REPUBLIC OF UGANDA

MINISTRY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

NATIONAL INFORMATION SECURITY STRATEGY

(NISS FINAL DRAFT)

March 2011

TABLE OF CONTENTS

List of Acronyms and Abbreviations

CA	Certification Authority
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
GPS	Global Positioning System
EAC	East African Community
ERM	Enterprise Resource Management
IA	Information Assurance
ICT	Information and Commnucation Technology
IFMS	Intergrated Financial Management System
IMPACT	International Mulitilateral Partnershiships Against Cyber Threats
IRM	Information Risk Management
ISM_3	Information Security Maturity Model
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MDA	Government Ministry, Department, Agency
MoICT	Ministry of Information and Communications Technology
MoJCA	Ministry of Justice and Consitutional Affairs

NBI	National Backbone Infrastructure
NISS	National Information Security Strategy
NITA-U	National Information Technology Authority – Uganda
OIC	Organisation of the Islamic Countries
PKI	Public Key Infrastracture
PPP	Public Private Partnership
UCERT	Uganda Computer Emergency Response Team
UCC	Uganda Communications Commission
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WSIS	World Summit on the Information Society

EXECUTIVE SUMMARY

The way of carrying out business in the world today is changing rapidly with new technologies taking the center stage. Both government and the private sector are increasingly adopting the emerging technologies to modernize their service delivery. Cheaper broadband internet and an increased reliance on Information Technology Systems in both the Public and Private sectors come with the increasing risk of cyber attacks and other IT security threats.

Over the past few years the security ramifications of online activity have begun to permeate the national consciousness. However, despite the growing level of interest in this field, there is still little known about the actual issues involved in securing networks and electronic assets. Many people consider anti-virus software used to defend against Internet e-mail viruses to be the cure-all for all varieties of information security threats. Viruses are a big problem, no doubt, potentially leading to huge losses in terms of lost productivity and corrupted intellectual assets. However, cyber crime can be much more than the release of an e-mail attachment. The true dangers of cyber crime are of far greater consequence. Individuals with technical knowledge of networks and networking devices can steal sensitive information or money through online access to bank accounts or credit card numbers used with online retailers or conduct a host of juvenile pranks like erasing backup files, raising the temperature in buildings, turning off phone and traffic systems.

It is in this regard that the Ministry of Information and Communications Technology is taking the lead in development of a National Information Security Strategy which aims at addressing security challenges that are envisaged in this era of technological advances.

Chapter one gives a brief background about security challenges highlighting justification of developing such a strategy with a Mission, Vision and Strategic objectives that are key in answering the security challenge at a National Level.

Chapter two highlights the situational analysis of the current state of security in the country combined with a peer review of selected countries to guide the development of this strategy taking into account what other countries have done. This Chapter also highlights issues of Information Security Risk Management and also provides the Information security positioning

of Uganda using the Information Security Maturity Management Model. This chapter also provides a SWOT analysis of the current security challenges of Uganda.

Chapter three provides detailed information on the guiding principles on which this National Information Security Strategy should be developed. It highlights information on the Identification and Classification of Information Structures , it also provides information on the key guiding principles of this strategy which are; Legal Framework, Research and Development, Human Resource Capacity Building, Awareness and Training, International Cooperation, Resource Mobilization , Developing an Information Security Culture, Ensuring that e-Transactions are secured, Securing Critical Government ICT infrastructure, Compliance of non Governmental Enterprises on Security and Dealing with Emerging Security Risks.

Chapter Four provides information on Security Governance, proposing the different tiers of Security Governance structures. It introduces a Cyber Emergency Response Team (CERT)- a specialized organ for handling cyber security with direct reporting lines to the Head of State. This chapter also highlights the factors like Good Leadership, Awareness creation, Change Management, Funding, Collaborative Relationships and a costed Action Plan to be the critical success factors. It also provides information on the different institutional roles and responsibilities to ensure that the strategy is implemented successfully.

Chapter Five gives information on implementation modalities with indicative funding requirements if the country is to deal effectively with issues of informational security. It also provides detailed key funding areas as listed in the section on key guiding principles for this strategy.

CHAPTER ONE

1. INTRODUCTION

Information and Communications Technologies (ICTs) are vital tools in any information and knowledge based societies. Today's information society is driven by new technologies, new procedures and new expertise, the use of which is improving the welfare of citizens, changing our way of interaction and social participation, and promoting equality and democracy. These new technologies improve the productivity and competitiveness of companies and open up new markets while creating new business opportunities.

However, these new technologies continue to be exploited by malevolent users and the phenomenon is becoming intrinsically linked to organized crime on the Internet and internal malpractices that take advantage of weaknesses within information systems. Vulnerabilities in software applications are purposely sought after in order to create malware that will enable unauthorized access and modification, thus compromising integrity, availability and confidentiality of the ICT networks and systems. Other threats to information security include breaches of personal privacy, e-mail spam, industrial espionage, piracy computer viruses, cyber terrorism and electronic warfare. Any of these can spread worldwide in an instant through information networks. With the increasing sophistication of malware, these threats cannot be overestimated and they could have awful consequences on the critical information infrastructure of any country. It is prudent therefore, that due diligence and due care are implemented to ensure proper national information security management.

1.1 Definition of Information Security

Information security is the protection information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It is in this regard that the Ministry of Information and Communications Technology whose mandate is to provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy in all matters of ICT in consultation with various stakeholders has developed a National Information Security Strategy to address the information security issues at national level.

1.2 Background

Today world over, Information and Communications Technology (ICT) is the preferred platform for improved, efficient and effective service delivery in most public and private enterprises. Developments in Information and Communications Technology (ICT) are dramatically changing the way information is collected, stored, processed, disseminated and used, thus making it one of the most powerful tools for modernization and development.

In Uganda, ICT has been identified as one of the pillars for the National Development Plan (2010) and also one of the rapidly growing areas that have the potential to 'leap-frog' the nation to benefit from the globalised economy. e-Government, e-Commerce and other ICT-based services are earmarked among the first five priority areas for service export development, particularly through the smart strategic partnership programme between the Government, private investors, civil society and development partners.

The raise in use of ICTs world over, improved technology with faster communications networks and reliance on its performance has resulted into governments and other major businesses gradually transferring their operations from the traditional manual systems to ICT based infrastructure. This however, has brought about a raise in cyber threats. During the months of November and December 2010, *wikileaks.ch* released to the public over the internet US cables, confidential information presumed to be the governments top secret. This unauthorised disclosure caused pandemonium and built anxiety between the US and the affected countries.

Now that Uganda is connected to the internet through the faster fibre optic digital networks, it is possible that such attacks can materialize against its digital infrastructure through cyber warfare; cyber terrorism and cyber attacks. The government therefore must expeditiously develop a National Information Security Strategy to support sub-sector policies and frameworks within the ICT sector to secure critical national infrastructure and information resources.

1.3 Justification

The ICT Sector has been overtaken by various security emerging threats such as; advanced identity thefts, increasingly sophisticated cyber attacks, botnets, social engineering, cyber espionage ,mobile phone and VoIP threats, increasingly malicious web application vulnerability exploits, and supply chain attacks infecting consumer devices distributed by trusted organizations. The World Summit on the

Information Society (WSIS) recommends that member states implement measures along the following areas for Information Security:-

- Critical information infrastructure protection;
- Promotion of a global culture of cyber security;
- Harmonizing national legal approaches,
- International legal coordination & enforcement;
- Countering spam;
- Developing watch, warning and incident response capabilities;
- Information sharing of national approaches, good practices and guidelines;
- Privacy, data and consumer protection.

