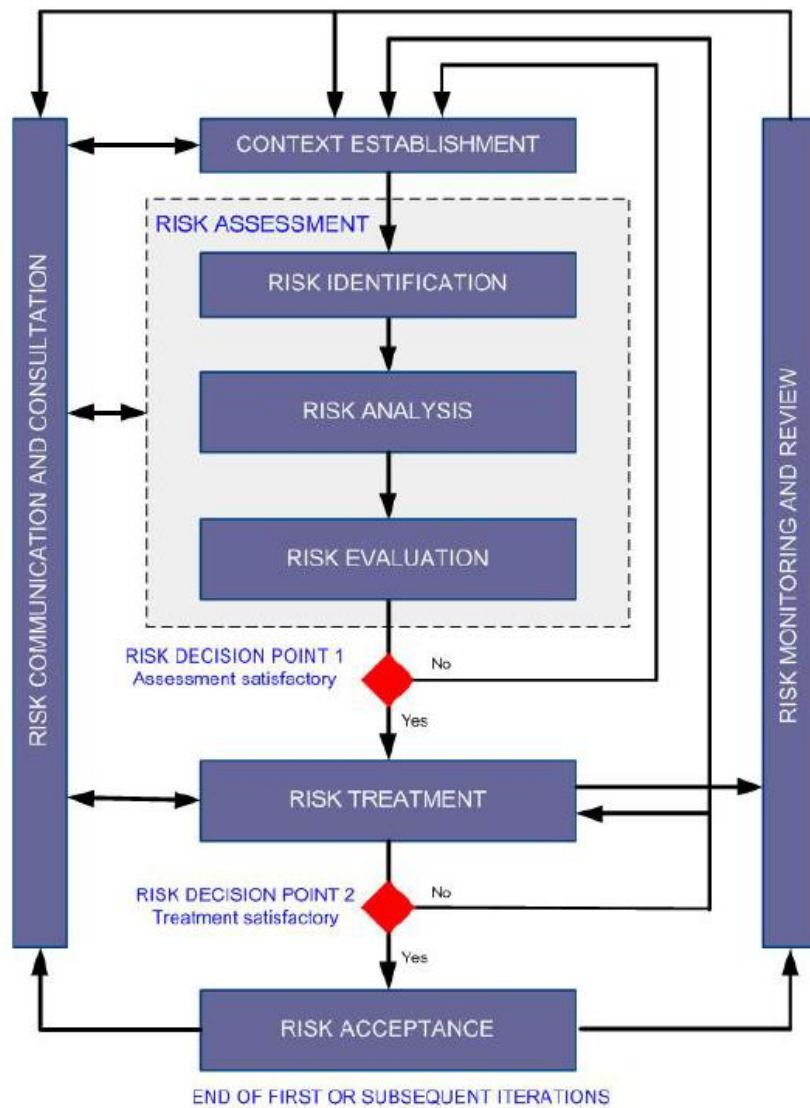


Figure 3 - ISO/IEC 27005:2011 Information security risk management process. Source (ISO, 2011)

Firstly, the context is established then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. If otherwise, then another iteration of the risk assessment with revised context will be conducted (ISO, 2011). Let's expound into these stages to get deeper understanding of each.

Context establishment is all about information about the organization relevant to the information security risk management. This involves setting the basic criteria necessary for information security risk management, defining the scope and boundary, and establishing appropriate resources to operate the information security risk management (ISO, 2011).

Basic criteria is all about selecting or developing the appropriate risk management approach that addresses risk evaluation criteria, impact criteria and risk acceptance criteria. Issues to be

considered when developing a risk evaluation criteria are; business strategic value, criticality of the information assets involved, legal and regulatory requirements, contractual obligations, operational security and stakeholders' expectations and perceptions (ISO, 2011).

The Standard states that the scope and boundary of the information security risk management is defined by the organization, having in mind the critical assets and the operating environment. The scope of information security usually consists of the organization's strategic business objectives, functions, legal requirements, contractual requirements, information security policy, overall approach to risk, geographical locations, constraints and interference.

The second stage in information security risk management as per the standard (ISO, 2011) is information security risk assessment. This stage determines the value of the information assets, identifies the threats and vulnerabilities that exists, existing controls and their effect on the risk identified, determines the potential consequences, and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.

Activities involved in risk assessment are; risk identification, risk analysis and risk evaluation. The purpose of risk identification is to determine what may happen to cause a potential loss and understand how, where and why the loss might happen (ISO, 2011). Steps involved in risk identification are; identification of assets, identification of threats, identification of existing controls, identification of vulnerabilities and identification of consequences.

A second activity within risk assessment is risk analysis, within which we have the methodologies to be employed, either qualitative or quantitative, assessment of consequences and incident likelihood, and determination of the level of risk. Qualitative risk analysis uses a scale of qualifying attributes to describe the magnitude of potential consequences and the likelihood of them occurring. Quantitative analysis on the other hand uses a scale of numerical values for both consequences and likelihood by using data from many sources.

The closing activity within risk assessment is risk evaluation. The purpose of risk evaluation is to prioritize risk treatment considering the levels of risk.

The third major stage within information security risk management is information security risk treatment. These are controls to reduce, retain, avoid or share in the risk and coming up with a risk treatment plan. ISO (2011) defines four options for risk treatment; risk modification, risk retention/acceptance, risk avoidance and risk sharing. Selection of these options is based on the outcome of the risk assessment, the expected cost for implementation and the expected benefits.

Risk modification is achieved through amending the controls which may protect the assets through correction, prevention, elimination, deterrence, detection, impact minimization, recovery, monitoring and awareness. Risk retention is accepting risk as is depending on risk evaluation and risk acceptance criteria.

Risk avoidance can be achieved by either completely avoiding an activity or risk which causes the condition. This option is best when the cost of treating a risk is high or the risk itself is too high. Risk sharing is involving other third parties like insurance companies that will support the consequences or sub-contractors who would monitor the information systems against an attack.

Information security risk acceptance follows risk treatment. Within this stage, the management needs to make a decision about the risk acceptance of the residual risk, subsequent to justification for the risks that do not meet the organization's risk acceptance criteria (ISO, 2011).

2.5 Current Methods and Frameworks in Information Security Risk Management

2.5.1 CRAMM

The acronym stands for CCTA Risk Analysis and Management Method. A risk analysis methodology together with a tool of the same name, developed by the British government to solely be used in risk analysis. CRAMM is not limited to Britain alone, it is also used by other countries for justifying investment in security at management level and also for benchmarking the security of an organization (ENISA, 2013).

The CRAMM process consists of three phases as per CCTA (2011); asset identification and valuation which is done via interviews, threat and vulnerability assessment to systems, and finally selection of mitigation strategies.

The cons of CRAMM are that it is limited to large government organizations, it requires expert knowledge to operate and it relies heavily on its dedicated tool (Harper et al, 2014).

2.5.2 FAIR

Factor Analysis of Information Risks (FAIR); a risk analysis methodology that relies less on the practitioner's experience or best practices and instead derives output from repeatable, consistent and financially sound computations (Harper et al, 2014).

The FAIR process comprises of ten steps in four stages (Jones, 2006). At stage one we have identification of assets at risk and identification of threat community under consideration. Stage two comprises of estimation of threat event frequency, estimation of threat capability, estimation of control strength, derivation of vulnerability and derivation of loss event frequency. Stage three

consists of estimation of worst case loss and probable loss while stage four is all about deriving and articulating risk.

According to Harpes et al (2014), the disadvantage of FAIR is that it only assists basic risk analysis on single assets and expert training will be required to do the same for a system wide analysis.

2.5.3 OCTAVE

The Software Engineering Institute at Carnegie Mellon University developed the Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) process (Alberts et. al, 1999). The main goal of the OCTAVE methodology is to help organizations in improving their ability to manage and protect themselves from information security risks (Steve, 2006).

The methodology is workshop-based rather than tool based, this forces the participants in the risk assessment to understand the risk and its components rather than relying on an expertise of a security tool. With this approach, the organization will understand the risk better than the tool and the decision made will come from the latter than the former (Steve, 2006).

The workshop consists of three phases and eight processes. Phase one gathers asset-based threat profiles critical to the organization and current employed security mechanism. Phase two is all about examining the information infrastructure in order to identify technological vulnerabilities that can lead to unauthorized action against critical assets. Phase three deals with developing security strategies and plans to mitigate identified risks (Harpes et al, 2014).

According to Harpes et al (2014), the con of this methodology is that it is intensive due to the many volumes, worksheets and processes involved and the skilled personnel that will be required.

2.5.4 RISK IT

A framework developed by ISACA to complement COBIT and Val IT frameworks in order to offer a more complete IT governance guidance resource. The main objective of this framework is to allow enterprises to make appropriate risk-aware decisions by providing an end to end comprehensive view of all risks related to the use of IT and thorough treatment of risk management at all levels (ISACA, 2009).

This framework has three processes. The first process entails relevant data collection to enable effective IT related risk identification, analysis and reporting. This is followed by a thorough risk analysis to come up with a risk profile that would be maintained to build an inventory of known risks and their attributes, and finally risk treatment (Harpes et al, 2014).

The disadvantage of this framework is that it does not go into technical details in describing risk assessment rather it gives guidelines to be followed in undertaking the process and secondly the framework is made for large organizations and to be consumed at the CIO level (Harpes et al, 2014).

2.5.5 EBIOS 2010

Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) methodology was developed by French Central Information Systems Security Division with the aim of helping management in decision making as far as assessment and treatment of risks associated with information systems is concerned (ENISA, 2013).

EBIOS follows five phases; phase one deals with context establishment, phase two deals with security requirements which are based on the feared security events, while phase three covers a risk study conducted in order to identify and analyze threat scenarios. In phase four, information from the previous steps is used to identify risks and describe the necessary and sufficient security goals relating to these risks. In phase five, necessary security controls are determined, and any residual risk is made explicit (Harpes et al, 2014).

A major throwback of this methodology, apart from having a complementing tool build on the five phases above, is that it is made for French organizations and has its operating language in the latter. This has made this methodology and the tool not to be used outside of France (Harpes et al, 2014).

2.5.6 CORAS

A platform for risk analysis of critical security systems managed by the open source community. The aim of the CORAS project is to build a practical model-based framework and computerized support for precise, unambiguous and efficient risk assessment of security-critical systems (Harpes et al, 2014).

It is dependent on its own modeling language, an extension of UML that can be used in conjunction with risk assessment to serve three goals; describing the assessment target, as a communication for different group of stake holders and for documenting the results and underlying assumptions (Raptis et al, 2002).

A few concerns noted by Harpes et al (2014) on this methodology is that it requires expert knowledge from various backgrounds, it is lengthy and it is also outdated.

2.5.7 MAGERIT v3 2014

A Risk Analysis and Management Methodology for Information Systems – MAGERIT was developed by the Spanish government to assist with management of information systems risks (MAGERIT, 2014).

Main goals of MAGERIT (2014) is to make information system stakeholders aware of the existence of risks and need for treatment, offer a systematic method for analyzing these risks and help in describing mitigation measures and also to prepare the organization for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case.

MAGERIT operates under five key steps. Step one identifies the assets to the organization, their inter-relationship and their value. Step two determines threats the assets are exposed to. Step three determines the available safe guards and countermeasures and how effective they are. While steps four and five is all about estimating the impact of the threat and the risk respectively, occurring on the asset. At the end of the analysis, it is recommended that step four and five be revisited in order to identify potential residual impact or residual risk (Harpes et al, 2014).

2.5.8 MEHARI

Method Harmonisee d'Analyse de Risques, which translates in English to Harmonised Risk Analysis Method. A risk assessment methodology developed in 1996 by the Club de la Sécurité de l'Information Français (CLUSIF), a non-profit information security organization (Behnia, 2012).

MEHARI was designed to support the implementation of ISO/IEC 27005 and it is aimed at executive personnel within an organization (CLUSIF, 2010). The method supports quantitative, scenario-based analysis of risk, similar to the one described in the ISO/IEC 27005 standard.

MEHARI makes use of a knowledge base of risk in order to support semi-automated procedures for evaluating risk for each individual scenario based on a set of input factors. These procedures are based on predefined formulas and parameters (Ionita, 2013).

The cons of this methodology are that it requires expert knowledge and can only be used in conjunction with a supporting software tool. Two versions of this tool exist; a commercial one and a limited free one based on Microsoft excel (Ionita, 2013).

2.6 Related works in Information Security Risk Management tools aligned to ISO/IEC 27005

Related works in this section considered risk management tools in the market that were compatible with the ISO/IEC 27005:2011. The research works of Ionita (2013), current established methodologies and tools in risk management was aimed at listing and comparing all risk management methodologies, frameworks and tools in the area of information security risk management.

From their list of twenty-five risk management tools, twelve were found to be aligned with the standard under this study. They were Acuity Stream, CCS Risk Manager, Countermeasures, EAR / PILAR, Ebios, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot, RM Studio, TRICK light, Verinice and vsRisk.

From their study and of the above twelve, we noted that expertise in risk management and information security is very necessary in order to use these tools. In addition, most of these tools were not offered for free. The only free part that a user could take advantage of was the free trial versions which were limited to either a number of days of use or the availed features. Expert knowledge especially in information security risk management and finances were limited resources to SMEs globally and Kenya was no exception.

Kunder and Clarke (2010) in their study of identifying problems SMEs face in conducting risk analysis, they came up with a methodology and a web based tool that uses organization based profiling. The organizational profiling method used an evaluation table to identify risk context which was derived from the business and the external environment categorized into four risk areas as legal and regulatory, reputation and customer confidence, productivity and financial stability.

Further to selecting the organizational profiles, controls were identified and were mapped corresponding to the assets identified. Controls could either be organizational based or asset based. Organizational in the sense that they were applicable to the organization horizontally and were concerned with practices and management procedures. While asset based controls were applicable to critical assets and were category specific (Kunder & Clarke, 2010).

In their study, they noted a gap within their tool that future researchers could leverage on to come up with a comprehensive tool. They noted that a feedback system is necessary to assist the user in post assessment by suggesting controls that would be implemented to reduce certain threats.

2.7 Conceptual Model of the study

The work that was carried out by this study was to come up with an easy to use software tool that could be used by SMEs in Kenya to conduct a compliance gap analysis with respect to ISO/IEC 27005:2011 standard. With this in mind, the conceptual framework of this study was borrowed from the process of managing information security risk as was portrayed in the Standard ISO/IEC 27005:2011. This is graphically represented in the figure below.

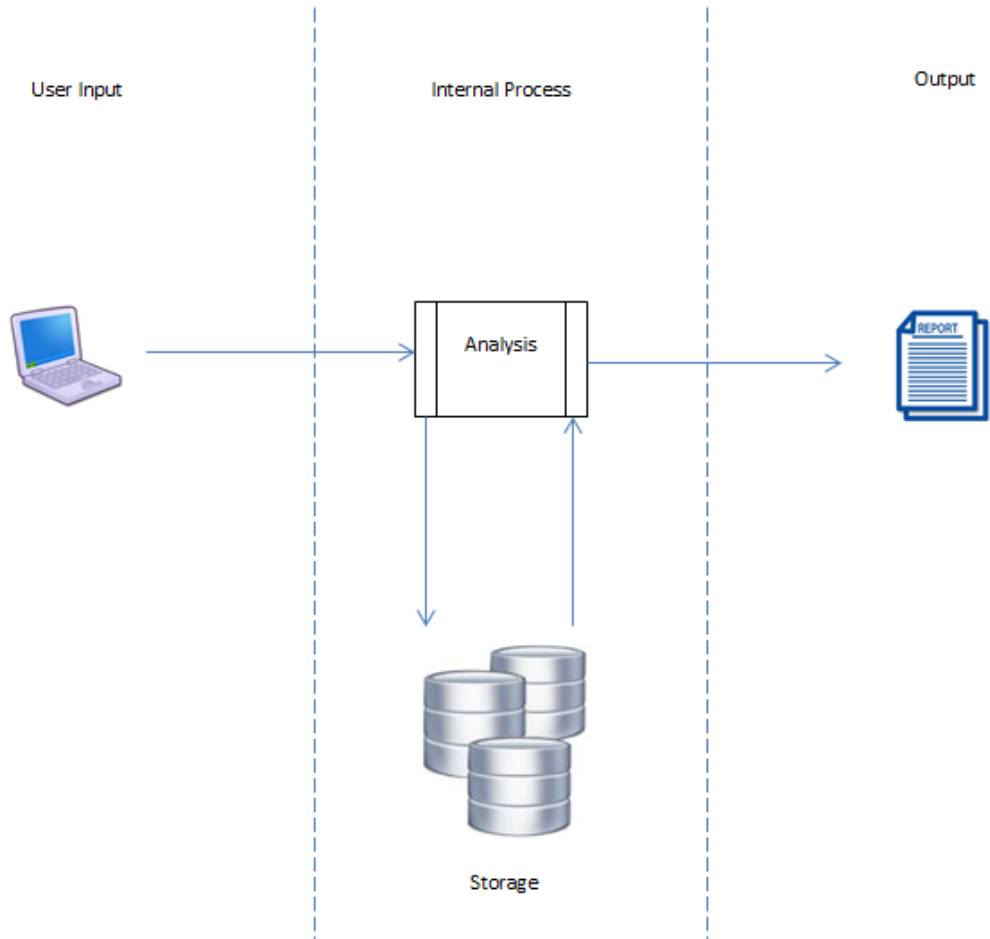


Figure 4 - Conceptual Model

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design

Research design is the researcher's blue print for carrying out a study with maximum control over factors that may interfere with the validity of the outcome (Burns & Grove, 2009). Parahoo (2006) defined research design as a plan stating how, when and where to collect and analyze data. Research design is also the researchers' way of coming up with answers to the posed research questions or testing the researcher's hypothesis (Polit et al, 2001).

In this study, the researcher used a descriptive qualitative research design because the sample size of the population that was used in the study was small and data was collected using interviews and questionnaires.

Dawson (2002) explained that qualitative research does not use statistical summary or analysis to quantify results but rather the approach involved interviews and observations. It was descriptive in the sense that data was collected from particular organizations to obtain a picture of information security risk management within the latter.

The advantage of this approach when gathering study data according to Dawson (2002), was that they are more open to changes and refinement of research ideas as the study progressed.

The steps that were followed while undertaking this study took the following sequence;

- i. Data collection by first developing a questionnaire and secondly conducting interviews and distributing the questionnaires to respondents
- ii. Data analysis from the filled questionnaires
- iii. Systems analysis where both functional and non-functional requirements were determined
- iv. Systems design and development based on the requirements
- v. System testing with the respondents

3.2 Study Population

Polit and Beck (2004) defined population as an aggregate or totality of all the objects or members that conform to a set of specifications. For this study, the researcher's population were SMEs in Kenya where information technology formed the core heart of their business. Within this group, the focus was on deposit taking microfinance institutions, institutions dealing with ecommerce but specialized in online shopping and institutions handling online payments.

In 2017, the Kenya Bureau of Statistics reported that as at December 2016, there were 50,043 licensed SMEs (KNBS, 2017). Less than 1% of this figure fell in the study population. As at the end of 2016, there were 13 deposit taking microfinance institutions (CBK, 2016), 9 online shopping websites and 5 online payment providers (Infohub, 2016).

3.3 Sampling Design

Selecting a part of the population to represent the entire population is called sampling (Polit & Beck, 2004). The sampling technique the researcher employed in this study was of probabilistic type and the sampling strategy used was simple random sampling. Probability sampling as defined by Polit & Beck (2004) involved random selection in choosing the elements.

Probability sampling was used because it gave the best chance of creating a sample that was truly representative of the population. This was different from non-probabilistic where every element does not have a chance of inclusion (Polit & Beck, 2004). The simple random technique was used due to its low error rate.

Neuman (2003) in his book titled, *Social Research Methods: qualitative and Quantitative Approaches*, stated that a 10 to 20% of the accessible population was an adequate sample size in a descriptive research study. As per Neuman, this gave the researcher a sample size of 6 elements, but to have confidence and be representative of the population, the researcher used a confidence level of 80% to come up with a sample size of 21 from the population.

3.4 Data Collection

The researcher utilized a survey as a research strategy and collected data from the sample population using interviews and questionnaires. Further to this, analysis of the collected data was used to confirm and ascertain the need for the proposed gap analysis tool and also to form part of the non-functional requirements. A detailed document review of the ISO/IEC 27005:2011 standard was also conducted to determine the application functional requirements.

The choice of a survey as one of the data collection tools by the researcher was because of its unique advantages such as data coming from real world observations and the respondents were the actual users on the ground, and also the sample population used in the study formed a generalized view of the entire population and this was expected to save on cost and time (Kelly et al, 2003).

The researcher conducted a survey of the various SMEs in Kenya where information technology formed the core heart of their business. Examples of such SMEs were deposit taking microfinance institutions, institutions dealing with ecommerce, institutions handling online payments and many others that fell in these areas.

The researcher employed semi structured interviews coupled with open and closed ended questionnaires to twenty of the identified SMEs to assess the level of importance they put to information security risk management and if any, the adequacy of an information security risk management policy or procedures and further to this, which globally recognized standards, frameworks or methodologies do they adhere to.

Interviews and questionnaires were used by the researcher because of their practicality and ease of administration especially for the latter. The questionnaires were developed to capture the following information;

- i. General business information such as static details and area of specialization
- ii. Awareness of Information Security Risk Management by the identified SMEs
- iii. Awareness of global standards, frameworks in Information Security Risk Management
- iv. How the identified SMEs conduct their Information Security Risk assessment
- v. Standards, frameworks employed by the identified SMEs in Information Security Risk Management
- vi. Existing personnel capability to conduct an Information Security Risk assessment as per ISO/IEC 27005:2011

The questionnaires targeted personnel within the identified SMEs who had executive decisions on the organization or persons who were senior and made decisions on the direction to be taken by the latter. These were the CEOs, MDs, Information Security Managers, IT Managers and or any other personnel whose position within the organization was mandated with information security risk management.

3.5 Data Analysis

Analysis of the responses from the questionnaires were done using Microsoft excel worksheet. The researcher used this tool because of its familiarity, accessibility and ease of use. The analyzed responses from the SMEs was displayed with the aid of graphs, charts and tables and from which was used to gauge the need for the proposed gap analysis tool and the viability of the same.

The researcher used the feedback from the respondents to confirm and ascertain the need for the proposed gap analysis tool and also to form part of the non-functional requirements since the functional requirements were picked from the review of the ISO/IEC 27005:2011 standard document, which is covered under the system analysis sub section.

3.6 System Analysis

Results of analysis of the data collected via the questionnaires and the detailed review of the standard under study formed the foundation for the system analysis and design phase of this research work. This phase had three steps; modeling of the requirements from the ISO/IEC 27005:2011 standard, design and development of the gap analysis tool, and a test of the latter which involved surveyed SMEs to confirm validity.

The first step as stated above was requirements definition. This covered both functional and non-functional requirements. Functional requirements basically described what the software must do while non-functional on the other described the behavior and appearance of the software. Functional requirements were must haves while non-functional requirements were classified as nice to have, they assist the application to operate smoothly.

The following were the functional requirements of the gap analysis tool as per the ISO/IEC 27005:2011 standard. The application is;

- i. Able to identify assets
- ii. Able to identify threats to assets
- iii. Able to identify existing controls to the threats
- iv. Able to identify consequences/impacts of the identified vulnerabilities
- v. Able to quantitatively and or qualitatively assess the level of risk given the assets, threats, existing controls and vulnerabilities
- vi. Able to communicate the results of risk assessment to relevant stakeholders via meaningful reports

The non-functional requirements of the application were;

- i. Reliable enough to perform the task it was developed for
- ii. The user expected it to be easy to learn and use
- iii. The user interface was expected to be aesthetically pleasing, clear and consistent

3.7 System Design

As part of the design phase, the researcher used the Rapid Application Development (RAD) method of software development. RAD relates to projects based on tight timescales, uses prototyping and uses high level development tools and techniques (Coleman & Verbruggen, 1998).

The advantage of this methodology was that it concentrated on quick development and delivery of a high quality working prototype at a low cost (Farrell, 2007). Another advantage of RAD

according to Farrell was that changes to the design or development could be introduced anytime in the development process. These sentiments were also echoed by Despa (2014).

RAD was used by the researcher due to the limited time of this research work, the need to come out with a working prototype as one of the deliverables and also the fact that changes to the design or development could be introduced anytime in the development process.

Below is an illustration of the gap analysis tool system architecture, as was defined by the functional requirements set out in the system analysis section.

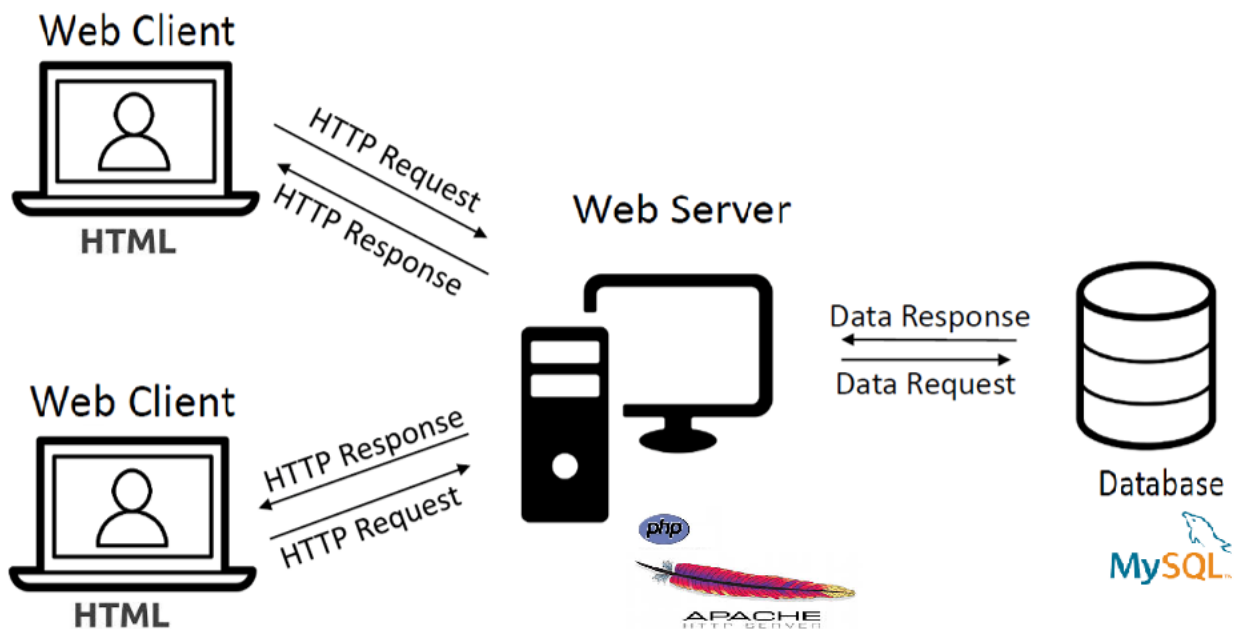


Figure 5 - System Architecture

3.8 System Development Tools and Technologies

The researcher used open source tools in the development of the gap analysis tool. The reason behind the choice was that open source tools were free, easy to learn, easy to use and the researcher was also very conversant with the specific tools used.

For front end development, the tool of choice was PHP complimented with HTML. PHP as the programming language was chosen because of its object oriented background and its integrated development environment that was easy to learn and use.

To cover back end, the researcher used MySQL database management system. The choice of the researcher was due to the advantages of this database system. That is, ease of use, speed of query execution, concurrency and the fact that it was free.

3.9 System Testing

The final user acceptance testing of the software tool was done together with the surveyed SMEs. Testing was one of the ways of confirming the validity of the application and both the functional and non-functional requirements that were stated earlier. A risk assessment report drawn at the end of the process, showing the risk level also helped in confirming validity.

3.10 Ethical Considerations

This study involved the participation of human respondents and institutions that wanted to remain anonymous. To this effect, the researcher gained consent from the relevant persons within the institutions under survey and also maintained their confidentiality and privacy as was promised.

CHAPTER FOUR: RESULTS AND DISCUSSIONS

4.1 Analysis of Survey Results

This section presents the analysis of the data obtained from the survey questionnaire filled by respondents from the SME sector where information technology forms the core of their business operations. A total of 40 questionnaires were given out via the Google forms platform between 21st February 2018 to 30th March 2018, and 33 responses were received, forming an overall response rate of 85%.

The survey was largely completed by IT/ICT management personnel, IT/ICT Security personnel, Systems Administrators, Heads of ICT and IT Risk and Compliance personnel. Appendices B and C both shows a copy of the introduction letter and the questionnaire that was used in the survey.

The survey questionnaire had three sections covering different items. The first section was capturing respondent's demographic information such as static details on self and institution. The second section was targeting respondents' awareness on information security risk management vis-à-vis knowledge on global standards, frameworks and methodologies, and skills capacity. The third and last section was more on knowledge and the need for an information security risk assessment software tool. That is the importance of such a tool and what kind of features it should have.

Below is a presentation of the analyzed results from respondents; per section and per question.

4.1.1 General demographic information of respondents

Job Role/Title of respondents	Number of Respondents	% on Total
Head of ICT/IT	2	6%
IT/ICT Manager	9	27%
IT/ICT Service/Channel Managers	3	9%
IT/ICT Security Officer/Managers	5	15%
Systems Administrators	6	18%
IT/ICT Risk and Compliance Manager	2	6%
IT/ICT Technical/Infrastructure Managers	3	9%
Business Systems Manager	1	4%
ICT/IT officers	2	6%
TOTAL	33	

Table 1: Role/Titles of respondents

Category of the Institutions within the SME sector that responded

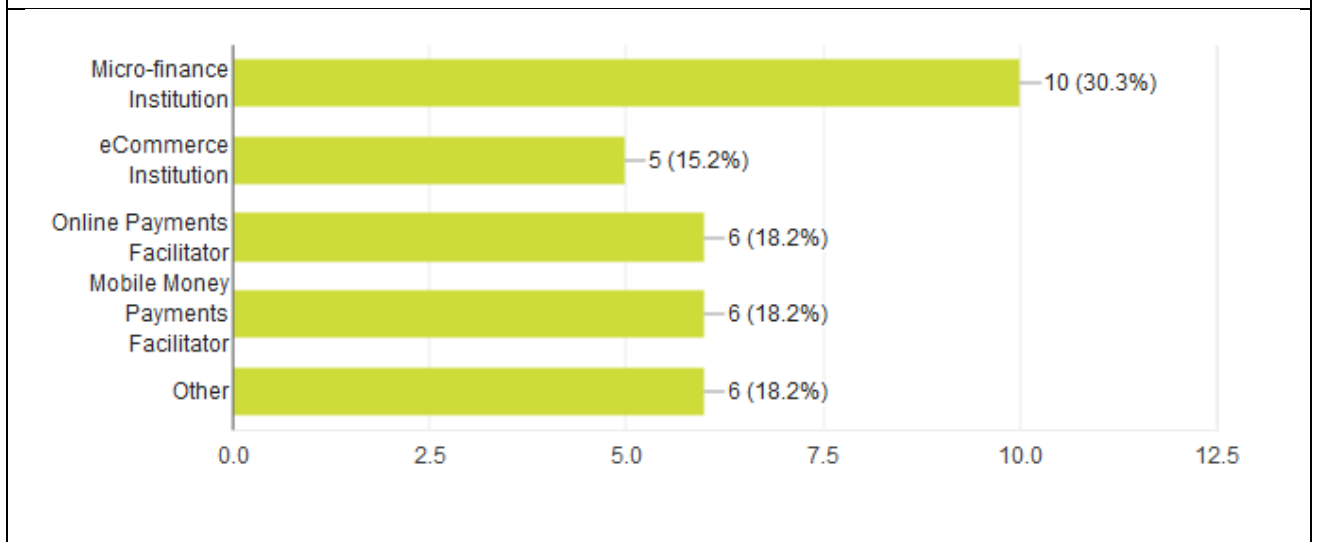


Table 2: Category of the Institutions

Of the surveyed institutions, what were their average ages in business operations

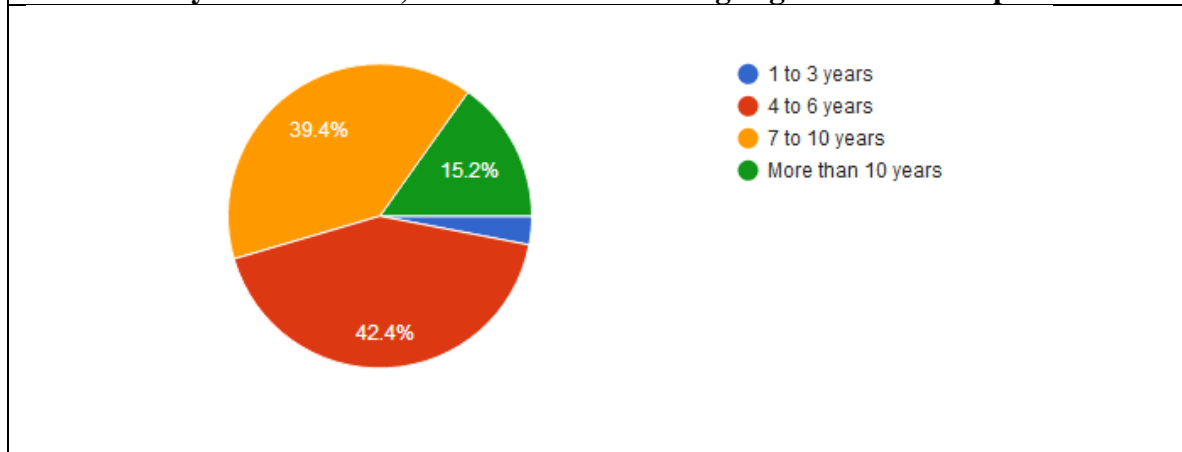


Table 3: Institution ages

Respondents were asked whether their institution has been involved in an information security incident within the last two years. Majority, making 72.7% responded to the negative followed by 24.2% who have had an incident once or twice. Of the 24.2%, 50% had the incident occurring internally and the other 50% had the incident coming from outside.