In January 2008, The East African Community instituted a task force to develop a cyber security framework. This framework contains a series of recommendations made to the governments of the partner states about reforming national laws to facilitate electronic commerce; to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers using online systems, and to protect individual privacy. The recommendations are designed to harmonize the law reform process between the EAC partner states, as well as reflecting international best practice

There have been considerable initiatives by the government of Uganda in the development and enactment of information security related bills into law, namely: Computer Misuse, Electronic signatures and the Electronic Transactions Laws. The NISS will provide a strategic guideline for the harmonization of all national efforts, EAC, and the international community to address information security and promote economic growth through the use of ICT by government itself, businesses, organizations and individual citizens.

Uganda 's significant advancement in ICTs investment is characterized by the recent connectivity to the submarine network, an effort that has created more bandwidth capacity in the country at reduced connectivity costs. This development exposes the national digital infrastructure to cyber threats and local security risks that should be addressed immediately in line with regional and international standards.

1.4 Vision

The vision is to provide a strategic direction for the national information security in order to promote trust and enable business and economic growth.

1.5 Mission

To provide a guideline that will reduce the probability of successful information security breaches and lower the risk of consequential damage within the national digital infrastructure.

1.6 Strategy objectives

The National Information Security Strategy shall have the following objectives;

i. Streamline the implementation of information security at the national and international level.
ii. Profile, Classify and Protect critical information infrastructure from disruption.
iii. Establish a framework responsible for the monitoring of the information security.
iv. Promote secure e-commerce and e-government services and other national IT projects.
v. Safeguard the privacy rights of individuals thorough good information security governance
vi. Development of a culture of cyber security awareness at national level and build human resource capacity.
vii. Uphold information security **risk** management and attain a good Information Security Maturity.

1.7 Strategy guiding principles

The NISS will provide a common platform for the information security efforts of the Government, businesses, Organizations and individual citizens. In order to align the strategic objectives with current government efforts and the international community, the following documents were largely consulted. World Summit on Information Society, National ICT Policy, EAC Cyber Law Framework, The Three National Cyber Laws, The Telecommunications Policy (2010), The e-Government framework (2010) and The National Development Plan (2010). The development context aimed at ensuring that;

i. There must be a strategy within government that will ensure access and full time availability of organized information and its integrity amongst its citizens and public service.
ii. The strategy implementation shall take into consideration the trend of Globalization to keep abreast with the modern, safe and better technologies of Information security.

iii. Government shall encourage citizen participation and mass awareness campaigns.

iv. The Government shall recognize the contribution of the business and private sector in enhancing information security.

v. The Government shall promote information protection schemes and mechanisms for assurance.

CHAPTER TWO

2. ANALYSIS OF CURRENT STATE OF INFORMATION SECURITY FRAMEWORK

2.1Situational analysis

The uptake of ICT in different Government Ministries, Departments, Agencies and Local Governments has not been uniform with some having more advanced systems than others. The Ministry of ICT organized interview sessions for the Government Ministries, Departments and Agents (MDAs) with a minimum level of ICT implementations. Different MDAs have different levels of ICT development and information security implementations. In the same way, IT information skills vary from entity to entity. Lack of knowledge in some institutions results into hiring of IT services to install, implement or update IT systems without much emphasis on information security. There are currently few MDAs with information security strategies or policies. Lack of top management support and too little financial support in implementing information security measures is also prevalent among many MDAs.

2.2 Peer Review of Selected Countries

International benchmarking with selected countries that have advanced in the areas of information security management was undertaken. They included two countries in the East African region (Rwanda and Kenya) and other countries that have been at Uganda's level of information security management in the recent past but have made significant leaps to address the risks associated with information security in a knowledge based economy that Uganda is strategically heading to. They countries included Mauritius, Malaysia, India and United Arab Emirates.

2.2.1 Mauritius

i. Developed law on Computer Misuse and Cybercrime Act (2203) to provide for repression of criminal activities committed through internet/ computer systems.

ii. To strengthen the legal framework for fighting cyber security, the following Acts were also developed;

   a. Data Protection Act
   b. ICT Act 2001
   c. Electronic Transaction Act 200
   d. Copyright Act 1997

e. Policy Framework for ISPs
f. Fair Trading Act

iii. The Information and Communication Technologies Authority (ICTA) was established to regulate the ICT sector in areas like telecommunications, usage of the internet and data protection.

iv. The Computer Emergency Response Team for Mauritius (CERT-MU) was established with the following main goals;

a. Handle security incidents and monitor security problems occurring within public and private sectors.

b. Provide guidance to providers of critical information infrastructure to adopt best practices in information security.

c. Warn and educate systems administrators and users about latest information security threats and suggest countermeasures by means of information dissemination.

v. Some of the services offered by the CERT-MU include;

a. Issuance of Security Alerts
b. Security Awareness programmes
c. Incident Response and Coordination
d. Collaboration with Industry and International CERTs

2.2.2 Malaysia

i. The Government recognized the potential cyber threats and through the Ministry of Science, Technology and Innovation developed a National Cyber Security Policy.

ii. The policy covers legislation and regulatory, technology, public-private cooperation, institutional and international aspects.

iii. The Government identified their countries' critical national infrastructure in order to plan appropriate security strategies according to the risks.

iv. The main areas considered are:

a. Effective Governance
b. Legislative & Regulatory Framework
c. Cyber Security Technology Framework
d. Culture of security and Capacity Building

e. Research & Development Towards Self-Reliance
f. Compliance and Enforcement
g. Cyber Security Emergency Readiness
h. International Co-operation

v. The Government established the Cyber Security Centre as a one-stop coordination centre for national cyber security initiatives.

vi. There is high level political and administrative buy-in in implementation of the cyber security strategy.

vii. Computer Emergency and Incident response is one of the core competencies of CyberSecurity Malaysia. These services responses are solely managed and coordinated by the Malaysian Computer Emergency Response Team (MyCERT), a division of CyberSecurity Malaysia.

viii. The team is always ready to serve Internet Users Malaysians in dealing with computer abuses and information security breaches including:

a. Assist Internet Users Malaysians in detecting, interpreting and responding to computer security incidents.
b. Alert Internet Users Malaysians in the event of security breach.
c. Coordinate expert advice whilst rendering remedial assistance.

ix. MyCERT acts as an independent focal point for Malaysian hosts, which allows both local and international experts, incident response teams, vendors, clients and law enforcement agencies, to cooperate and conduct vital technical and remedial action at sites affected by computer security incidents.

x. MyCERT to publish new advisories on new trends of security incidents and to assist other organizations in mitigating and reducing damages.

xi. MyCERT has the capacity to advise and provide assistance to law enforcement agencies but the team do not undertake any policing role or regulatory position.

2.2.3 India

i. The Government of India developed the Information Technology Act (2000) that addressed issues concerning use of electronic documents and signatures, judicial dispensation system for cyber crimes.

ii. Because of the increased use of the internet in daily lives and business, the government realized the need for a more comprehensive strategy to fight cyber crime and protect critical national assets.

iii. Information Technology Amendment Act (2008) that included sections on cyber terrorism and data protection.

iv. Set-up of the Public Key Infrastructure to promote the use of Digital Signatures.

v. Partnered with academic institutions to promote research and development in the area of information security.

vi. Development of the Information Security Policy Assurance Framework that caters for both Government and critical infrastructure.

vii. Development and roll out of a national awareness campaign on information security.

viii. The Department on Information Technology (DIT) developed a Cyber Security Strategy that addresses objectives with emphasis on the following initiatives;

   a. Security policy
   b. Compliance and Assurance that also covers India's critical infrastructure. The areas identified are in defence, finance, energy, transportation and telecommunications.
   c. Security Incident Early Warning Response
   d. Security training skills/ competence development
   e. Awareness Creation on IT security related issues
   f. Security promotion and publicity
   g. Security research and development for securing the infrastructure, meeting the domain specific needs

ix. Establishment of Computer Emergency Response Team to combat cyber crime and provide information security services to the critical information infrastructure sectors. The areas covered include;

x. Providing a single point of contact for reporting local problems.

xi. Incident handling and response

xii. Vulnerability analysis

xiii. Conduct training, research and development

xiv. Awareness creation

xv. Acting as the national point of contact and referral in incidents of cyber-intrusions

xvi. International co-operation with similar international bodies.