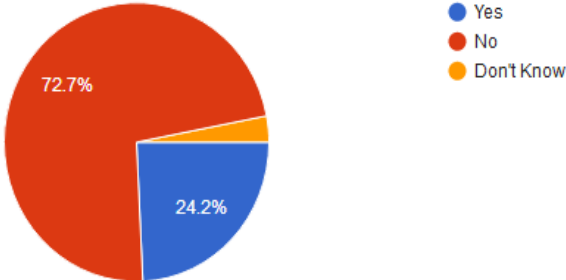
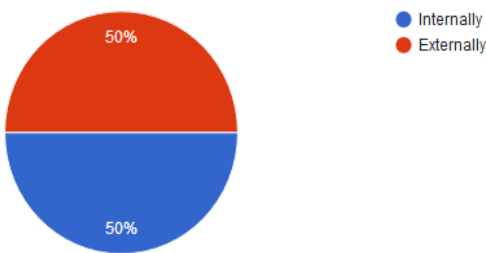
Has your organization/institution been involved in an Information Security Incident in the last two years?	If YES, did the cause originate internally or externally?
 <p>A pie chart with three segments: a large red segment (72.7%), a smaller blue segment (24.2%), and a very small yellow segment (3.1%). A legend to the right identifies the colors: blue for 'Yes', red for 'No', and yellow for 'Don't Know'.</p>	 <p>A pie chart with two equal segments: a blue segment (50%) and a red segment (50%). A legend to the right identifies the colors: blue for 'Internally' and red for 'Externally'.</p>

Table 4: Information Security incidents within institutions

4.1.2 Awareness of Information Security Risk Management

Of the 33 respondents, 97% are aware of what an Information Security Risk Management is. This can be attributed partly to training and partly to general knowledge as can be seen from the charts below.

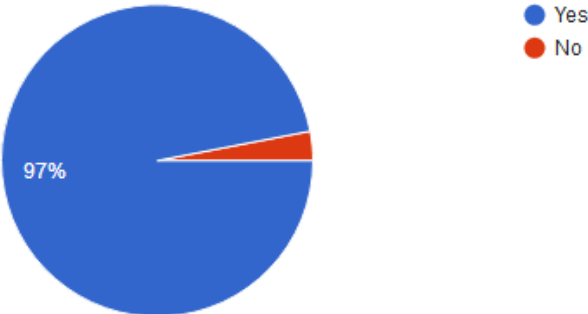
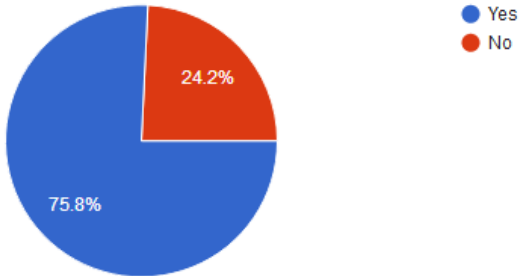
Do you know what Information Security Risk Management is?	Have you been trained on Information Security Risk Assessment and Management?
 <p>A pie chart with two segments: a large blue segment (97%) and a small red segment (3%). A legend to the right identifies the colors: blue for 'Yes' and red for 'No'.</p>	 <p>A pie chart with two segments: a blue segment (75.8%) and a red segment (24.2%). A legend to the right identifies the colors: blue for 'Yes' and red for 'No'.</p>

Table 5: Information Security Risk Management awareness

For the respondents who have had training on Information Security Risk Management, 21.2% confirmed that the training was based on a standard, which tally's with those who also confirmed that their training was based on a framework of the latter. 9.1% of the respondents were not sure what their training was based on. Majority of the respondents on this question which formed the 54.5% responded 'none' which clearly states that their training was not based on a standard, a framework nor a methodology in Information Security Risk Management.

What Information Security Risk Management training was based on

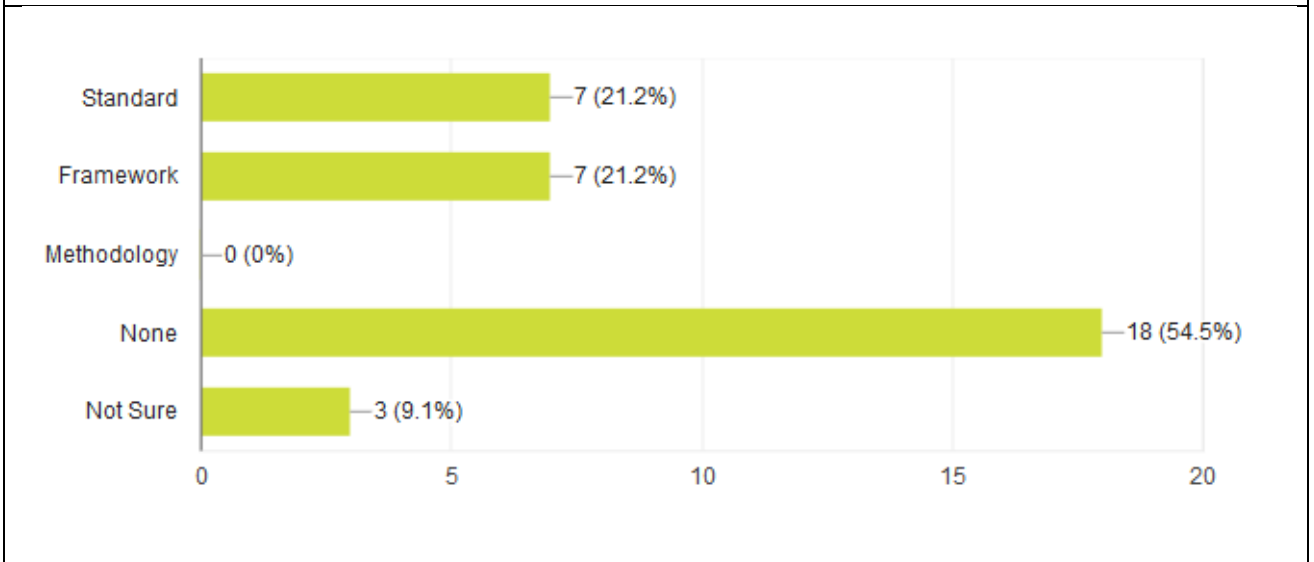


Table 6: Information Security Risk Management training

Respondents whose training was based on a standard or a framework or a methodology

	ISO/IEC 27005 provides guidelines for information security risk management	ISO/IEC 27002 provides guidelines for managing information security	ISO/IEC 27001 describes best practices in information security management	CoBIT 5 for Information Security Risk Management	NIST 800-53 promotes standard for implementing information security controls
Standard	1	5	2		1
Framework				6	

Table 7: Training materials

Respondents were asked what necessitates the trainings within their institutions and how often they are done. Majority at 66.7% stated that they have been trained once and this was necessitated by other things such as skills/knowledge gaps.

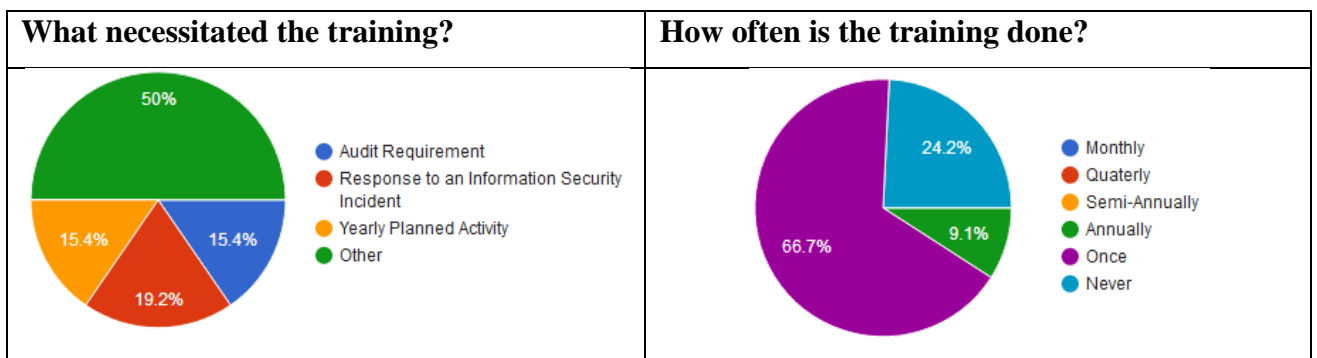


Table 8: Cause and period of training

Respondents were also asked whether their institutions have an Information Security Risk Management Plan and how often they conduct Information Security Risk assessments. 60% of the 33 respondents confirmed that they have an Information Security Risk Management Plan and 57%

of the same number confirmed that they only do risk assessments once a year. These risk assessments are mostly yearly planned and done at least once a year and some are due to audit requirements coming from noted exceptions. 81.5% of the respondents outsource the Information Security Risk assessment services from professional firms and individuals, a clear indicator that most of the SMEs in this study do not have internal capacity for this kind of critical activity.

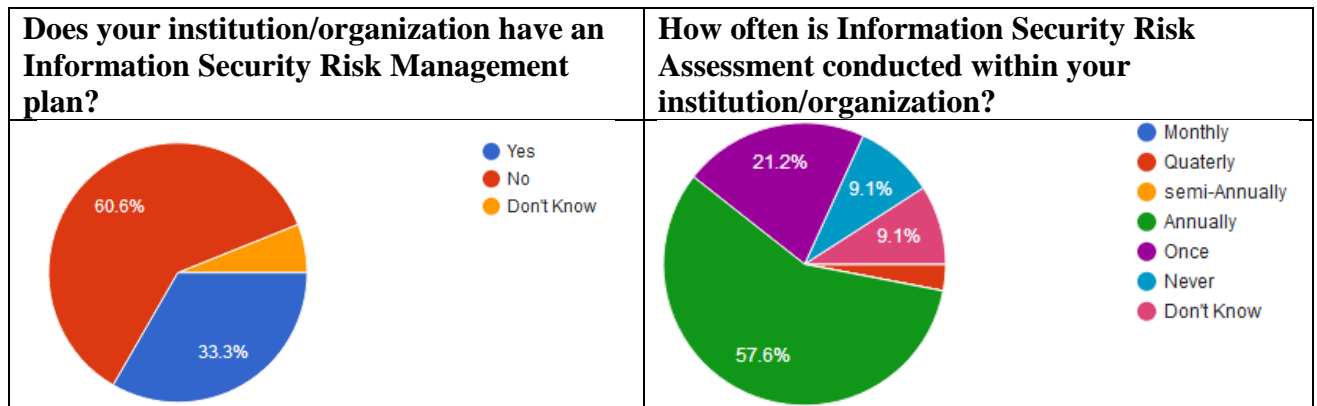


Table 9: Information security Risk Plan

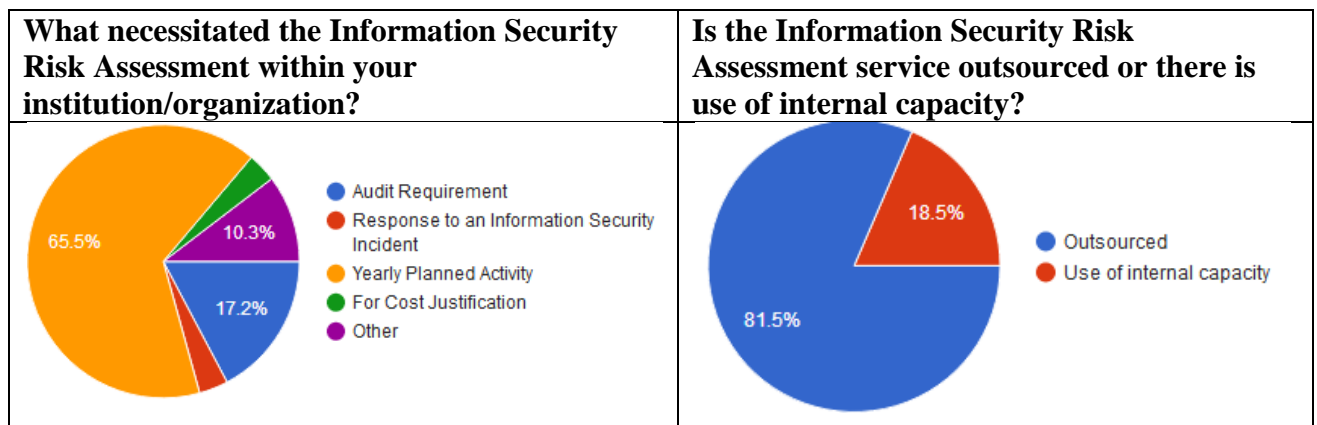


Table 10: What necessitates risk assessment

The researcher also wanted to know the respondents' awareness of any global standards, framework or methodologies relevant to Information Security Risk Management and which ones have been implemented by their respective institutions. 48% of the respondents are not aware of any global standard or framework or methodology in Information Security Risk Management while at the same time, 36.4% are aware of a standard and 30.3% are aware of a framework. Of the 36.4%, 8 respondents are aware of the ISO/IEC 27005, the global standard that pertains to Information Security Risk Management, the standard under study. The same number was recorded for those who are aware of an IS Risk Management framework as provided by ISACA's CoBIT 5.