2.2.4 United Arab Emirates (UAE)

i. UAE passed Federal Law on The Prevention of Information Technology Crimes (2006).

ii. The Law covers cyber crimes and also online human trafficking.

iii. Established the United Arab Emirates Computer Emergency Response Team (aeCERT) with the aim of facilitating detection, prevention and response of cyber security incidents. Some of the goals under this initiative are;

   a. Enhancing the cyber security law and assisting in the creation of new laws.
   b. Enhancing information security awareness across the UAE.
   c. Building national expertise in information security, incident management and computer forensics.
   d. Providing a central trusted point of contact for cyber security incident reporting in the UAE.
   e. Establishing a national center to disseminate information about threats, vulnerabilities, and cyber security incidents.
   f. Fostering the establishment of and provide assistance to sector-based Computer Security Incidents Response Teams (CSIRTs).
   g. Coordinating with domestic and international CSIRTs and related organizations.
   h. Becoming an active member of recognized security organizations and forums.

iv. Entered a partnership and co-operation agreement with the International Multilateral Partnership against Cyber Threats (IMPACT). This was done to develop the capabilities of cyberspace security in the UAE, enhance the aeCERT capabilities in this area and to exchange information and benefit from all the experiences of IMPACT.

v. As part of strengthening the implementation of the cyber law, UAE launched a major reform of its court system to cope with the growth of the internet in the country. Accordingly, a ministerial resolution was taken to create special courts specifically dedicated to cybercrimes to speed up litigation and serve litigants more effectively.

2.3 INFORMATION SECURITY RISK MANAGEMENT

Risk management is the identification, assessment, and prioritization of risks as the effect of uncertainty on objectives, followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, negligence, natural causes and disasters as well as deliberate attacks from an adversary. **IT** risk management should be considered a component of a wider national ICT risk management system.

The establishment, maintenance and continuous update of an Information Security Management Systems (ISMS) provide a strong indication that Government MDAs are using a systematic approach for the identification, assessment and management of information security risks.

According to IT Risk management, there should be a framework that enables users to: Integrate the management of IT risk with the overall Enterprise Resource Management (ERM), Compare assessed IT risk with risk appetite and risk tolerance of the organization, and Understanding how to manage the risk. - IT Risk encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit\value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.

It is important therefore, that Government should consider a national IT Risk management strategy in the following areas of information security management.

Table 1.0 Generic National Information RISK Register

	External Risks	
	Risk	**Risk Description**
I.	Legal and regulatory compliance risk	Failure to comply with the national laws in which business operations are carried out; failure to comply with any regulatory, reporting and taxation standards, failure to comply with contracts; or failure of contracts to protect business interests
II.	Reputation risk	The negative effects of public opinion, customer opinion and market reputation, and the damage caused to the brand by failure to manage public relations
III.	Economic risk	Failure to monitor economic factors affecting information security implementation and governance.
IV.	Technology risk	Failure to plan, manage and monitor the performance of technology-related projects, products, services, processes, staff and delivery channels
V.	Political risk	Failure to accurately predict the political environment and relevantly uphold information management
VI.	Criminal and illicit acts risk	Loss or damage caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, extortion etc
VII.	Financial risk	Failure to secure adequate funding for information security

		governance.
VIII.	Supplier risk	Failure to evaluate adequately the capabilities of suppliers leading to breakdowns in the supply process or substandard delivery of supplied goods and services; failure to understand and manage the supply chain issues
No.	**Risk**	**Description**
Internal Risks		
IX.	Facilities and operating environment risk	Loss or damage to operational capabilities caused by problems with premises, facilities, services or equipment
X.	Health and safety risk	Threats to the personal health and safety of staff, customers and members of the public
XI.	Information security risk	Unauthorized disclosure or modification to information, loss of availability of information, or inappropriate use of information
XII.	Control frameworks risk	Inadequate design or performance of existing risk management infrastructure including effectiveness of policies and procedures in implementing security controls.
XIII.	Processing and behavioral risk	Problems with service or product delivery caused by failure of internal controls, information systems, employee integrity, errors and mistakes, or through weaknesses in operating procedures
XIV.	Corporate governance risk	Failure of leaders or directors to fulfill their personal statutory obligations in managing and controlling the institutions including misuse of resources
XV.	Project management risk	Failure to plan and manage the resources required for achieving tactical project goals, leading to budget overruns, time overruns or both, or leading to failure to complete the project; the technical failure of a project or the failure to manage the integration aspects with existing parts of the business and the impact that changes can have on business operations
XVI.	Strategic risk	Failure to meet the long-term strategic goals of business, including dependence on any estimated or planned outcomes that may be in control of third parties
XVII.	Human resources risk	Failure to recruit, develop or retain employees with the appropriate skills and knowledge or to manage employee relations
XVIII.	Social risk	Inability to control and otherwise manage social engineering behaviors and threats to information security

The strategy must be phased to document and indicate;

a) Risk Assessment Process- that includes; Documentation of System Identification, System Purpose and Description and System Security Level.

b) Risk Determination Phase which includes; Identification of System Environment Threats, system Vulnerabilities, a description of envisaged risk, Existing Controls, Risk materialization matrix and a determination of the Risk level.

c) Safeguard Determination Phase- to include identification of safeguards, determination of Residual Severity of Impact and Residual Risk Levels.

Mitigation strategies are discussed in Chapter 5 (operationalisation) in detail.

2.4 Information Security Positioning for Uganda (soft controls)

The Ministry of ICT in collaboration with the Swedish Program for ICT in Developing Regions (SPIDER) commissioned a study in 2008 from within 14 Government MDAs (see table 2.0) to assess information security implementation. Specific areas of concern included; physical security, web security, access control security, data security, application security, network and communication, security risk assessment & audit, security incident management and IT security strategy considerations.

In order to develop an information based action plan, interviews were carried out among these respondents to assess availability of relevant risk mitigation frameworks from which the information obtained would help in the assessment of information security position in key government sectors.

Below are current ICT installations running in Government MDAs from which respondents were chosen.

Table 2.0 Some of the current ICT systems running in Government MDAs

Information System in place	Government MDAs
Integrated Resource Management System	Ministry of Defense
Local Governments Information Communication System	Ministry of Local Government.
URANET and Electronic Tax (e-Tax)	Uganda Revenue Authority
Electronic Funds Transfer System,	Bank of Uganda
Salary and Wage Processing System	MOFPED
Integrated Personnel Payroll System (IPPS)	Ministry of Public Service
Court Case Management System	Judiciary
Land Information Management System	Ministry of Lands
e-Government Intercom	Ministry of ICT
Automation of the National Voters' Register	Electoral Commission
Health Management Information System (HMIS)	Ministry of Health
Education Management Information System (EMIS)	Ministry of Education
Rural Information System	Ministry of Trade
National Identification System	Ministry of Internal Affairs
Integrated Management Information System	National Social Security Fund

2.4.1 Analysis of Information Security soft controls among Government MDAs

Table 3.0

Information Security Control	in place	not in
Test environment for applications testing before moving to live environment	27%	73%
Quality Assurance /IT Audit on the organizational environment	36%	64%
Review and updating IT Security Policy	55%	45%
Developing and rolling out a security awareness program	36%	64%
Drafting IT Security incident management procedures	36%	64%
Review and update change management policies and procedures	36%	64%
Scanning of the network and identifying and closing ports open but not in use	64%	36%
Review Telnet and FTP usage and seek secure options	64%	36%
Security updates and alerts knowledge management	40%	60%
Password and access control procedures hardening and enforcing	82%	18%

The presention of these results show that there are still major challenges in implenting soft controls.