Respondent aware of global standards, framework or methodology

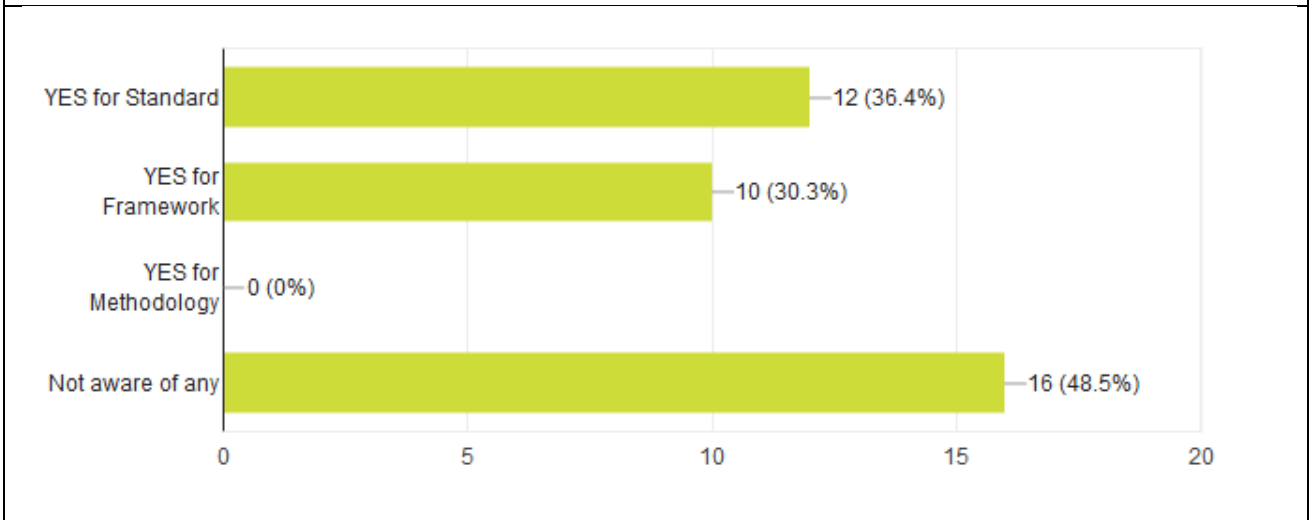


Table 11: Respondent aware of global standards, framework or methodology

Global standards, framework or methodologies respondents are aware of			Global standards, framework or methodologies adopted by respondents institutions
ISO/IEC 27005	Standard	8	0
ISACA CoBIT 5 Risk IT	framework	8	3
NIST	Standard	2	1
ISO/IEC 27002	Standard	3	1
ISO/IEC 27001	Standard	2	2
None			10

Table 12: Global standards, framework or methodologies awareness and adoption

4.1.3 The need for an Information Security Risk Assessment Software Tool

On the need for an Information Security Risk Assessment software tool, respondents were asked whether they are familiar with any and if yes, whether the software tool was purchased by their respective institutions or it was acquired for free via open source communities or developed in-house. They were also asked whether the software tool was based on any global standard, framework or methodology related to Information Security Risk Management.

From the responses, 9.1% are familiar with a software tool for information security risk management and the software tool was mostly purchased and it was not based on any global standard, framework or methodology.

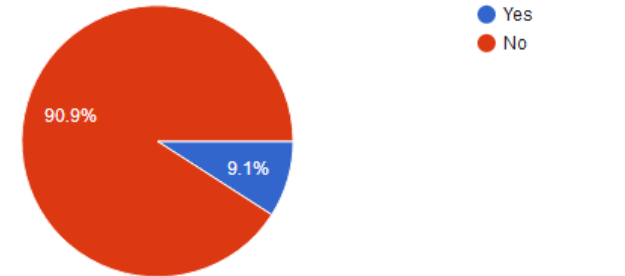
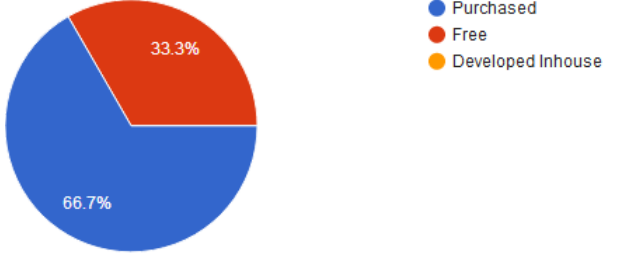
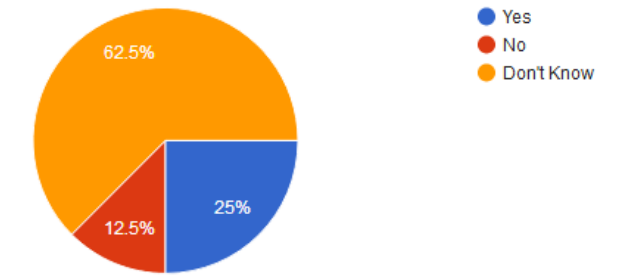
<p>Are you familiar with any Information Security Risk Assessment Software Tool?</p>	 <p>● Yes ● No</p>
<p>If YES, was the software tool purchased or acquired for free (open source) or developed in house?</p>	 <p>● Purchased ● Free ● Developed Inhouse</p>
<p>Is the software tool based on any global Standard, Framework or Methodology in Information Security Risk Assessment and Management?</p>	 <p>● Yes ● No ● Don't Know</p>

Table 13: Familiarity with risk assessment software tool

The researcher asked the respondents whether an Information Security Risk Assessment Software tool is necessary for their institution, 93.9% respondent to the affirmative showing clear indication of the need for such a tool. They were further asked why such a tool is needed within their institution and what kind of features should it have. These responses are displayed on appendices D and E respectively.

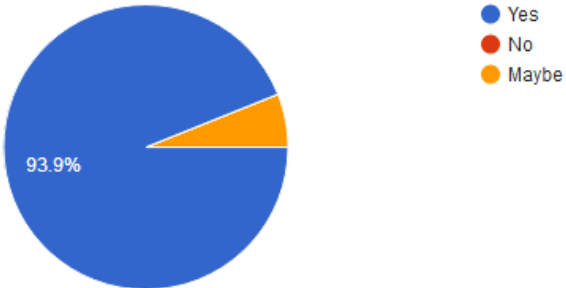
<p>Do you think a software tool for Information Security Risk Assessment and Management is necessary for your institution/organization?</p>
 <p>● Yes ● No ● Maybe</p>

Table 14: Necessity for an information security risk assessment tool

4.2 Prototype Testing

This section presents the results of the testing of the prototype that was done with a few of the respondents of the survey questionnaire from the SME sector where information technology forms the core business operations.

4.2.1 Prototype Usability

All the users who tested the prototype after development found it easy to use since they had some knowledge in risk assessment and having taken part in the survey. They found the application to be very user friendly, does not require training and navigation was not a problem.

4.2.2 User Acceptance Test

The participants who tested the prototype were happy with it and accepted it on the following grounds: -

- i. It was user friendly, easy to learn and navigate through.
- ii. It was a free application hence no cost implications.
- iii. It could be availed in-house or online depending on user choice.
- iv. It was an application that greatly reduced time taken in doing IT security risk assessments.
- v. The generated reports were elaborative and clear to understand.

4.2.3 Prototype Availability

All of the respondents who took part in the survey and tested the software tool can get access to an internet and access the online host and furthermore, the application can be hosted in house either within a central location for authorized persons to access or on a specific user PC who is charged with IT risk management or information security matters.

4.3 Discussion

From the analyzed survey results, it was evident that even though the study population was aware of what an information security risk management was, they lacked proper in house skills and tools to do assessments and gauge their respective institutions compliance to global risk standards. This was further reinforced by the fact that many of the respondents outsource their annual information security risk assessments from professional firms or individuals who have the necessary tools, skills and expertise to handle such tasks.

It was evident from the tests done using the software prototype, together with the feedback from the testers, that Information security risk assessment or IT risk assessment in general is an easy task when a tool specific to the task is used. Having such a tool, as reported by one tester, can make an institution or company do their IT risk assessments as many times within the year. A free

and easy to use information security risk assessment software tool was highly welcomed by these institutions.

CHAPTER FIVE: CONCLUSION & FUTURE WORK

5.1 Conclusion

The main aim of this research was to come up with a software tool that can be used by SME's in Kenya to conduct an information security risk assessment as outlined in the ISO/IEC 27005:2011. From testing of the software tool, respondents were happy with it and accepted it on the fact that it was user friendly, easy to learn and navigate through, it can be deployed centrally and or per individual working environment, it had clear elaborative reports, reduces time in conducting an IT security risk assessment and it was free.

From the literature review, we found that there were other similar standards, methodologies and frameworks, having different modes of implementation and jurisdiction of acceptance and use. Some were globally accepted like the Risk IT framework, the NIST and the ISO/IEC 27005:2011 standards, while others were specific to countries, such as the AS/NZS 4360:2004 for Australia and New Zealand, CRAMM that is specifically used by the British government and MAGERIT v3 2014, which was developed by the Spanish government to assist with management of information systems risks.

From the analyzed survey results, it was evident that even though the study population was aware of what an information security risk management was, they lacked proper in house skills and tools to do an information security risk assessments and gauge their respective institutions compliance to global risk standards. This was further confirmed by the fact that many of the respondents outsource their annual information security risk assessments from professional firms or individuals who have the necessary tools, skills and expertise to handle such tasks.

Tests were done with the developed tool and it was noted how easily and quickly the users used the application in assessing their risk levels in that the need for a manual was not necessary. Secondly, many of the testers attested that the risk assessment reports both for the individual asset and for the entire institution given the assets, was clear and concise on the different risk levels.

5.2 Limitations and Challenges

The study was limited to information security risk assessment and management in SMEs in Kenya with a focus on the ISO/IEC 27005:2011 standard. The study did not however look at security risk assessment and management of an institution in general which is also an important consideration in effective information security risk management. Another limitation was that, being an outsider, there were aspects of confidentiality and privacy that were looked at as far as sensitive risk information on the testing SMEs were concerned.

Challenges that were realized in the course of coming up with the prototype and subsequent testing were;

- i. It was very easy to deviate from the original requirements thereby increasing the complexity of the application.
- ii. Limited commitment by testers to test the prototype fully and give conclusive feedback that will enhance the application.

5.3 Future work

Further work is recommended in enhancing the tool to be comprehensive to cover all aspects of an institution as far as risk assessment and management is concerned without focusing on IT security risks alone. The enhanced application should also be accessible in all mobile platforms; Android, iOS and others that would be available at the time.

REFERENCES

1. Alberts, C.J., Behrens, S.G., Pethia, R.D. and Wilson, W.R., 1999. Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0.
2. ARBT, 2017. African Review of Business and Technology: SMEs are growing Kenya's economy. July 2017. Source: <http://www.africanreview.com/finance/business/smes-are-growing-kenya-s-economy-3>
3. Africa, F., 2017. Top Priorities for the Continent in 2017. Source: https://www.brookings.edu/wp-content/uploads/2017/01/global_20170109_foresight_africa.pdf
4. Al-Mayahi, I. and Sa'ad, P.M., 2012, January. ISO 27001 Gap Analysis-Case Study. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
5. AS/NZS, 2004. Australian/New Zealand Standard. Risk Management. Australia International and Standards New Zealand, as/nzs 4360:2004 edition, 2004.
6. Berg, H.P., 2010. Risk management: Procedures, Methods and Experiences. Electronic Journal Reliability: Theory & Applications. Vol. 1, pp.79-95.
7. Behnia, A., Rashid, R.A. and Chaudhry, J.A., 2012. A survey of information security risk analysis methods. SmartCR, 2(1), pp.79-94.
8. BSI, 2013. German BSI Standards 100-1, 100-2, 100-3, 100-4. Source: <https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html>
9. Burns, N., & Grove, S. K. (2009). The practice of nursing research : appraisal, synthesis, and generation of evidence. St. Louis, Mo: Saunders Elsevier.
10. CCTA, 2011. How CRAMM works. Central Computing and Telecommunications Agency (CCTA) of the United Kingdom.
11. CBK, 2016. The Central Bank of Kenya Annual Bank Supervision Report.
12. Coleman, G. & Verbruggen, R., 1998. A quality software process for rapid application development. Software Quality Journal, 7(2), pp.107-122.
13. Dawson, C. 2002. Practical Research Methods: A user friendly guide to mastering research. Oxford: How To Books Ltd.
14. Deloitte, 2016. Kenya Economic Outlook 2016: The Story Behind the Numbers. Source; <http://nic-bank.com/ke/platinum/wp-content/uploads/2016/01/KENYAS-ECONOMIC-OUTLOOK-REPORT-BY-DELOITTE.pdf>

15. DESPA, M.L., 2014. Comparative study on software development methodologies. Database Systems Journal, Vol. 5, Issue 3.
16. ENISA, 2006. Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs). European Network and Information Security Agency.
17. ENISA, 2013. European Network and Information Security Agency. Inventory of risk management / risk assessment methods. <http://rm-inv.enisa.europa.eu/methods>, February 2013.
18. Farrell, A., 2007. Selecting a Software Development Methodology based on Organizational Characteristics. An Essay Submitted in Partial Fulfillment of the Requirements for the Degree of “Master of Science in Information Systems”, Athabasca University, Athabasca.
19. Hubbard, D.W, 2009. The Failure of Risk Management: Why It’s Broken and How to Fix It. John Wiley & Sons.
20. Harpes, C., Schaff, G., Martins, M., Kordy, B., Trujillo, R. and Ionita, D., 2014. Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TressPass) project. Currently established risk-assessment methods, deliverable 5.2.1.
21. Haythorn, M. 2014. Running Head: Information Security Risk Assessment Methods, Frameworks and Guidelines.
Source:www.infosecwriters.com/Papers/MHaythorn_Risk_Frameworks_guidelines.pdf
22. Infohub, 2016. Source: <http://www.infohub.co.ke/2016/04/list-of-online-shopping-websites.html>
23. ISO, 2011. ISO/IEC 27005: 2011 (EN) Information technology--Security techniques--Information security risk management. Switzerland. ISO/IEC.
24. ISO, 2013. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. Switzerland. ISO/IEC.
25. Ionita, D., 2013. Current established risk assessment methodologies and tools. Source: <http://essay.utwente.nl/63830>.
26. ISACA, 2009. The Risk IT framework. Information Systems Audit and Control Association (ISACA). Source: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fm_k_Eng_0109.pdf
27. Jones, J., 2006. An introduction to factor analysis of information risk (FAIR). Norwich Journal of Information Assurance. Vol. 2 Issue 1, p.67.

28. Kelley, K., Clark, B., Brown, V. and Sitzia, J., 2003. Good practice in the conduct and reporting of survey research. *International Journal for Quality in health care*, Vol. 15, Issue 3, pp.261-266.
29. KNBS, 2017. *The Economic Survey: The Kenya National Bureau of Statistics*.
30. Kunder, R. and Clarke, N.L., 2013. Web-based Risk Analysis for SMEs. *Advances in Communications, Computing, Networks and Security*. Volume 10, p.120.
31. Knight, K.W., 2010. AS/NZS ISO 31000: 2009-The new standard for managing risk. *Keeping good companies*. Vol. 62, issue 2, p.68.
32. Lindsay, E. 2014. Gap analysis and risk assessment. source:
https://www.transfusionguidelines.org/document-library/documents/gap-analysis-and-risk-assessment-edwin-lindsay/download-file/rtc-ne_edu_pres_lindsay.pdf
33. MAGERIT, 2006. *Methodology for Information Systems Risk Analysis and Management. Book 1 - The Method*. Ministry of Public Administration, Portugal.
34. Mihailescu, V.L., 2012. Risk analysis and risk management using MEHARI. *Journal of Applied Business Information Systems*. Vol. 3. Issue 4, p.143.
35. Neuman, L. (2003). *Social Research Methods: qualitative and Quantitative Approaches*. America. Allyn and Baron Publishers.
36. NIST, 2011. National Institute of Standards and Technology. Special Publication 800-39: *Managing Information Security Risk*.
37. OECD, 2000. *A policy brief on Small and Medium-sized Enterprises: Local Strength, Global Reach*.
38. Potter, C., Miller, A. and Horne, R. 2015. *Information security breaches survey 2015*. Price Water House Coopers. Earl's Court, London. Source:
<https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf>
39. Parahoo, K. (2006). *Nursing research : principles, process, and issues*. Basingstoke, Hampshire, [England]; New York: Palgrave Macmillan.
40. Polit, D. F., Hungler, B. P., & Beck, C. T. (2001). *Essentials of nursing research : methods, appraisal and utilization*. Philadelphia: Lippincott.
41. Polit, D. F., & Beck, C. T. (2004). *Nursing research: Principles and methods*. Lippincott Williams & Wilkins.
42. Raptis, D., Dimitrakos, T., Gran, B.A. and Stølen, K., 2002. The CORAS approach for model-based risk management applied to e-commerce domain. In *Advanced Communications and Multimedia Security* (pp. 169-181). Springer, US.
43. Steve, E., 2006. *An Introduction to information systems risk management*. SANS Institute InfoSec Reading Room. Available on-line at

http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

44. Tawileh, A., Hilton, J. and McIntosh, S., 2007, September. Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In ISSE (pp. 331-339).

APPENDIX A: Project Schedule

Milestone	Deliverable	Duration (Wks)	Comments
M1	Project Proposal preparation	4	Done
M1 Evaluation	Proposal Presentation	2	Done
M2	Project Implementation (Write up and demo)	12	Done
M2 Evaluation	M2 presentation	2	Done
M3	Conclusion of project. Prepare project report.	4	Done
M3 Evaluation	M3 Presentation	2	Done

APPENDIX B: Letter of Introduction

ANDREW E. OKOTH
P.O.BOX 3464-00100
NAIROBI, KENYA.
Email: andreokoth@gmail.com
Tel: +254720819990

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

REF: RESEARCH SURVEY QUESTIONNAIRE

My name is Andrew Eliezor Okoth, a student pursuing Master of Science in Distributed Computing Technology in the School of Computing and Informatics at the University of Nairobi under the registration number P53/73070/2014. I am undertaking a research study entitled "AN INFORMATION SECURITY RISK MANAGEMENT GAP ANALYSIS TOOL BASED ON ISO/IEC 27005:2011 COMPLIANCE FOR SMES IN KENYA ". I would be grateful if you would volunteer to assist in this project by completing a questionnaire accessible via the link below.

The research study is designed to come up with an efficient Information Security Risk Assessment gap analysis software tool that can give an overview of an organization's status as regards the ISO/IEC 27005:2011 standard. The latter is the global standard in Information Security Risk Management. Participation in the study involves completion of a questionnaire which consists of 3 major sections and which may require approximately 20 minutes to complete.

The survey questionnaire targets personnel in the I.T Department or any person who is in charge of ICT matters within the institution. You are not required to put your name or the name of your institution/organization. If you do so, you or your institution/organization will not be identified by the name within the project. If you have any concerns regarding the questions or use of the questionnaire within the research project, please do not hesitate to contact me at andreokoth@gmail.com.

Kindly answer the questions as comprehensively as possible and to the best of your knowledge. You may also consult with colleagues about answers to particular questions, or if another person in your institution is better positioned to answer this survey, kindly forward this e-mail to that person.

Kindly complete the survey by March 2nd, 2018. I will appreciate your time and effort.

Yours Sincerely,
Andrew E. Okoth

APPENDIX C: Survey Questionnaire

INFORMATION SECURITY RISK MANAGEMENT SURVEY QUESTIONNAIRE

This survey questionnaire is meant to capture information on an organization's or institution's awareness of Information Security Risk Management and the necessity of having a supporting tool.

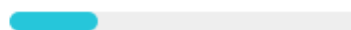
The questionnaire has 3 major sections;

General Information Section which captures general information of the respondent and the institution/organization.

Information Security Risk Assessment and Management section which captures the respondents awareness and knowledge of the latter, and the respondent's organization/institution's awareness of the same.

Information Security Risk Assessment software tool section which captures the respondents knowledge, use and necessity of the latter.

NEXT



Page 1 of 4

Never submit passwords through Google Forms.

*Required

General Information

This section is set to capture the general static details of the respondent and the organization/institution. Some of the details are optional but you are encouraged to fill them unless otherwise.

1. Your name (optional)

Your answer

2. What is your role/title within your organization/institution *

Your answer

3. Your institution/organization name

Your answer

4. Which category does your institution/organization fall in *

- Micro-finance Institution
- eCommerce Institution
- Online Payments Facilitator
- Mobile Money Payments Facilitator
- Other

If OTHER, kindly specify

Your answer _____

5. How old is your institution/organization *

Choose 

6. Has your organization/institution been involved in an Information Security Incident in the last two years? *

- Yes
- No
- Don't Know

7. If YES, did the cause originate internally or externally?

- Internally
- Externally

BACK

NEXT

 Page 2 of 4

*Required

Information Security Risk Assessment and Management

This section captures the respondents awareness and knowledge of Information Security Risk Assessment and Management, and the respondent's organization/institution's awareness of the same.

1. Do you know what Information Security Risk Management is?

*

Yes

No

If YES, briefly explain

Your answer

2. Have you been trained on Information Security Risk Assessment and Management? *

Yes

No

3. If YES, was the training based on an Information Security Risk Management Standard or a Framework or a Methodology? *

- Standard
- Framework
- Methodology
- None
- Not Sure

4. Which Standard or Framework or Methodology was the training based on?

Your answer

5. How often is the training done? *

- Monthly
- Quaterly
- Semi-Annually
- Annually
- Once
- Never

6. What necessitated the training?

- Audit Requirement
- Response to an Information Security Incident
- Yearly Planned Activity
- Other

If OTHER kindly specify

Your answer

7. Does your institution/organization have an Information Security Risk Management plan? *

- Yes
- No
- Don't Know

8. How often is Information Security Risk Assessment conducted within your institution/organization? *

- Monthly
- Quaterly
- semi-Annually
- Annually
- Once
- Never
- Don't Know

9. What necessitated the Information Security Risk Assessment within your institution/organization?

- Audit Requirement
- Response to an Information Security Incident
- Yearly Planned Activity
- For Cost Justification
- Other

If OTHER kindly specify

Your answer

10. Is the Information Security Risk Assessment service outsourced or there is use of internal capacity?

- Outsourced
- Use of internal capacity

11. Are you aware of any global Standard or Framework or Methodology used in Information Security Risk Assessment and Management? *

- YES for Standard
- YES for Framework
- YES for Methodology
- Not aware of any

12. If YES to any of the above, which global Standard or Framework or Methodology are you aware of?


Your answer

13. Of the Standard or Methodology or Framework you have stated above, which one does your institution/organization follow or use?

Your answer

BACK

NEXT

 Page 3 of 4

*Required

Information Security Risk Assessment software tool

This section captures the respondents knowledge, use and necessity of an Information Security Risk Assessment software tool within his/her organization/institution.

1. Are you familiar with any Information Security Risk Assessment Software Tool? *

Yes

No

2. If YES, was the software tool purchased or acquired for free (open source) or developed inhouse?

Purchased

Free

Developed Inhouse

3. If 1 above is YES, can you name the software tool and its vendor or source?

Your answer _____

4. Is the software tool based on any global Standard, Framework or Methodology in Information Security Risk Assessment and Management?

- Yes
- No
- Don't Know

5. If 4 above is YES, which global Standard or Framework or Methodology is this?

Your answer

6. Do you think a software tool for Information Security Risk Assessment and Management is necessary for your institution/organization? *

- Yes
- No
- Maybe

7. Kindly elaborate on your choice of answer in 6 above *

Your answer

8. For such a software tool, what kind of features do you think it should have? *

Your answer

BACK

SUBMIT

 Page 4 of 4

APPENDIX D: Why your institution needs a software tool

7. Kindly elaborate on your choice of answer in 6 above

emerging security issues are key to be addressed proactively

Helps asses and apply control measures to mitigate against risks

It will help us in assessing the level of IT risk that our institution is exposed to.

My institution is open to the internet 99% of the time hence opened to cyber attacks, so such a tool will greatly help in assessing these risks.

it will help with internal risks assessments and thus management of the same in terms of controls to put in.

HELP IN ASSESSMENT AND MANAGEMENT OF RISKS

cyber security is a growing concern and a tool to help us in managing threats will be welcomed.

it will help with identification of risks and management of the same.

very necessary to help with risk assessment.

It will help in risks and threat assessments.

for risk assessment.

such a tool will help us in identifying and managing IT risk.

it will assist with risk assessment and vulnerability assessment along with the mitigation procedures.

Assist in risk identification, analysis and management.

if it is free, the my employer would not need to outsource this service.

it will be good for risk assessment

it will make information security management easier fro companies.

it will provie an effective way of assessing, identifying and managing risks to information systems.

it will help with risk assessment

cost reduction in outsourcing.

to identify risk;threats, vulnerabilities to information systems

assist with risk identification and may be management.

ours being a finance institution, such a solution is welcomed.

very necessary for risk management

it will make risk assessment easier in that it can be done anytime

A tool of this kind will greatly help in the management of threats and risks to information systems.

most tools are commercial based, a free one that do the same job is very much welcomed

any tool that will assist in this endeavour is highly welcomed.

With such a tool outsourcing will of the service will be stopped.

It will be easier for institutions like ours to do risk assessments anytime and without cost implication.

It will help in managing of risks

I dont think it is necessary, but if I am informed and educated on the need/purpose, then maybe it may be needed.

This would ensure tracking is done adequtely

APPENDIX E: Probable features

8. For such a software tool, what kind of features do you think it should have?

IT security detection and prevention

Assessment, control, dashboards.

Not sure but i think capability to assess IT risk, ability to list IT risks, ability to provide recommendation on the identified risks.

identify risks, identify threats, identify controls, come up with reports, should be easy to use, should be light on the systems.

it should be able to identify threats and controls.

easy to use, efficient, gives correct results.

be able to report on the risk exposure level of an institution.

easy to use, able to identify it risks.

should be able to identify risks.

identify threats and risks to information systems.

risk, threat identification, risk knowledge management

robust enough to identify the risks

easy to use, able to identify risks, threats and advice on mitigation procedures

it should be able to identify threats and any related risks.

should be free, user friendly, robust.

can identify threats and risks

it should be able to identify risks and put in a controlling procedure.

it should be free and easy to use.

risk identification, categorization.

should be able to identify risk

be able to identify threats and vulnerabilities.

risk identification and control advice should be one of the major feature.

A solution to provide risk assessment for all IT systems

easy to use, has informative reports.

it must be easy to use, it should be able to identify risks and advice accordingly via a report.

threat identification, risk categorization, risk monitoring, risk assessment.

risk identification, threat analysis, reporting

easy to use

Easy to use and give out clear reports

Should be easy to use, accurate, abke to identfy risks, threats etc

Workable

Categories of all the risk areas to be checked and a summary of the compliance levels

Audit of systems.

APPENDIX F: Application installation requirements

The end product of this project was an application prototype that could be hosted on the web and also locally. The application was implemented both locally and on a web. The following minimum installation prerequisites are required.

For the web;

- Processor - Intel x86 Architecture 3GHz processor or equivalent
- RAM - 2 GB RAM
- Hard Disk - 100GB and above
- Must be on for 24 hours every day.

For the localhost on a user machine;

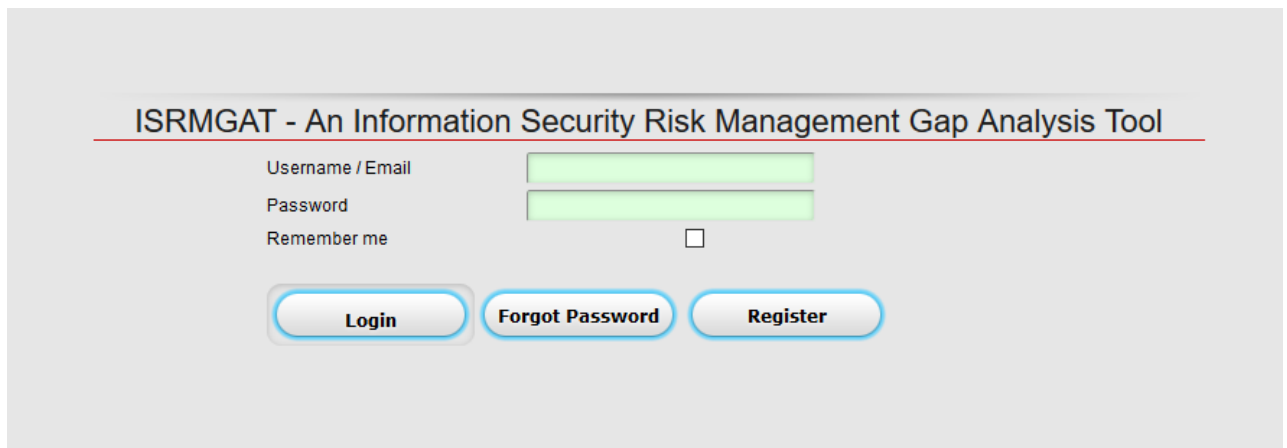
- Processor - Intel x86 Architecture 3GHz processor or equivalent
- GB RAM
- 40 GB hard disk space.
- CD-ROM drive or a floppy drive.
- VGA or higher resolution monitor.
- Mouse or other pointing device.

Software requirements;

- Operating System - Windows 7/8/10, Windows Server 2008/2012, Linux distributions such as Ubuntu, Fedora, Redhat.
- Apache Version - Apache 2.2
- MySQL Version - 5.7 and above
- PHP Version 7 and above.
- Browser - Internet Explorer 8/Edge, Firefox, Google Chrome, Safari
- Web Server Packages - XAMPP, WAMPP, LAMPP

APPENDIX G: Application screen shots

Login page



ISRMGAT - An Information Security Risk Management Gap Analysis Tool

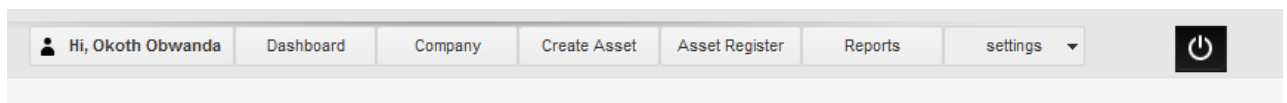
Username / Email


Password

Remember me

[Login](#) [Forgot Password](#) [Register](#)

Menus



Hi, Okoth Obwanda | Dashboard | Company | Create Asset | Asset Register | Reports | settings ▾ | 

Account Setting and password change page

My Account - Settings

Here you can make changes to your profile. Please note that you will not be able to change your email which has been already registered.

Your Name / Company Name

Okoth Obwanda

Your name or company name

Address (full address with ZIP)

7645-00200, Nairobi, Kenya.

Country

Kenya

Phone

67676676

Fax

232323

Website

http://www.atupiconsult

Example: http://www.domain.com

User Name

andrew

Email

andreokoth@gmail.com

Save

Change Password

If you want to change your password, please input your old and new password to make changes.

Old Password

New Password

Update

Dashboard

Dashboard [+]

Summary

Total Companies	4	Total Assets	8
-----------------	---	--------------	---

Company Ratings

Company	Assets	Risk Score
Uwezo Microfinance Bank	5	HIGH : 16
Caritas Microfinance Bank	3	HIGH : 20

Company Information page

Company Information

Company Name	<input type="text"/>	Address (123-00300)	<input type="text"/>
Phone No (format: 254xxxxxxxx)	<input type="text" value="254"/>	Email	<input type="text"/>
Mobile No (format: 254xxxxxxxx)	<input type="text" value="254"/>	Fax No	<input type="text"/>
Website (http://)	<input type="text"/>	Business Entity	--Select--
Registration No	<input type="text"/>	Pin No	<input type="text"/>

Contact Person information

Contact Person	<input type="text"/>	Contact Person Phone No	<input type="text" value="254"/>
Contact Person Email	<input type="text"/>	Logo	<input type="button" value="Browse..."/> No file selected.