2.3 Information Security Maturity

Users of IT are constantly facing new issues as they attempt to secure themselves in an increasing risk environment. A Security Maturity Model is a means of describing the maturity of an organizations information security management. A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainably produce required outcomes. A maturity model usually provides:

a) a place to start
b) the benefit of an organization's prior experiences
c) a common language and a shared vision
d) a framework for prioritizing actions.
e) a way to define what improvement means for your organization.

A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison.

There are various security maturity models that describe maturity levels in different business areas in which information security plays a key role. Some published security maturity models specialize in security auditing, security documentation, security awareness, security management etc. See Table 4.0

Table 4.0: Information Security Maturity Models

Model	Area of Focus
NIST CSEAT- IT Security Maturity Model	Focused toward levels of documentation.
Citigroup's Information Security Evaluation Model (CITI-ISEM)	Focused toward organizational awareness and adoption
COBIT Maturity Model	Focused toward auditing specific procedures
SSE-CMM Six level of progressive maturity	Focused toward security engineering and software design
CERT/CSO Security Capability Assessment	Focused toward measurement of quality relative to levels of documentation.
ISMS (IM)-Maturity Capability Model	Focused toward information security culture.
Information Security Management Maturity Model (ISM_3)	Focused toward information security management process

The Information Security Management Maturity Model (ISM^3, or ISM-cubed) offers a practical and efficient approach for specifying, implementing and evaluating process-oriented information security management (ISM) systems. In ISM^3, two types of maturity are considered; coverage and capability. Capability maturity levels are described below and the process maturity levels are described in Table 5.0

Level 1. Undefined: The process might be used, but it is not defined.

Level 2. Defined: The process is documented and used.

Level 3. Managed: The process is Defined and the results of the process are used to fix and improve the process.

Level 4. Controlled: The process is Managed and milestones and need of resources is accurately predicted.

Level 5. Optimized: The process is Controlled and improvement leads to a saving in resources.

Information Security Management Maturity Model is widely used to manage the information security risk because of its compatibility with ISO 27001 information security management standard.

Based on the gathered data from the survey, Figure 2.0 presents key indicators that determine information security maturity. Though not exhaustive, some important deductions can be made as discussed later.

Figure 2.0 Information security maturity in Uganda

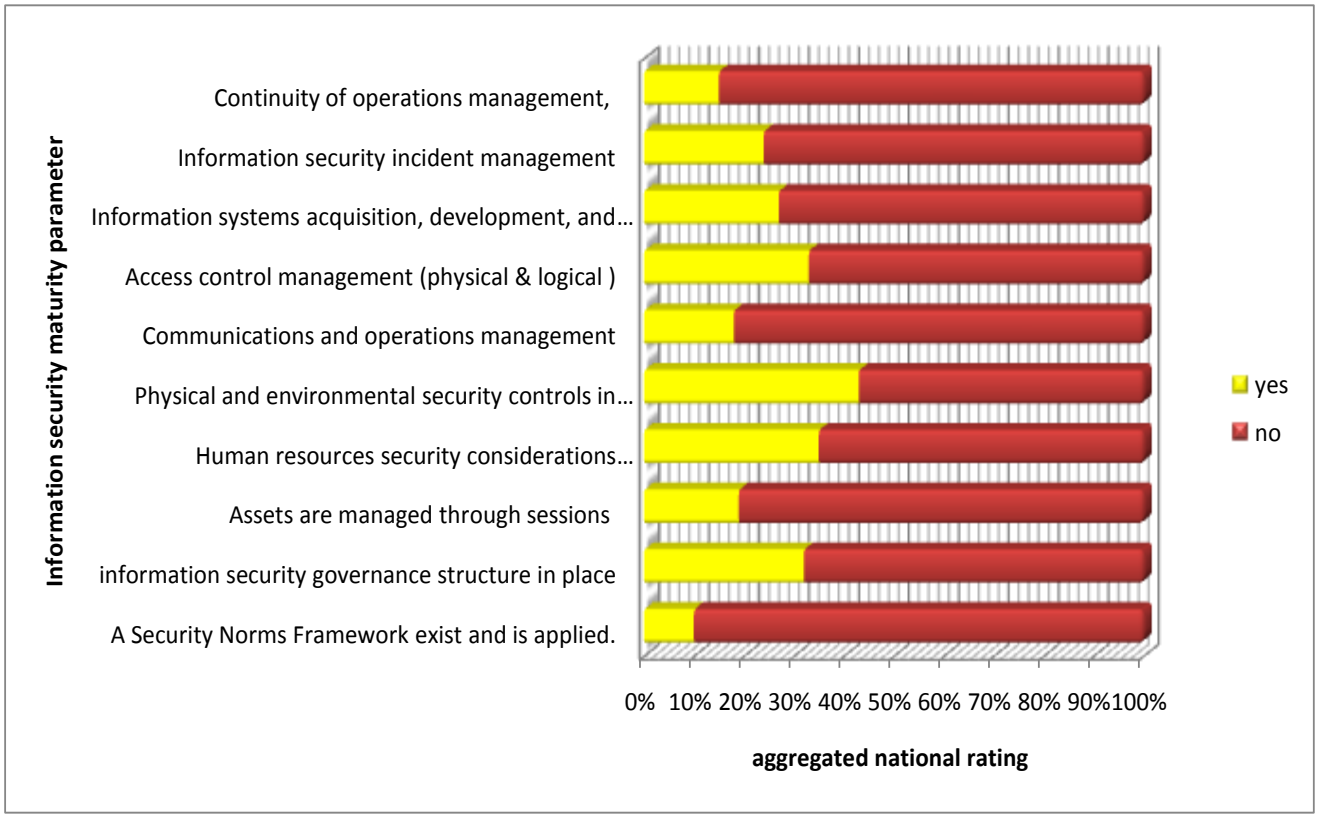
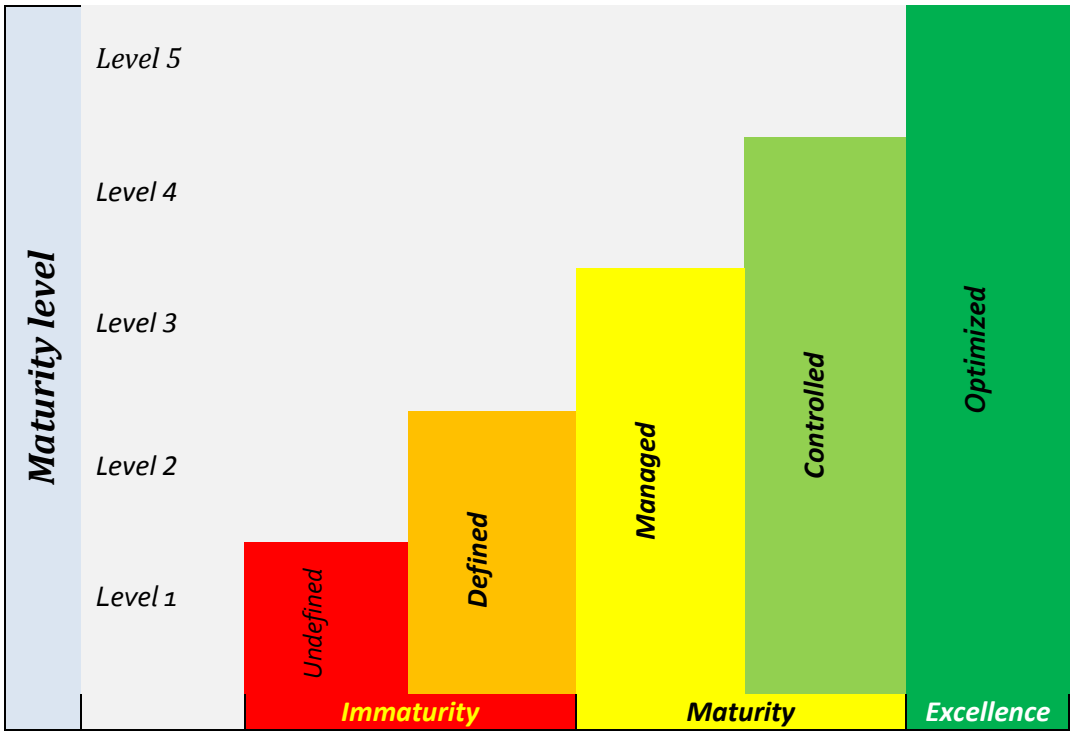