Company Information

Serial No	Company Name	Address	Phone	Email	Contact Phone No	Preview	
<input type="checkbox"/>							
<input type="checkbox"/>	IS100001	Uwezo Microfinance Bank	P.O BOX 1654-00100, Nai	254703591302	info@uwezombank.com	254703591302	Preview
<input type="checkbox"/>	IS100002	Rafiki Microfinance Bank	P.O. Box 12755-00400 Nairobi, Kenya.	254711073000	info@rafikimfb.co.ke	254711073000	Preview
<input type="checkbox"/>	IS100003	Daraja Microfinance Bank	P. O. Box 100854 – 00101	254707444888	info@darajabank.co.ke	254718444888	Preview
<input type="checkbox"/>	IS100004	Caritas Microfinance Bank	P. O Box 15352 – 00100.	254515150000	info@caritas-mfb.co.ke	254729986331	Preview

Asset creation page

Create Asset

Company	<input type="text" value="Uwezo Microfinance Bank"/>	Asset Name	<input type="text"/>
Purchase Date	<input type="text"/>	Location	<input type="text"/>
Date of Birth	<input type="text"/>	Decommission Date	<input type="text"/>

Description

Asset register page

Asset Register											
<input type="checkbox"/>	Company	Asset ID	Asset Name	Remarks	Asset Location	Purchase/Emp D	ROY	Preview	Threats	Controls	Report
<input type="checkbox"/>	Uwezo Microfina	AS1	Windows 2012 E	Used for emailing	Server Room	2015-08-17	4	Preview	Threats	Controls	Report
<input type="checkbox"/>	Caritas Microfina	AS2	VOIP desk phone	Used by employee	On user desks	2011-06-06	3	Preview	Threats	Controls	Report
<input type="checkbox"/>	Uwezo Microfina	AS3	Staff smart phone	Mobile devices u	mobile with users	2015-12-18	7	Preview	Threats	Controls	Report
<input type="checkbox"/>	Uwezo Microfina	AS4	IS Manager Pc	Normal user PC	IS Manager Office	2015-02-05	2	Preview	Threats	Controls	Report
<input type="checkbox"/>	Uwezo Microfina	AS5	Loan officer Lap	PC used by the	Banking hall	2016-05-09	3	Preview	Threats	Controls	Report
<input type="checkbox"/>	Uwezo Microfina	AS6	T24 Banking app	Core business ap	Server room	2010-06-20	2	Preview	Threats	Controls	Report
<input type="checkbox"/>	Caritas Microfina	AS7	Company data	Company data in	Various	2005-04-06	7981	Preview	Threats	Controls	Report
<input type="checkbox"/>	Caritas Microfina	AS8	Head of ICT	Has been in IT s	ICT	2010-01-04	17	Preview	Threats	Controls	Report

Asset Threat page

Asset Name :: Windows 2012 Exchange Server (AS1)

Purchase Date	2015-08-17	Location	Server Room
Manufactured Date	2013-01-01	Decommission Date	2022-08-17
		Remaining Operational Years	4

Remarks

Used for emailing, calendaring, contacts, scheduling and collaboration of meetings. Serves 45 employees.

Threats

KEY

Threat Likelihood	Threat Impact
Very likely (VL) = 5	Severe (SV) = 5
Likely (L) = 4	Significant (SG) = 4
Possible (P) = 3	Moderate (MD) = 3
Unlikely (U) = 2	Minor (MN) = 2
Very unlikely (VU) = 1	Negligible (N) = 1

Threat Title

Threat Likelihood

Threat Impact

Remarks

Threat Register

<input type="checkbox"/>	Asset ID	Threat Name	Remarks	Likelihood	Impact
<input type="checkbox"/>	AS1	Malware attacks	Malware attacks can cause denial of service attacks, a very critical	4	4
<input type="checkbox"/>	AS1	Hardware failures	Failure can be due to old age of the server, inappropriate environm	3	4
<input type="checkbox"/>	AS1	Destruction	Destruction by an aggrieved employee.	3	4
<input type="checkbox"/>	AS1	Unauthorised access	unauthorized users gaining access for purposes of snooping for inte	3	3
<input type="checkbox"/>	AS1	Fire	fire in the data center that burn the server and destroy the storage	3	4

Current Control page

Asset Name :: Windows 2012 Exchange Server (AS1)

Asset ID	AS1	Location	Server Room
Purchase Date	2015-08-17	Decommission Date	2022-08-17
Manufactured Date	2013-01-01	Remaining Operational Years	4

Remarks

Used for emailing, calendaring, contacts, scheduling and collaboration of meetings. Serves 45 employees.

Threats

THREAT	REMARKS	LIKELIHOOD	IMPACT	RISK LEVEL
Malware attacks	Malware attacks can cause denial of service attacks. a very critical situation when the server is unavailable.	4	4	HIGH =16
Hardware failures	Failure can be due to old age of the server, inappropriate environment.	3	4	MEDIUM =12
Destruction	Destruction by an aggrieved employee.	3	4	MEDIUM =12
Unauthorised access	unauthorized users gaining access for purposes of snooping for internal users and to get email addresses for phishing.	3	3	MEDIUM =9
Fire	fire in the data center that burn the server and destroy the storage media.	3	4	MEDIUM =12
Overall Risk Rating for Windows 2012 Exchange Server				HIGH [16]

Controls

Threat Name

Control Name

Control Level

○ 1 ○ 2 ○ 3 ○ 4 ○ 5
 <-- Weak Medium Strong -->

Remarks

Submit

Reset

Asset Controls

Asset ID	Threat Name	Control	Control Remarks	Control level
AS1	Malware attacks	Firewall	test control	3
AS1	Hardware failures	daily data backup	daily back up of data in-case hardware failure results to l	4
AS1	Destruction	Secure lock and entry to the server room	Server room is protect by a lock which allows access to al	4

Sample Report for Risk Assessment of an asset

WINDOWS 2012 EXCHANGE SERVER RISK ASSESSMENT REPORT

Asset ID	AS1	Location	Server Room
Purchase Date	2015-08-17	Decommission Date	2022-08-17
Manufactured Date	2013-01-01	Remaining Operational Years	4

Remarks

Used for emailing, calendaring, contacts, scheduling and collaboration of meetings. Serves 45 employees.

Threats to Windows 2012 Exchange Server

THREAT	REMARKS	LIKELIHOOD	IMPACT	EXISTING CONTROLS	CONTROL LEVEL	RISK LEVEL
Malware attacks	Malware attacks can cause denial of service attacks. a very critical situation when the server is unavailable.	4	4	Firewall	Medium : 3	HIGH =16
Hardware failures	Failure can be due to old age of the server, inappropriate environment.	3	4	daily data backup	Strong : 4	MEDIUM =12
Destruction	Destruction by an aggrieved employee.	3	4	Secure lock and entry to the server room	Strong : 4	MEDIUM =12
Unauthorised access	unauthorized users gaining access for purposes of snooping for internal users and to get email addresses for phishing.	3	3	One person with admin rights	Medium : 3	MEDIUM =9
Fire	fire in the data center that burn the server and destroy the storage media.	3	4	Fire depressants	Strong : 4	MEDIUM =12
Overall Risk and Control rating for Windows 2012 Exchange Server as at 12, July 2018 .						HIGH [16]

Sample Risk Assessment report for an institution given the assets

RISK ASSESSMENT REPORT

Uwezo Microfinance Bank
P.O BOX 1654-00100, Nairobi – Kenya.
Office No: 254703591302
Email: info@uwezombank.com
Website: http://uwezombank.com
Date: 12, July 2018

Asset List				
Asset No#	Asset Name	Remarks	ROY	Risk Score
AS1	Windows 2012 Exchange Server	Used for emailing, calendaring, contacts, scheduling and collaboration of meetings. Serves 45 employees.	4	HIGH : 16
AS3	Staff smart phones and Ipads	Mobile devices used by sales personnel, for making calls to clients, checking work emails and also doing other personal things.	7	MEDIUM : 12
AS4	IS Manager Pc	Normal user PC with nothing much, just links to information security tools.	2	MEDIUM : 9
AS5	Loan officer Laptop	PC used by the loans officer at the banking hall. Has some sensitive company and customer information.	3	MEDIUM : 9
AS6	T24 Banking application	Core business application. hosted within a linux server in the server room.	2	HIGH : 16
Overall risk rating given the assets and controls in place for Uwezo Microfinance Bank as at 12, July 2018				HIGH [16]

User creation page

Create New User

Company ▼

User ID (Type the username)

Email

User Level ▼

Password (if empty a password will be auto generated)

Send Email

**All created users will be approved by default.

APPENDIX H: Sample code

Asset_controls

```
<?php

include 'dbc2.php';
/*page_protect();
$conn = mysql_connect("localhost", "root", "");
mysql_select_db("cbo");*/
$id = filter_input(INPUT_GET, 'id', FILTER_SANITIZE_STRING);
// set your db encoding -- for ascent chars (if required)
mysql_query("SET NAMES 'utf8'");
include("inc/jqgrid_dist.php");
// you can customize your own columns ...
$col = array();
$col["title"] = "No"; // caption of column
$col["name"] = "id"; // grid column name, must be exactly same as returned column-name from sql (tablefield or field-alias)
$col["width"] = "5";
$col["editable"] = false;
$col["hidden"] = true;
$col["search"] = false;
$col["align"] = "right";
$cols[] = $col;
$col = array();
$col["title"] = "Asset ID";
$col["name"] = "docno";
$col["width"] = "5";
$col["editable"] = false;
$col["hidden"] = false;
$col["align"] = "left"; // this column is not editable
$col["search"] = false; // this column is not searchable
$col["editrules"] = array("required"=>true, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Threat Name";
$col["name"] = "asset_threat_title";
$col["width"] = "15";
$col["editable"] = false;
$col["hidden"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
#$col["align"] = "center"; // this column is not editable
$col["search"] = true;

$cols[] = $col;
$col = array();
$col["title"] = "Control";
$col["name"] = "asset_control_title";
$col["width"] = "15";
$col["editable"] = true;
$col["hidden"] = false;
$col["search"] = true;
$col["editrules"] = array("edithidden"=>true);
$col["edittype"] = "textarea"; // render as textarea on edit
$col["editoptions"] = array("rows"=>4, "cols"=>20); // with these
$cols[] = $col;
$col = array();
$col["title"] = "Control Remarks";
$col["name"] = "controls_description";
$col["width"] = "20";
$col["editable"] = true;
$col["hidden"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
#$col["align"] = "center"; // this column is not editable
$col["search"] = false;
$col["edittype"] = "textarea"; // render as textarea on edit
$col["editoptions"] = array("rows"=>4, "cols"=>20); // with these attributes
$cols[] = $col;
$col = array();
$col["title"] = "Control level";
$col["name"] = "controls_level";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$col["align"] = "center"; // this column is not editable
$col["search"] = false;
```

```

$col["editttype"] = "select"; // render as select
$col["editoptions"] = array("value"=>'5:Strong (5);4:Strong (4);3:Medium (3);2:Weak (2);1:Weak (1)');
$cols[] = $col;
$grid["grouping"] = false; //
$grid["groupingView"] = array();
$grid["groupingView"]["groupField"] = array("pname"); // specify column name to group listing
$grid["groupingView"]["groupColumnShow"] = array(false); // either show grouped column in list or not (default: true)
$grid["groupingView"]["groupText"] = array("<b>{0} - {1} Item(s)</b>"); // {0} is grouped value, {1} is count in group
$grid["groupingView"]["groupOrder"] = array("asc"); // show group in asc or desc order
$grid["groupingView"]["groupDataSorted"] = array(true); // show sorted data within group
$grid["groupingView"]["groupSummary"] = array(true); // work with summaryType, summaryTpl, see column: $col["name"] = "total";
$grid["groupingView"]["groupCollapse"] = false; // Turn true to show group collapse (default: false)
$grid["groupingView"]["showSummaryOnHide"] = true; // show summary row even if group collapsed (hide)
$g = new jqgrid();
// $grid["url"] = ""; // your paramterized URL -- defaults to REQUEST_URI
$grid["rowNum"] = 20; // by default 20
$grid["sortname"] = 'id'; // by default sort grid by this field
$grid["sortorder"] = "ASC"; // ASC or DESC
$grid["caption"] = "Asset Controls"; // caption of grid
$grid["autowidth"] = true; // expand grid to screen width
$grid["multiselect"] = true; // allow you to multi-select through checkboxes
$g->set_options($grid);
$g->set_actions(array(
    "add"=>false, // allow/disallow add
    "edit"=>true, // allow/disallow edit
    "delete"=>true, // allow/disallow delete
    "rowactions"=>false, // show/hide row wise edit/del/save option
    "edithidden"=>false,
    "search" => "advance" // show single/multi field search condition (e.g. simple or
    advance)
));

// you can provide custom SQL query to display data
$g->select_command = ("SELECT * FROM a_assets_threats where docno = '$id' AND asset_control_title IS NOT NULL AND controls_level IS NOT NULL");
// this db table will be used for add,edit,delete
$g->table = "a_assets_threats";
// pass the cooked columns to grid
$g->set_columns($cols);
// generate grid output, with unique grid name as 'list1'
$out = $g->render("list1");
$themes = array("redmond", "smoothness", "start", "dot-luv", "excite-bike", "flick", "ui-darkness", "ui-lightness", "cupertino", "dark-hive");
$i = rand(0,8);
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
<head>
<script src="http://code.jquery.com/jquery-latest.js" type="text/javascript"></script>
<link rel="stylesheet" href="//code.jquery.com/ui/1.11.4/themes/smoothness/jquery-ui.css">
<script src="//code.jquery.com/jquery-1.10.2.js"></script>
<script src="//code.jquery.com/ui/1.11.4/jquery-ui.js"></script>
<script src="vallenato/jquery-latest.js" type="text/javascript"></script>
<script src="vallenato/vallenato.js" type="text/javascript"></script>

<link rel="stylesheet" href="vallenato/vallenato.css" type="text/css" media="screen">
<link rel="stylesheet" type="text/css" media="screen" href="js/themes/<?php echo $themes[9]?>/jquery-ui.custom.css"></link>
<link rel="stylesheet" type="text/css" media="screen" href="js/jqgrid/css/ui.jqgrid.css"></link>

<script src="js/jquery.min.js" type="text/javascript"></script>
<script src="js/jqgrid/js/i18n/grid.locale-en.js" type="text/javascript"></script>
<script src="js/jqgrid/js/jquery.jqGrid.min.js" type="text/javascript"></script>
<script src="js/themes/jquery-ui.custom.min.js" type="text/javascript"></script>
<link href="styles.css" rel="stylesheet" type="text/css" />
<link href="class/gh-buttons.css" rel="stylesheet" type="text/css" />
<script>
$(function() {
    $("#dor_date").datepicker();
    $("#s_date").datepicker();
    $("#e_date").datepicker();
    $("#sb_date").datepicker();
    $("#handovedate").datepicker();
    $("#e_last_inspection").datepicker();
});
</script>
</head>
<body>
<div class="form" >

```

```

<?php
/*$assets = "SELECT * FROM a_assets where docno ='$id' group by id ";
$result = mysql_query($assets);
$data = mysql_fetch_assoc($result);
$docno = $data['docno'];
$asset_name = $data['asset_name'];
$asset_location_0 = $data['asset_location_0'];
$asset_location = $data['asset_location'];
$asset_purchase_date_0 = $data['asset_purchase_date_0'];
$asset_purchase_date = $data['asset_purchase_date'];
$asset_decommissioning_date_0 = $data['asset_decommissioning_date_0'];
$asset_decommissioning_date = $data['asset_decommissioning_date'];
$description = $data['description'];
$notes = $data['notes'];
$createdby = $data['createdby'];
$date = $data['date'];*/
$assets = "SELECT * FROM a_assets_view where docno ='$id'";
$result = mysql_query($assets);
$data = mysql_fetch_assoc($result);
$docno = $data['docno'];
$asset_name = $data['asset_name'];
$asset_location_0 = $data['asset_location_0'];
$asset_location = $data['asset_location'];
$asset_purchase_date_0 = $data['asset_purchase_date_0'];
$asset_purchase_date = $data['asset_purchase_date'];
$asset_decommissioning_date_0 = $data['asset_decommissioning_date_0'];
$asset_decommissioning_date = $data['asset_decommissioning_date'];
$asset_dob_0 = $data['asset_dob_0'];
$asset_dob = $data['asset_dob'];
$description = $data['description'];
$notes = $data['notes'];
$createdby = $data['createdby'];
$date = $data['date'];
$remaining_years = $data['remaining_years'];
$Remaining_Operational_Years = $data['Remaining_Operational_Years'];
$query=mysql_query("select MAX(id)from a_callins");
$result =mysql_fetch_array($query);
$cur_auto_id0= $result['MAX(id)']+1;
$cur_auto_id='AC'.str_pad($cur_auto_id0,1,'0',STR_PAD_LEFT);
$query=mysql_query("select MAX(risk_score)from threat_analysis_result where docno ='$id'");
$result =mysql_fetch_array($query);
$risk_score= $result['MAX(risk_score)'];
if($risk_score >=1 && $risk_score <=6 ){
    $txtbox = "<td style=background-color: #00FF00;>LOW [ ".$risk_score." ]</td>";
}elseif($risk_score >=7 && $risk_score <=12 ){
    $txtbox = "<td style=background-color: #FFFF00;>MEDIUM [ ".$risk_score." ]</td>";
}elseif($risk_score >=13 && $risk_score <=25 ){
    $txtbox = "<td style=background-color: #FF0000;>HIGH [ ".$risk_score." ]</td>";
}
}
//This function separates the extension from the rest of the file name and returns it
function findexts ($filename)
{
    $filename = strtolower($filename) ;
    $exts = split("[\\\.]", $filename) ;
    $n = count($exts)-1;
    $exts = $exts[$n];
    return $exts;
}
//This applies the function to our file
$ext = findexts ($_FILES['photo']['name']) ;
//This line assigns a random number to a variable. You could also use a timestamp here if you prefer.
$ran = rand () ;
//This takes the random number (or timestamp) you generated and adds a . on the end, so it is ready of the file extension to be appended.
$ran2 = $ran.".";
//This is the directory where images will be saved
$target = "dcim/";
$target = $target . $ran2.$ext;
//$target = $target . basename( $_FILES['photo']['name']);
$message="";
$message2="";
$sac="";
if (isset($_POST['submit'])){
    $sql="UPDATE a_assets_threats
SET
asset_threat_title2='".$_POST['assets_threat_title'].'",
asset_control_title='".$_POST['assets_control_title'].'",
controls_level='".$_POST['controls_levels'].'",
controls_description='".$_POST['controls_descriptions'].'",