Figure 3.0 ISM³ (Information Security Maturity Management Model)



Though, there are initiatives already undertaken in some Ministries and or Authorities and National Companies, there is not much achievement so far registered. It can be deduced that basing on the ISM³, Uganda's information security maturity rating is **Level 1.**

At ISM³ Leve1, Security is not acknowledged as a desirable property of the organization. This was largely attributed to the fact there is lack of responsible officers charged with executing information security functions in many Government MDAs. The absence of incidents is the result of luck or individual efforts. The presence of incidents invariably leads to the maximum impact that could be expected.

On the other hand however, at level 5 of maturity, Security is acknowledged as a desirable property of the organization. The absence of incidents is the result of continuous organizational efforts. The presence of incidents doesn't lead to the maximum impact that could be expected.

a) Expectations, incidents and assets are evaluated quantitatively.
b) Organizational security responsibilities are defined.
c) A Security Norms Framework exists and is applied.

d) Assets are accessed using sessions only.
e) Security measures are audited.
f) Responsibilities are partitioned and supervised.
g) Quantitative information is collected about incidents or close calls.
h) Security measures are selected using objective criteria.
i) A "Continuity of Operations Plan" exists. This plan considers the organization's evolution and is properly implemented.
j) The best security measures are taken considering the budget. It can be determined if the budget is consistent with the targets defined by the Security Norms Framework.

The results of the organizational efforts are permanent.

The National Information Security Strategy therefore proposes and adoption of ISM[3] as a methodology for determining information security maturity growth in the country.

2.4 SWOT ANALYSIS

Table 5 : SWOT and Recommendation Strategies

Strengths	**Recommended Strategy**
1. Presence of Government political will in the area of national information security.	• Ensure continuous stakeholder involvement to bring on board key perspectives, including, academia, consumers, gender, disabled, and the youth • Establish the office of security at MoICT to oversee National Information Security Management.
2. Establishment of the National Information Technology Authority – Uganda.	• Support NITA to coordinate, and implement information security activities • Support NITA to establish a directorate for National Information Security related functions.
3. Constitution of the National Information Security Working Group.	• Facilitate the NIS working group to perform an advisory role for the implementation of the NIS strategy.
4. Ongoing approval process of the National IT Policy, E-Government Framework, Information Management Policy and E-Waste Policy	• Ministry of ICTs should coordinate all government related ICT initiatives and build capacity to initiate, implement and monitor ICT infrastructure projects. • Liaise with project management functional groups to ensure adequate security considerations.
Weaknesses	
1. Difficulty in attracting, recruiting and retaining skilled Information Security personnel.	• Identify, recruit and train information security personnel • Establish incentives to retain information security personnel
2. Inadequate budgetary allocations.	• Increase in budgetary allocations to information security area in MDAs
3. The roll out of ICT infrastructure is not standard across Government.	• Implement standardization policy framework • Acquire an international standard certification for Information security management across all government functions

	• Acquire a standards certification authority.
4. Lack of information security awareness and persistent poor information security culture	• Development of web portal on information security. • Development of Public Relations campaign on information security targeting the public • Awareness creation among top-level political and administrative leadership • Carry out information security awareness and training campaign in government MDAs and the public sector • Promote teaching of ICT in schools including modules on Information Security • Promote Public Access points, e.g. internet cafes, Internet Labs at Schools, Police, Military, Agricultural, Public Libraries and other institutions. • Market sensitization on the potential benefits of using ICT services • Promote development and usage of local content • Advocate the safe use of ICT as a trade enabler both locally, regionally and internationally.
5. Lack of supportive legal framework such as for the protection of intellectual property rights and data protection.	• Establish and implement a legal framework for information security management. • Establish and operationalise special cyber crime courts system
6. There are inadequate standards and maturity models adopted in the area of information security.	• Development of an Information Security Audit framework for MDAs and national companies • Development of a legal instrument requiring all national companies to report information security incidents • Develop a national cryptology policy • Development of a Data protection Act • Development or adaptation of information systems and infrastructure security standards • Development of guidelines, rules and standards on the infrastructure for digital signatures

	• Development of procurement guidelines for services in risk management, auditing, security assessment tools • Establishment of a global consensus and framework for electronic payments • Development and implementation of a national information security assessment framework
7. Lack of PKI infrastructure which impedes secured and trusted transactions.	• Implement a public key infrastructure certification authority in Uganda.
8. Lack of a cyber security specialist center	• Implement a National Computer Incident Response Team
Opportunities	
1. Actively participate in international co-operations on information security.	• Join international/ regional agencies created for fighting cyber crime. E.g. OIC CERT, IMPACT • Organization of an annual international event on information security • Ratification of the Budapest Convention on Cyber Crime and the European Convention on Cyber Crime
2. Increased availability of ICT literate graduates.	• Implement ICT including information security awareness campaigns among graduates
3. Improvement in the planning, monitoring and evaluation of the ICT sector.	• Ensure that information security activities are incorporated in the planning, monitoring and evaluation frameworks
4. Continued improvement in funding for ICT sector.	• Increase in budgetary allocations to information security area in MDAs • Proactively Solicit development partners for funding support for information security activities
5. Presence of the Ministry of ICT, NITA-U and the ICT Parliamentary Session Committee.	• Utilize these key stakeholders to obtain sufficient funding and the necessary support for legal and regulatory frameworks on information security.

Threats	
a) Cyber crime, cyber warfare and cyber terrorism.	• Establishment of a national Computer Incident Response Team with a 24/7 call center • Establishment of constituency Computer Incident Response Teams • Establishment of a Watch and Alert Center • Establishment of cyber reporting mechanisms for MDAs • Development of Business Continuity management framework for critical national infrastructure • Utilization of the national data centre to host all Government applications • Development of a national disaster recovery infrastructure plan for critical MDAs and national companies, utilize the NBI
b) Undefined cross-border jurisdiction for cyber litigation.	• Develop and implement cross-border jurisdiction for cyber crime litigation • Ratification of the Budapest Convention on Cyber Crime • Join international/ regional agencies created for fighting cyber crime. E.g. OIC CERT, IMPACT
c) Reliance on imported hardware and software.	• Put in place mechanisms that detect and control the quality of imported hard and software • Promote usage and certification of locally engineered software applications
d) Fast changing technology.	• Increase vigilance on adoption of upcoming technologies with emphasis on information security
e) Resistance to information security usage strategies and similar ICT initiatives by some public servants.	• Create and sustain awareness campaigns on information security among public servants • Establish risk assessment and audit compliance mechanisms among government MDAs

CHAPTER THREE

STRATEGY DEVELOPMENT GUIDING PRINCIPLES

3.1 The Strategy Framework

The National Development Plan (2010) under objectives, strategies and interventions, section 328, objective 2, strategy 1, calls for the enhancement of use and application of ICT services in business and service delivery. This requires a national information security strategy in order to safeguard the use and application of ICT services in service delivery.

The draft national IT policy (2010) for Uganda under the IT Security objective, strategy 1; calls for development of the National Information Security Strategy. The IT policy identifies information security as a sector on its own that requires a strategy which is in line with the aim of this strategy.

The draft Uganda National e-government framework (2010) points out information management and security aspects as one of the critical success factors for the e-Government programme implementation. Information security implementation is important in securing information and the platform for establishing trust in any e-government application.

The ICT Thematic Paper (2009) under the objective for the information technology subsector, strategy (iii) calls for establishment of a secure and enabling environment for the promotion of electronic commerce and creation of a National Information Security Centre. This identifies the need for national strategy on information security that is in the best interest of the country which is in line with the objectives. This strategy has been developed in the context of the international conventions that Uganda is party or signatory to. The Declaration of Principles of World Summit on the Information Society (WSIS2003, section B5) calls for building confidence and security in the use of ICTs as a prerequisite for the development of the information society and for building confidence among users of ICTs. Governments are required to put in place the necessary frameworks to secure ICT infrastructure and information against cyber threats. It is the intention of the Government of Uganda to consolidate its efforts and focus its energies to provide for national information security.

From the Analysis described in previous chapters, it is crucial to note that the policy, standards, laws and strategies have been aligned to fit international standards in the fight against cyber crimes. Lessons learnt can therefore be categorized in the functional areas of legal framework, incident handling, human resource capacity, awareness training and education, research and development, international cooperation and Resource mobilization as follows:

3.2 Identification and Classification of Information Infrastructures

All the countries benchmarked in the section above started with the identification of their critical infrastructure before applying any security measures. This should be the beginning point for risk assessments and implementation of critical protective measures. One distinct challenge here will involve identifying and securing infrastructures that are critical for the functioning of the society as a whole. This infrastructure and many others need to be safeguarded in this era of cyber warfare and cyber terrorism. There is also need to upgrade all MDAs to a uniform standard with attainable baselines and implement a common security norms framework in order to achieve information security maturity growth.

3.2.1. Information asset identification

Virtually every piece of information is considered an asset if used to conduct Government business. Examples of information assets include, but are not limited to:

a) Data/Information collections such as databases, data files, policies, standards, procedures, information archives, disaster recovery/continuity plans, and other paper or digital records.
b) Software assets such as application software and system software (as outlined in table 2.0 and others).
c) Physical assets, including computers (desktops, servers, notebooks, PDAs), communication equipment (telephone systems, fax machines, modems), storage media (tapes, removable disks, CDs), and even some facility equipment (generators, power supplies, air conditioners, furniture).
d) Outsourced services such as vendor support, consulting, contingency services, communication infrastructure, and environmental services (electricity, heating, etc.)

3.2.3. Information asset classification

To determine the measures required to adequately secure an information asset, the asset must be classified. The data owner is responsible for ensuring that each asset is evaluated against the criteria below and classified based on at least one of the three primary information security criteria; confidentiality, integrity, and availability. Criteria for classifying information include:

Confidentiality: For classification purposes, confidentiality refers to the sensitivity and the access controls required to protect the information. Does legislation policy require the information be protected, or is it freely distributable? Is the information time sensitive? Will its confidentiality status change after some time? Confidentiality is defined in terms of:

a) **Confidential**: Access is restricted to a specific list of people. Examples include human resources/payroll data such as salaries, garnishment orders, child support orders, and employee health information. Stored credit card numbers are also confidential.
b) **Sensitive**: Access and use of the information must be protected from routine disclosure and is restricted to specific uses only. This includes information required to be protected by legislation and/or generally recognized best practices.
c) **Public**: Where the resources are publicly accessible. For example, the Ministry Bulletin, the Ministry and enterprise Web Sites, recruitment brochures.

Access control is a primary component of confidentiality. Who must have access to the asset? Who should have access to the asset? Who can manipulate/modify the information? How should the information be stored? This is controlled by assigning access rights for individuals, groups, and the public. The asset owner determines these access rights. For data stored in the Colleague system, access is determined by security classes and defined in terms of:

a) **Never Do** – no access (to the particular role or security class);
b) **Privileged** – access to specified individuals/roles;

c) **Inquiry only** – access to read information only; and
d) **Do Only** – write access unless restricted by inquiry only or privileged.

Availability: This is a measure of criticality. How important is it that the information asset is accessible/ available to the authorized constituent? Is it a single instance or is a backup available? Availability is measured based on reliability and timely access to the asset. In other words, is the system up and running when needed? How long can the asset be down or unavailable? For classification purposes, the availability hierarchy is:

a) **Vital**: The asset is essential to the organization; even a brief outage is significant and may result in a serious negative impact, financial or legal.
b) **Critical**: Necessary for routine operation of the organization, must be available during normal working hours and/or during registration, reporting, or other business cycles. Brief outage other than during these periods is acceptable; outages during these periods are significant and result in serious negative impact.
c) **Important**: Significant to a small segment of the organization such as a single department or committee. Should be available during normal working hours, outages of up to 24 hours do not significantly impact the organization.
d) **Routine**: Has value to the organization and should be routinely available, but extended outages (1-5 days) would not significantly impact it.

Integrity: Integrity is seldom used for primary information classification, but may be used as a 'tie-breaker' when determining priority during business continuity and contingency planning. How important is it that the information is 100% accurate and can be verified as tamper-free? How critical is the accuracy of information to the nation or stakeholder? Can it be duplicated or replaced? Integrity is defined in terms of value: **high, medium or low**. As this is often a subjective valuation, justification may be required for assigning a value classification if the rationale is not obvious or is questionable.

Currently, Government information assets have not been profiled and classified using a published information security identification and classification scheme. It is recommended therefore that in order

to secure all information, a national information classification should be put in place. This is necessary to enumerate and classify the assets that need to be protected.

3.3 Legal Framework

The Cyber Laws that have been enacted to form specific legislation for information security. There is need for supporting standards to operationalise the Laws. To this end, the Government of Uganda shall:

a) Review and amend the relevant Laws and Acts to provide for the mandatory requirement for national institutions to carryout Due Diligence, implement Due Care and act in Prudence.
b) Review and amend the relevant Laws and Acts to provide for legislature that will compel national institutions to declare to the respective Government entity in charge of information security any information security incident that has potential to affect other Information systems or shared services.
c) Develop legislation to deal with data classification, intellectual property and data handling and protection to safe guard data and ownership.
d) Develop a standard business continuity framework for all Government MDAs.
e) Create a framework for the nation's critical internet resources like the Internet Addressing for Government and Domain management to ensure security.
f) Provide for more legislation especially in the area of information protection, copyright laws, privacy laws etc.

3.4 Research and Development

In Uganda, there is lack of research and development in the area of information security. To this end, the Government of Uganda shall:

a) Promote and provide Incentives for Research and Development (R&D) in the area of information security.
b) Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development.