```



```

createdby2="$_SESSION['user_name'].",
date2="date("Y-m-d H:i:s")."
WHERE id="$_POST['assets_threat_title']."";
/*INSERT INTO a_assets_controls (docno,asset_threat_title2,asset_control_title, control_level, control_description, createdby2,date2) VALUES
("$_POST['asset_threat_title']
,$_POST['asset_control_title']
,$_POST['controls_level']
,$_POST['controls_description']
,$_SESSION['user_name']
,date("y-m-d H:i:s").");
//,$_md5(date("d:m:Y H:i:s"))*/
if (mysql_query($sql) or die(mysql_error())){
//move_uploaded_file($_FILES['photo']['tmp_name'], $target)
//echo $sql;
echo $messages="Saved successfully";
}else{
echo $messages="Error: ".mysql_error();
}
?>
<form enctype="multipart/form-data" action="" method="POST" onSubmit="if(!confirm('Are You Sure?')){return false;}">
<table width="100%" align="center" border="0" class="form" id="accordion-container">
<tr>
<td colspan="4"><div><strong><a href="a_asset_list.php" target="myacc" class="button icon arrowleft"> Back </a></strong></div><br /></td>
</tr>
<tr class="headingTOP">
<td colspan="4">Asset Name :: <strong><?php echo $asset_name; ?></strong> (<strong><?php echo $docno; ?></strong></td>
</tr>
<tr>
<td width="29%"><strong>Asset ID</strong></td>
<td width="22%"><?php echo $docno; ?></td>
<td width="24%"><strong><?php echo $asset_location_0; ?></strong></td>
<td width="25%"><?php echo $asset_location; ?></td>
</tr>
<tr>
<td><strong><?php echo $asset_purchase_date_0; ?></strong></td>
<td><?php echo $asset_purchase_date; ?></td>
<td><strong><?php echo $asset_decommissioning_date_0; ?></strong></td>
<td><?php echo $asset_decommissioning_date; ?></td>
</tr>
<tr>
<td><strong><?php echo $asset_dob_0; ?></strong></td>
<td><?php echo $asset_dob; ?></td>
<td><strong>Remaining Operational Years</strong></td>
<td><?php echo $remaining_years; ?></td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td><p><br />
</p></td>
</tr>
<tr>
<td colspan="4"><?php echo $description; ?></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr class="headingTOP">
<td colspan="4">Threats</td>
</tr>
<tr>
<td colspan="4"><?php
// Retrieve all the data from the "example" table where client_id ='$id'
$query = "SELECT * from threat_analysis_result where docno = '$id'";
// store the record of the "example" table into $row
$result = mysql_query($query) or die(mysql_error());
// Print out the contents of the entry in a table
echo "<table align='center' border='0' cellspacing='3' class='inventory' width='100%'>";
//echo "<tr><td colspan='4' ><img src='assets/images/Logo_Half.png' width='auto' height='auto' /> </td> </tr>";
echo "<thead class='heading2'><tr><th width='15%'>THREAT</th> <th width='35%'>REMARKS</th><th width='8%'>LIKELIHOOD</th><th width='8%'>IMPACT</th><th width='6%'>RISK LEVEL</th></thead>";
// keeps getting the next row until there are no more to get

```

```

$i=0;
while($row = mysql_fetch_array($result)){
    $i++;
    //get alternating color for rows
    if ($i%2){
        $bg="#E6F2FF";
    }else{
        $bg="#FFFFFF";
    }
    //end alternating
    // Print out the contents of the entry in a table
    //echo number_format("1000000",2);
    echo "<tr><td bgcolor= $bg>";
    echo $row['asset_threat_title'];
    echo "</td><td bgcolor= $bg align = 'left'>";
    echo $row['threat_description'];
    echo "</td><td bgcolor= $bg align = 'center'>";
    echo $row['asset_threat_likelyhood'];
    echo "</td><td bgcolor= $bg align = 'center'>";
    echo $row['asset_impact'];
    //echo "</td><td bgcolor= $bg align = 'center'>";
    //echo $row['state'];
    //(strpos($row['state'], $row['state']) === 'HIGH')
    if($row['states']=='LOW') // [val1] can be 'approved'
        echo "</td><td style='background-color: #00FF00;' align = 'center'>".$row['state']."</td>";
    else if($row['states'] == 'HIGH') // [val2] can be 'rejected'
        echo "</td><td style='background-color: #FF0000;' align = 'center'>".$row['state']."</td>";
    else if($row['states']=='MEDIUM') // [val3] can be 'on hold'
        echo "</td><td style='background-color: #FFFF00;' align = 'center'>".$row['state']."</td>";
    else if($row['states']=='NO RESULT') // [val3] can be 'on hold'
        echo "</td><td style='background-color: $bg;' align = 'center'>".$row['state']."</td>";
        echo "</td></tr>";
        echo "<tr bgcolor='#fff'><td colspan='4' align = 'center'><strong>Overall Risk Rating for $asset_name "; $row['result'];
        echo $tbody;
        echo "</td></tr>";
        echo "</table>";
?></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr class="headingTOP">
<td colspan="4">Controls</td>
</tr>
<tr>
<td><strong>Threat Name</strong></td>
<td><?php $sql1 = ("SELECT distinct asset_threat_title,id FROM a_assets_threats where docno = '$id'");
$result1 = mysql_query($sql1);
echo "<select name='assets_threat_title' >";
while ($row = mysql_fetch_array($result1) {
    echo "<option value="" . $row['id'] . ""> . $row['asset_threat_title'] . "</option>";
}
echo "</select>";
?></td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr>
<td width="29%"><strong>Control Name</strong></td>
<td width="22%"><input name="assets_control_title" type="text" required="required" id="assets_control_title" value="" /></td>
<td width="24%"><strong>Control Level</strong></td>
<td width="25%"><table width="200">
<tr>
<td><label>
<input name="controls_levels" type="radio" required="required" id="controls_levels_0" value="1" />
1</label></td>
<td><input type="radio" name="controls_levels" value="2" id="controls_levels_1" />
2</label></td>
<td><input type="radio" name="controls_levels" value="3" id="controls_levels_2" />
3</label></td>
<td><input type="radio" name="controls_levels" value="4" id="controls_levels_3" />
4</label></td>
<td><input type="radio" name="controls_levels" value="5" id="controls_levels_4" />
5</label></td>
</tr>

```

```

        <tr>
        <td colspan="2" bgcolor="#F71013">&lt;--- Weak</td>
        <td bgcolor="#FBF90C">Medium</td>
        <td colspan="2" bgcolor="#0CF34A">Strong ---&gt;</td>
        </tr>
    </table></td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
<td>&nbsp;</td>
<td colspan="2"><p><strong><br />
</strong></p></td>
</tr>
<tr>
<td colspan="4"><textarea name="controls_descriptions" cols="45" rows="5" required="required" id="controls_descriptions"></textarea></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td><input name="control_notes" type="hidden" id="control_notes" value="" /></td>
</tr>
<tr>
<td colspan="4">&nbsp;</td>
</tr>
<tr>
<td colspan="4" align="center"><input name = "createdby" type="hidden" id="createdby" value="<?php echo $_SESSION['user_name'];?>" />
<input type="submit" name="submit" id="submit" class="button pill primary" value="Submit" />
<input type="reset" name="Reset" class="button pill danger" value="Reset" /></td>
</tr>
<tr>
<td colspan="4">&nbsp;<?php echo $out ?></td>
</tr>
</table>
</form>
</div>
</body>
</html>

```

Company

```

<?php
include 'dbc2.php';
page_protect();
error_reporting(-1);
$username = $_SESSION['user_name'];
$sessionid = $_SESSION['user_id'];
$subscription = "SELECT * FROM users where id = '$sessionid'";
$result = mysql_query($subscription);
$data = mysql_fetch_assoc($result);
$subscription = $data['subscriptions'];
$u_level = $data['user_level'];
// set your db encoding -- for ascent chars (if required)
mysql_query("SET NAMES 'utf8'");
include("inc/jqgrid_dist.php");
// you can customize your own columns ...
$col = array();
$col["title"] = "No"; // caption of column
$col["name"] = "id"; // grid column name, must be exactly same as returned column-name from sql (tablefield or field-alias)
$col["width"] = "5";
$col["editable"] = false;
$col["hidden"] = true;
$col["search"] = false;
$col["align"] = "right";

$cols[] = $col;
$col = array();
$col["title"] = "Serial No";
$col["name"] = "c_serial";
$col["width"] = "10";
$col["editable"] = false;
$col["hidden"] = false;
$col["align"] = "left"; // this column is not editable
$col["search"] = true; // this column is not searchable
$col["editrules"] = array("required"=>true, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Company Name";
$col["name"] = "c_name";

```

```

$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
#$col["align"] = "center"; // this column is not editable
$col["search"] = false;
$cols[] = $col;
$col = array();
$col["title"] = "Address";
$col["name"] = "c_address";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Phone";
$col["name"] = "c_phone";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Email";
$col["name"] = "c_email";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Mobile";
$col["name"] = "c_mobile";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Fax";
$col["name"] = "c_fax";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Website";
$col["name"] = "Website";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Entity";
$col["name"] = "entity";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;

```

```

$col = array();
$col["title"] = "Pin No";
$col["name"] = "pin_no";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "registration no";
$col["name"] = "registration_no";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
$col["align"] = "left"; // this column is not editable
$col["search"] = false;
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Contact Person";
$col["name"] = "c_contact_person";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = true;
#$col["align"] = "center"; // this column is not editable
$col["search"] = false; // this column is not searchable
$col["editrules"] = array("required"=>false, "edithidden"=>true);
$cols[] = $col;
$col = array();
$col["title"] = "Contact Phone No";
$col["name"] = "contact_phone";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["align"] = "center"; // this column is not editable
$col["search"] = false; // this column is not searchable
/*$cols[] = $col;
$col = array();
$col["title"] = "Contact Phone No";
$col["name"] = "cp_phone";
$col["width"] = "10";
$col["editable"] = true;
$col["hidden"] = false;
$col["align"] = "center"; // this column is not editable
$col["search"] = true; // this column is not searchable
$col["editrules"] = array("required"=>false, "edithidden"=>true);
*/
$cols[] = $col;
$col = array();
$col["title"] = "Preview";
$col["name"] = "preview";
$col["width"] = "10";
$col["editable"] = false;
$col["hidden"] = false;
$col["align"] = "center"; // this column is not editable
$col["search"] = false; // this column is not searchable
$col["link"] = "a_company_preview.php?id={c_serial}";
$col["linkoptions"] = "target=myacc";
$cols[] = $col;
$grid["grouping"] = false; //
$grid["groupingView"] = array();
$grid["groupingView"]["groupField"] = array("pname"); // specify column name to group listing
$grid["groupingView"]["groupColumnShow"] = array(false); // either show grouped column in list or not (default: true)
$grid["groupingView"]["groupText"] = array("<b>{0} - {1} Item(s)</b>"); // {0} is grouped value, {1} is count in group
$grid["groupingView"]["groupOrder"] = array("asc"); // show group in asc or desc order
$grid["groupingView"]["groupDataSorted"] = array(true); // show sorted data within group
$grid["groupingView"]["groupSummary"] = array(true); // work with summaryType, summaryTpl, see column: $col["name"] = "total";
$grid["groupingView"]["groupCollapse"] = false; // Turn true to show group collapse (default: false)
$grid["groupingView"]["showSummaryOnHide"] = true; // show summary row even if group collapsed (hide)
$g = new jqgrid();
// $grid["url"] = ""; // your parameterized URL -- defaults to REQUEST_URI
$grid["rowNum"] = 20; // by default 20
$grid["sortname"] = 'id'; // by default sort grid by this field
$grid["sortorder"] = "ASC"; // ASC or DESC
$grid["caption"] = "Company Information"; // caption of grid
$grid["autowidth"] = true; // expand grid to screen width

```

```

$grid["multiselect"] = true; // allow you to multi-select through checkboxes
$g->set_options($grid);
$g->set_actions(array(
    "add"=>false, // allow/disallow add
    "edit"=>true, // allow/disallow edit
    "delete"=>true, // allow/disallow delete
    "rowactions"=>false, // show/hide row wise edit/del/save option
    "edithidden"=> true,
    "search" => "advance" // show single/multi field search condition (e.g. simple or
    advance)
));

// you can provide custom SQL query to display data
if ($u_level=='5') {
    $g->set_command = ('SELECT * FROM a_company ');
} else if ($u_level=='1') {
    $g->set_command = ("SELECT * FROM a_company where c_serial = '$subscription'");
}
/*if (isset($_SESSION['user_id'])) {
}
if (checkAdmin()) {
$g->set_command = ('SELECT * FROM a_company ');
}*/
// this db table will be used for add,edit,delete
$g->table = "a_company";
// pass the cooked columns to grid
$g->set_columns($cols);
// generate grid output, with unique grid name as 'list1'
$out = $g->render("list1");
$themes = array("redmond", "smoothness", "start", "dot-luv", "excite-bike", "flick", "ui-darkness", "ui-lightness", "cupertino", "dark-hive");
$i = rand(0,8);?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
<head>
<script src="http://code.jquery.com/jquery-latest.js" type="text/javascript"></script>
<link rel="stylesheet" href="//code.jquery.com/ui/1.11.4/themes/smoothness/jquery-ui.css">
<script src="//code.jquery.com/jquery-1.10.2.js"></script>
<script src="//code.jquery.com/ui/1.11.4/jquery-ui.js"></script>
<script src="vallenato/jquery-latest.js" type="text/javascript"></script>
<script src="vallenato/vallenato.js" type="text/javascript"></script>
<link rel="stylesheet" href="vallenato/vallenato.css" type="text/css" media="screen">
<link rel="stylesheet" type="text/css" media="screen" href="js/themes/<?php echo $themes[9]?>/jquery-ui.custom.css"></link>
<link rel="stylesheet" type="text/css" media="screen" href="js/jqgrid/css/ui.jqgrid.css"></link>
<script src="js/jquery.min.js" type="text/javascript"></script>
<script src="js/jqgrid/js/i18n/grid.locale-en.js" type="text/javascript"></script>
<script src="js/jqgrid/js/jquery.jqGrid.min.js" type="text/javascript"></script>
<script src="js/themes/jquery-ui.custom.min.js" type="text/javascript"></script>
<link href="styles.css" rel="stylesheet" type="text/css" />
<link href="class/gh-buttons.css" rel="stylesheet" type="text/css" />
<script>
$(function() {
    $("#dor_date").datepicker();
    $("#s_date").datepicker();
    $("#e_date").datepicker();
    $("#sb_date").datepicker();
    $("#handovodate").datepicker();
    $("#c_last_inspection").datepicker();
});
</script>
</head>
<body>
<div class="form" >
<?php
$query=mysql_query("select MAX(id)from a_company");
$result =mysql_fetch_array($query);
$cur_auto_id0= $result['MAX(id)']+1;
$cur_auto_id ='IS1'.str_pad($cur_auto_id0,5,'0',STR_PAD_LEFT);
//This function separates the extension from the rest of the file name and returns it
function findexts ($filename)
{
    $filename = strtolower($filename) ;
    $exts = split("[\\.]", $filename) ;
    $n = count($exts)-1;
    $exts = $exts[$n];
    return $exts;
}
//This applies the function to our file
$ext = findexts ($_FILES['photo']['name']);