3.5 Human Resource Capacity

Human resource is central to effective information security as it has been established as the weakest point. There is also limited awareness of the cyber laws among the wider public who will be affected. This strategy will assist in operationalisation of the cyber laws. There is lack of adequate human resource base with required expertise in information security in areas like information security management, auditing and forensics within Government. It should also be noted that Government currently may not have the necessary incentives to attract and retain skilled information security professionals.

Qualified information security professionals are inadequate, which will likely continue to be the case in the near future. The industry in Uganda has not had the time to grow the officers necessary for these roles yet information security challenges keep growing at a rapid pace. This translates into more time and money to get staff constantly trained on commercially available products. Obtaining the necessary credentials for information security requires considerable training and experience. A deliberate program to recruit, training and retain information security professional needs to be developed for Government of Uganda in order to have at least one such professional in all MDAs.

A qualified and highly skilled human resource base is pivotal to a successful information security strategy implementation. There is lack of adequate skills and expertise in this area. To this end, the Government of Uganda shall:

a) Promote and facilitate inclusion of Information Security in national curriculum in all institutions of learning.
b) Develop and implement programs to equip and retain the workforce within Government concerning skills in information security.
c) Develop a network of information security knowledgeable IT officers across Government MDAs.
d) Provide for basic skills in information security as a requirement for recruitment of Government IT officers.
e) Provide for acquiring information security officers in Government Ministries, Departments and Agencies

3.6 Awareness, Training and Education

Awareness is crucial in building an information security knowledgeable culture. Currently, there is limited awareness across Government, private sector and the wider public. Financial institutions and

banks have done information security awareness amongst their employees and clients ahead of other sectors. There is therefore, need for creation of security awareness among the public, private, business, civil society and wider public.

Awareness throughout the nation is an important success factor for the information security strategy implementation. To this end, the Government of Uganda shall:

a) Promote, foster and maintain culture of information security for awareness creation in Government, business and private sectors, civil society and the citizenry.
b) Organize annual events to promote information security.
c) Establish an effective mechanism of disseminating information security issues for different constituencies.

3.7 International Co-operation

The threat of cyber attacks are such that they are borderless and can be launched from any country in the world. Accordingly, it is important for Uganda to be part of international collaborations involved in fighting information security. To this end, the Government of Uganda shall:

Develop strategies and partner with international reputable organizations that will help it build capacity to manage any risk associated with information security arising out of border cyber activity.

3.8 Resource Mobilization

Currently, there is lack of adequate funds allocated to implementation of information security in most MDAs. To this end, the Government of Uganda shall:

a) Increase the budgetary allocation to the implementation of information security.
b) Put in place mechanism for resource mobilization from development partners.

3.9 Developing a culture of Information Security

We need to establish a culture of security in public, and private sectors linked to the use of IT. A lot of users are not aware of the risks arising from using an information network. Many do not know of existing solutions for avoiding potential threats. This makes it difficult for an individual to assess the risks associated with Internet access. This also indicates a need to raise users' awareness of security threats and improve their skills in dealing with them. Safe use of the Internet also has an ethical

dimension. This exerts new demands on acceptable ethical codes of conduct both on the part of Internet service providers and users themselves.

Currently, most government MDAs do not conform to any international accepted standards on information security. There is no model custom or published on security maturity that is in use to act as a guide in defining a maturity progression. The National Information Technology Authority – Uganda (NITA-U) was established in 2009 to address among others, the matter of defining standards, risk management strategies for information security. NITA-U should be facilitated to implement information security standards like ISO 2700 series, COSO, and COBIT and seek to establish progressive information security maturity levels. To achieve this, a framework for promoting information security maturity in the country should be developed. The goal of any maturity model is to lay out a program of work to achieve clear progress through easily identifiable milestones. The three goals in information assurance should focus on:

a) Embedding Information Risk Management culture within the organization.
b) Implementing best practice Information Assurance measures.
c) Effective compliance.

3.10 Ensuring that e-Transactions are secured

Far more extensive use of cryptography is recommended in order to strengthen trust and confidence in electronic communication, e.g. to ensure that financial transactions are indeed secure and that private communications remain private. However, there is a potential drawback to private individuals or enterprises using advanced cryptography to protect their own information against unauthorized access, as this could obstruct police investigations into serious crime and cyber terrorism. These considerations must be weighed carefully against each other.

3.11 Securing Critical Government ICT Infrastructure

The national information security strategy will need to address the need for business continuity management for critical national infrastructure. However, the challenge here will be to define a comprehensive set of generic criteria for securing critical functions in Government, partly because they differ so greatly. A generic set of common security measures will take care of the basic protection but issues of establishing an ICT national disaster program for the critical infrastructure must be addressed specifically.

3.12 Compliance of non Governmental enterprises on security

Respective management of public and private enterprises are primarily responsible for assuring that enterprise's assets are secure. The employees must be made aware of the substantial financial damage that could occur if there is a security breach. Enterprises need to set up an in-house IT-security unit / task force with clearly defined responsibilities. The management ought to allocate adequate resources for security work. The companies without an in-house security unit / task force must see to it that the company commands enough skills to be able to assure adequate IT-security by engaging the services of external security experts. Security consequences of outsourcing of IT services need also to be evaluated. Clear lines of responsibility must exist for those implementing the IT-security measures and those auditing the actual implementation.

3.13 Dealing with emerging Security Risks

Increasing use of laptops, mobile phones and PDAs with Internet access are bringing new risks for businesses. Broadband technology enables IT equipment to stay "always on". Exchanging and synchronizing data between portable and stationary units is becoming easier all the time. All this creates new challenges connected with uncontrolled information exchange and results in increased vulnerability and exposure to potential new types of attack. Theft of proprietary information is also a major risk to information security. When intellectual property (IP) is in an electronic form, it is much easier to steal. If this information is stored on computers connected to the Internet, cyber thieves can potentially steal it from anywhere in the world.

Three major issues have fueled the growth in cyber security incidents:

a) Increased number of vulnerabilities,
b) Labour-intensive processes required to address vulnerabilities,
c) The complexity of attacks.

These threats are expected to continue to grow in magnitude, speed, and complexity, making prevention and clean-up even more difficult. These factors contribute to the need for a proactive plan to address information security issues within every company and putting in place a national cyber security specialist centre under NITA-U or MoICT to provide safety of national cyberspace. It can provide other value addition security services including;

Cyber Help Centre, Computer Emergency Response Team, Digital Forensics, Security Management and Best Practices, Security Assurance and Certification, Vulnerability Assessment Services, Information Security Professional Development and Cyber Security Policy Research.

CHAPTER FOUR

4.0 Information Security Governance

According to ISO 38500, Information Security Governance is a system by which an organization directs and controls Information Security. Information security governance should not be confused with Information security management. Information security management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

Currently, there is lack of a national co-ordination approach for handling information security incidents. To this end:

a) The Government of Uganda shall institute the following proposed information security governance structure

Level	IS Strategy Committee	IS steering Committee	IS Technical Working Group
Responsibility	Provides insight, strategic direction of the Information Security Strategy	Define NISS objectives and align them to national business objectives	Responsible for technical implementation of the information security strategy
Authority	Advice to Government on National information Security	Assist leadership in the delivery of the NISS	Day to day management of Information Security
Membership	Permanent Secretaries,	Executives, Specialists, key advisors	Information Security practitioners

b) Creation of a government department to execute information security management responsibilities for the Government of Uganda.

c) Creation of a national Computer Incident Response Team (CIRT) to handle and provide specialized support for all information security incidents to both government and private sector. It is proposed that the CIRT be an autonomous institution operating under a highly placed Government institution in order to circumvent bureaucracies involved in responding to information security breaches. Due to the nature of cyber attacks, responses have to be swift and may involve classified spending.