```

```

//This line assigns a random number to a variable. You could also use a timestamp here if you prefer.
$ran = rand () ;
//This takes the random number (or timestamp) you generated and adds a . on the end, so it is ready of the file extension to be appended.
$ran2 = $ran.". ";
//This is the directory where images will be saved
$target = "dcim/";
$target = $target . $ran2.$ext;
//$target = $target . basename( $_FILES['photo']['name']);
$message="";
$message2="";
$ac="";
if (isset($_POST['submit'])){
$sql="INSERT INTO a_company(c_serial, c_name, c_address, c_phone, c_email,c_mobile,c_fax,website,entity,pin_no,
registration_no,c_contact_person, contact_phone, c_contact_email,photo,createdby,user_id, date) VALUES
('" . $cur_auto_id
.",'" . $_POST['c_name']
.",'" . $_POST['c_address']
.",'" . $_POST['c_phone']
.",'" . $_POST['c_email']
.",'" . $_POST['c_mobile']
.",'" . $_POST['c_fax']
.",'" . $_POST['website']
.",'" . $_POST['entity']
.",'" . $_POST['pin_no']
.",'" . $_POST['registration_no']
.",'" . $_POST['c_contact_person']
.",'" . $_POST['contactp_phones']
.",'" . $_POST['c_contact_email']
.",'" . $ran2.$ext
.",'" . $_SESSION['user_name']
.",'" . $_SESSION['user_id']
.",'" . date("d:m:Y H:i:s")."')";
//.'" . md5(date("d:m:Y H:i:s"))
if (mysql_query($sql) or die(mysql_error())){
    //move_uploaded_file($_FILES['photo']['tmp_name'], $target)
//echo $sql;
echo $message="Updated successfully";
}else{
echo $message="Error: ".mysql_error();
}
if(move_uploaded_file($_FILES['photo']['tmp_name'], $target))
{
//Tells you if its all ok
echo $message2= "The file ". $ran2.$ext. " has been uploaded, and your information has been added to the directory";

// header("Location: p_clients.php");
// exit();
}
}
?>
<form enctype="multipart/form-data" action="" method="POST" onSubmit="if(!confirm('Are You Sure?')){return false;}">
<table width="100%" border="0" class="form" id="accordion-container">
<tr class="headingTOP">
<td colspan="4">Company Information</td>
</tr>
<tr>
<td width="29%">Company Name </td>
<td width="22%"><input name="c_name" type="text" required="required" id="c_name" />
<input name="account_no" type="hidden" id="account_no" value="71<?php echo str_pad($cur_auto_id,8,'0',STR_PAD_LEFT);?>" /></td>
<td width="24%">Address <span class="example">(123-00300)</span></td>
<td width="25%"><textarea name="c_address" pattern="\d{6}-\d{5}" required="required" id="c_address"></textarea></td>
</tr>
<tr>
<td>Phone No <span class="example">(format: 254xxxxxxxx)</span></td>
<td><input name="c_phone" type="tel" required="required" id="c_phone" pattern="\d{12}" value="254" /></td>
<td>Email</td>
<td><input name="c_email" type="email" required="required" id="c_email" pattern="[a-z0-9._%+~]+@[a-z0-9.-]+\.[a-z]{2,3}" /></td>
</tr>
<tr>
<td>Mobile No <span class="example">(format: 254xxxxxxxx)</span></td>
<td><input name="c_mobile" type="tel" pattern="\d{12}" required="required" id="c_mobile" value="254" /></td>
<td>Fax No</td>
<td><input name="c_fax" type="text" id="c_fax" /></td>
</tr>
<tr>
<td>Website <span class="example">(http://)</span></td>
<td><input name="website" type="url" id="website" pattern="https?://.+&#x27;>title="Include http://" /></td>
<td>Business Entity</td>

```

```

<td><select name="entity" required="required" id="entity">
  <option value="--Select--">--Select--</option>
  <option value="Limited Liability">Limited Company</option>
  <option value="Partnership">Partnership</option>
  <option value="Sole Proprietorship">Sole Proprietorship</option>
  <option value="Other">Other</option>
  <option value="Individual">Individual</option>
</select></td>
</tr>
<tr>
<td>Registration No</td>
<td><input type="text" name="registration_no" id="registration_no" /></td>
<td>Pin No</td>
<td><label for="entity">
  <input type="text" name="pin_no" id="pin_no" />
</label></td>
</tr>
<tr>
<td colspan="2">&nbsp;</td>
<td colspan="2">&nbsp;</td>
</tr>
<tr class="headingTOP">
<td colspan="4">Contact Person information</td>
</tr>
<tr>
<td>Contact Person</td>
<td><input name="c_contact_person" type="text" required="required" id="c_contact_person" /></td>
<td>Contact Person Phone No</td>
<td><input name="contactp_phones" type="tel" id="contactp_phones" pattern="^\d{12}$" value="254" /></td>
</tr>
<tr>
<td>Contact Person Email</td>
<td><input name="c_contact_email" type="email" required="required" id="c_contact_email" /></td>
<td>Logo</td>
<td><input name="photo" type="file" class="button" /></td>
</tr>
<tr>
<td colspan="2">&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr>
<td colspan="4" align="center"><input name="createdby" type="hidden" id="createdby" value="<?php echo $_SESSION['user_name'];?>" />
  <input type="submit" name="submit" id="submit" class="button pill primary" value="Submit" />
  <input type="reset" name="Reset" class="button pill danger" value="Reset" /></td>
</tr>
<tr>
<td colspan="4">&nbsp;<?php echo $out ?></td>
</tr>
</table></form>
</div>
</body>
</html>

```

Dashboard

```

<?php
include 'dbc.php';
page_protect();
error_reporting(0);
$username = $_SESSION['user_name'];
$sessionid = $_SESSION['user_id'];
$subscription = "SELECT * FROM users where id = '$sessionid'";
$result = mysql_query($subscription);
$data = mysql_fetch_assoc($result);
$subscription = $data['subscriptions'];
$user_level = $data['user_level'];
//Retrieves data from MySQL
$id = filter_input(INPUT_GET,'id', FILTER_SANITIZE_STRING);
//$subscriptions = $_SESSION['subscriptions'];
if ($user_level=='5') {
  $assets = "SELECT count(*) AS assets FROM a_assets";
  $result = mysql_query($assets);
  $data = mysql_fetch_assoc($result);
  $assets = $data['assets'];
  //a_companys = "SELECT count(*) as companys FROM a_company WHERE user_id = $sessionid";
  $a_companys = "SELECT count(*) as companys FROM a_company";
  $result = mysql_query($a_companys);
  $data = mysql_fetch_assoc($result);
  $companys = $data['companys'];
}

```



```

} else if ($u_level=='1') {
    $assets = "SELECT count(*) AS assets FROM a_assets where c_serial = '$subscription'";
    $result = mysql_query($assets);
    $data = mysql_fetch_assoc($result);
    $assets = $data['assets'];
    //$a_companys = "SELECT count(*) as companys FROM a_company WHERE user_id = $sessionid;";
    $a_companys = "SELECT count(*) as companys FROM a_company WHERE c_serial = '$subscription'";
    $result = mysql_query($a_companys);
    $data = mysql_fetch_assoc($result);
    $companys = $data['companys'];
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Untitled Document</title>
<script src="http://code.jquery.com/jquery-latest.js" type="text/javascript"></script>
<script src="vallenato/jquery-latest.js" type="text/javascript"></script>
<script src="vallenato/vallenato.js" type="text/javascript"></script>
<link rel="stylesheet" href="vallenato/vallenato.css" type="text/css" media="screen">
<link href="styles.css" rel="stylesheet" type="text/css" />
<link href="invoice/2/table.css" rel="stylesheet" type="text/css" />
<link href="class/gh-buttons.css" rel="stylesheet" type="text/css" />
</head>
<body>
<div id="accordion-container">
<h2 class="accordion-header">Dashboard</h2>
<!--<div class="accordion-content">-->
<table width="100%" class="inventory">
<tr>
<th colspan="4" align="center" class="headingTOP">Summary</th>
</tr>
<tr>
<th>Total Companys</th>
<td width="30%"><a href="invoice/2/a_rpt_company_all.php" target="_new" class="button"><?php echo number_format ($companys);
?></a></td>
<th width="27%">Total Assets</th>
<td width="25%"><a href="invoice/2/a_rpt_assests_all.php" target="_new" class="button"><?php echo number_format ($assets); ?></a></td>
</tr>
<tr>
<th colspan="4" class="heading2">Company Ratings</th>
</tr>
<tr>
<th colspan="4"><?php
// Retrieve all the data from the "example" table where client_id =$id
if ($u_level=='5') {
    $query = "SELECT DISTINCT(c_name) AS service_category,count(*) as t_jobs, max(risk_score) AS risk_score,c_serial FROM
rpt_a_assets_views GROUP BY c_serial;";
} else if ($u_level=='1') {
    $query = "SELECT DISTINCT(c_name) AS service_category,count(*) as t_jobs, max(risk_score) AS risk_score,c_serial FROM
rpt_a_assets_views where c_serial = '$subscription' GROUP BY c_serial;";
}
// store the record of the "example" table into $row
$result = mysql_query($query) or die(mysql_error());
// Print out the contents of the entry in a table
echo "<table align='center' border='0' cellspacing='3' class='inventory' width='800px'>";
//echo "<tr><td colspan='4' ><img src='assets/images/Logo_Half.png' width='auto' height='auto' /> </td> </tr>";
echo "<thead><tr><th>Company</th> <th>Assets</th> <th>Risk Score</th> </tr></thead>";
// keeps getting the next row until there are no more to get
$i=0;
while($row = mysql_fetch_array($result)){
    $i++;
    //get alternating color for rows
    if ($i%2){
        $bg="#E6F2FF";
    }else{
        $bg="#FFFFFF";
    }
    //end alternating
    // Print out the contents of the entry in a table
    //echo number_format("1000000",2);
    echo "<tr><td bgcolor= $bg align = 'left'>";
    echo $row['service_category'];
    //echo "</td><td bgcolor= $bg align = 'center'>";
    //echo $row['service_category'];
}
}

```

```

        echo "</td><td bgcolor= $bg align = 'center'>";
        echo $row['t_jobs'];
        //echo "</td><td bgcolor= $bg>";
        //echo $row['risk_score'];
        if($row['risk_score'] >=1 && $row['risk_score'] <=6 )
            echo "</td><td style='background-color: #00FF00;' align='center'>LOW : ".$row['risk_score']. "</td>";
        elseif($row['risk_score'] >=7 && $row['risk_score'] <=12 )
            echo "</td><td style='background-color: #FFFF00;' align='center'>MEDIUM : ".$row['risk_score']. "</td>";
        elseif($row['risk_score'] >=13 && $row['risk_score'] <=25 )
            echo "</td><td style='background-color: #FF0000;' align='center' >HIGH : ".$row['risk_score']. "</td>";
        else if($row['risk_score']==") //[/val3] can be 'on hold'
            echo "</td><td style='background-color: $bg;' align='center'>No Result</td>";
            echo "</td></tr>";
        }
        //echo "<tr bgcolor=#fff><td colspan='3'>&nbsp;&nbsp;&nbsp;</td></tr>";
        //echo "<br />";
        echo "</table>";
?></th>
</tr>
<tr>
<th colspan="4" align="center" class="headingTOP"><p align="center">&nbsp;&nbsp;&nbsp;</p></th>
</tr>
</table>
</div>
</div>
</body>
</html>

```

Report_form

```

<?php
include 'dbc2.php';
page_protect();
mysql_query("SET NAMES 'utf8'");
$username = $_SESSION['user_name'];
$sessionid = $_SESSION['user_id'];
$subscription = "SELECT * FROM users where id = '$sessionid'";
$result = mysql_query($subscription);
$data = mysql_fetch_assoc($result);
$subscription = $data['subscriptions'];
$user_level = $data['user_level'];
include("inc/jqgrid_dist.php");
$themes = array("redmond", "smoothness", "start", "dot-luv", "excite-bike", "flick", "ui-darkness", "ui-lightness", "cupertino", "dark-hive");
$i = rand(0,8);
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
<head>
<script src="http://code.jquery.com/jquery-latest.js" type="text/javascript"></script>
<link rel="stylesheet" href="//code.jquery.com/ui/1.11.4/themes/smoothness/jquery-ui.css">
<script src="//code.jquery.com/jquery-1.10.2.js"></script>
<script src="//code.jquery.com/ui/1.11.4/jquery-ui.js"></script>
<script src="vallenato/jquery-latest.js" type="text/javascript"></script>
<script src="vallenato/vallenato.js" type="text/javascript"></script>
<link rel="stylesheet" href="vallenato/vallenato.css" type="text/css" media="screen">
<link rel="stylesheet" type="text/css" media="screen" href="js/themes/<?php echo $themes[9]?>/jquery-ui.custom.css"></link>
<link rel="stylesheet" type="text/css" media="screen" href="js/jqgrid/css/ui.jqgrid.css"></link>
<script src="js/jquery.min.js" type="text/javascript"></script>
<script src="js/jqgrid/js/i18n/grid.locale-en.js" type="text/javascript"></script>
<script src="js/jqgrid/js/jquery.jqGrid.min.js" type="text/javascript"></script>
<script src="js/themes/jquery-ui.custom.min.js" type="text/javascript"></script>
<link href="styles.css" rel="stylesheet" type="text/css" />
<link href="class/gh-buttons.css" rel="stylesheet" type="text/css" />
<script>
$(function() {
    $( "#inspection" ).datepicker();
    $( "#s_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s2_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e2_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s3_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e3_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s4_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e4_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s5_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e5_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s6_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e6_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s7_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e7_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();

```

```

    $( "#s8_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e8_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s9_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e9_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s10_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e10_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#s11_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
    $( "#e11_date" ).datepicker({ dateFormat: 'yy-mm-dd' }).val();
});
</script>
</head>
<body>
<table width="100%" align="center" id="accordion-container">
<tr class="headingTOP">
<td colspan="5">Reports</td>
</tr>
<form action="invoice/2/a_rpt_assests.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
<tr>
<td width="17%"><strong>Company</strong></td>
<td width="11%"><?php
    if ($u_level=='5') {
    $sql1 = ("SELECT distinct c_serial,c_name FROM a_company");
    } else if ($u_level=='1') {
    $sql1 = ("SELECT distinct c_serial,c_name FROM a_company where c_serial = '$subscription'");
    }
    $result1 = mysql_query($sql1);
    echo "<select name='id' >";
    while ($row = mysql_fetch_array($result1)) {
    echo "<option value=" . $row['c_serial'] . ">" . $row['c_name'] . "</option>";
    }
    echo "</select>";
    ?></td>
<td width="27%">&nbsp;</td>
<td width="27%">&nbsp;</td>
<td width="18%">
<div class="button-group">
<input type="submit" name="submit2" id="submit2" class="button pill primary" value="Generate" >
<input type="reset" name="Reset2" class="button pill danger" value="Reset" />
</div>
</td>
</tr>
</form>
<form action="invoice/2/a_rpt_jobs_cards.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="invoice/2/a_rpt_employees.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="invoice/2/a_rpt_jobs_cards_customer.php?id=<?php $row['c_serial']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="invoice/2/a_rpt_jobs_cards_customer_period.php?id=<?php $row['c_serial']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="invoice/2/a_rpt_jobs_cards_status.php?id=<?php $row['status']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="rpt_com_property_report.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="rpt_com_monthly_arrears.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="rpt_com_monthly_arrears_period.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="rpt_com_monthly_utility_billings.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
<form action="rpt_com_monthly_utility_receipts.php?id=<?php $row['pname']; ?> method=" enctype="multipart/form-data" target="_new"POST">
</form>
</table>
</body>
</html>

```