4.1 Important Milestones and Critical Success Factors

No.	Critical success factors
1	Creation of a National Information Security Advisory Group to oversee Information Security Governance
2	Government to create an Agency on which other institutions can benchmark in the area of information security implementation.
3	Establishing a Directorate of security at NITA to implement National Information Security Management
4	Constant training and facilitation of the critical human resource levels required to implement information security governance and management.
5	Government commitment to continuous funding of information security governance programmes.
6	Development of a concise national information security program
7	A monitoring and evaluation framework to be developed and implemented using a reputable information security maturity model.
8	Implementation of a National Computer Incident Response Team

4.2 Distinguished Institutional Roles and Responsibilities

While the MoICT is responsible for overseeing the development, implementation, and maintenance of the Government's security program, it shall provide the necessary facilitation for the development of an excellent information security maturity level. Oversight requires the Ministry to provide NITA-U with guidance and approval of information security plans, policies and programs; and periodically review reports on the effectiveness of the information security program.

The Ministry shall provide support to NITA-U and hold it accountable for; central oversight and coordination, assignment of responsibility centers, risk assessments and risk measurement and mitigation, testing, reporting, and acceptable residual risk.

NITA-U shall put in place a mechanism to ensure that various institutions (information owners and information custodians) charged with any information aspect have provided for its risk measurement and mitigation in line Governments information security management objectives. Detailed roles and responsibilities are presented in table 7.0 below.

Table 7.0 Distinguished institutional roles and responsibilities

Institution	Roles and Responsibilities
MoICT	• The Ministry of ICT shall be responsible for policy, regulation and quality assurance as concerns Information Security. • Provide technical support in institutionalization of a strategic advisory group. The Group shall periodically review the information security strategy and monitor implementation and recommend revision at a strategic level of governance. • Develop a Private Public Partnership policy to guide strategy implementation within the private sector • Take lead in consultation with development partners. • Develop meaningful co-operation with the business sector in the area of information security and fighting cyber crime. • Monitor level of information security maturity in MDAs • Take the lead in the establishment of a national CIRT under Office of the President

NITA-U	• Set information security standards for the Business Process Outsourcing Industry and MDAs • Ensure that best practice and consistent standards are applied across government to ensure information security implementation. • Develop and implement a national information security program that includes information risk assessment frameworks, risk mitigation schemes, for all national institutions. • Establishment for minimum rules and standards on the infrastructure for digital signatures.
UCC	• Establish responsibility rules for the internet service providers to ensure information security. • Develop mechanisms for controlling abuses.
Ministry of Public Service	• Integrate information security skills into core competencies at all IT officer levels.
Ministry of Justice and Constitutional Affairs	• Establish special courts to deal with cyber crimes. • Integrate cyber crime litigation skills into core competencies at all levels.
Uganda Police Force	• Develop a cyber crime unit within the Force to deal with cyber crime
Bank of Uganda	• Develop mechanism for enforcing mandatory security risk assessment and audits in all financial and banking institutions. • Develop and implement a framework for electronic payments.
Local Governments	• The Local Governments shall be the link with the communities and shall carry out sensitization about on Information Security as well as promotion and awareness campaigns in the communities. • Ensure that all IT Infrastructure and Resources at the District meets the required security standards
Other stakeholders	• Incorporate Information Security Strategy objectives into the approach for service delivery and into institutional frameworks. • Align expenditure of funds and resources that support IT investments in line with the strategy. • Participate in Information Security awareness campaigns

CHAPTER FIVE

5. OPERATIONALISATION

5.1 Information Security Governance

Strategies	Objectives	Outputs	Resp.	Timeframe	Source of Funding	Budget Estimate USD(000)				
						2011	2012	2013	2014	**2015**
Creation of an Information Security Advisory Group	To provide advisory service to information security Governance	3 Tier advisory groups working at different levels of IS Governance	MoICT	2011-2016	GOU	1500	300	300	300	300	300
Capacity Building in NITA	To institutionalize a coordination center for Information Security Management	A Directorate of Information Security at NITA	NITA	2011-2016	GOU	6800	2300	1200	1400	1400	1500
Cyber Security Specialist Center	To establish constituency Computer Incident Response Teams	Constituency Computer Incident Response Teams established	MoICT Office of the President	2011-2016	GOU	4100	2000	600	500	500	**500**

5.2 Information Security Maturity and Standardization

Strategies	Objectives	Outputs	Resp.	Timeframe	Source of Funding	Budget Estimate USD(000)				
							2011	2012	2013	2014	**2015**
Standardization	To Develop an Information Security Audit for MDAs and national companies	Information Security Audit report and security roadmap	MoICT NITA-U	2011-2011	GOU	1,500	1,500				
	To Develop a legal instrument requiring all national companies to report information security incidents	Legal instrument on information security incidents in place	MoICT, NITA-U	2012-2014	GOU	450		300	150		
	To Develop a national cryptology policy	A national cryptology policy in place	MoICT	2011-2013	GOU	120	90		30		
	To Develop a Data protection Act	A Data protection Act ready for implementation	MoICT	2011-2012	GOU	250	110	10			
	To develop or adapt information systems and infrastructure security standards	Security standards for information systems and infrastructure in place recommended ISO 27000 series	NITA-U	2011-2013	GOU	180	60	60	30	30	
	To Develop guidelines, rules and standards on the infrastructure for digital signatures	Approved guidelines, rules and standards on infrastructure for digital signatures	NITA-U	2012-2014	GOU	80	40	20	20		
	To Develop procurement guidelines for	Procurement guidelines that are consistent with	MoICT	2012-2014	GOU	45	45				

	services in risk management, auditing, security assessment tools	national PPDA guidelines									
	To establishment a global consensus and framework for electronic payments	Electronic payments framework	MoICT NITA-U BoU	2012-2015	GOU	520	120	120	80	50	**50**
	Development and implementation of a national information security assessment framework	Implemented national information security assessment framework	NITA-U	2011-2012	GOU	600	400	200			
	To establish a special cyber crime courts system	Cyber crime courts system established	MoJCA MoICT	2013-2015	GOU	450			300	100	**50**
	To create a cyber crime investigation unit in Uganda Police Force	Cyber crime investigation unit established in Uganda Police Force	UPF MoICT	2012-2013	GOU	425		325	200		
	To establish an agency in charge of all information security matters	Agency in charge of all information security matters established	MoICT	2011-2013	GOU	1200	700	300	200		
	To Develop information security standards for the common number system for initiatives like national ID project	Information security standards for the common number system developed	NITA-U	2011-2012	GOU	125	100	25			
	Attain level 4 of the ISM^3 maturity level	Compliance for level 4 maturity level among all MDAs by 2016	NITA-U	2011-2016	GOU	1500	300	300	300	300	**300**

5.3 Human Resource Development

5.4 Information Security Culture

Strategies	Objectives	Outputs	Implementing Agency	Timeframe	Source of Funding	Budget Estimate USD(000)				
						2011	2012	2013	2014	**2015**
Government IT officers Publicity,	To develop capacity in information security management Development of Public Relations campaign on information security	Web Portal developed Campaign on information security developed	IT portfolio in government MDAs MoICT UCC NITA-U Trained Government Officers in place MoICT NITA-U	2011-2016 2013-2016	GOU GOU	2500 1650	750	600 750	500 500	200 **400**
Judiciary Training	To Reinforce cyber crime litigation competence of Judges, Magistrates and State attorneys Awareness creation among top level political and administrative leadership	Judiciary team trained to deal with cyber crimes High level workshops and benchmark study tours	MoJCA MoICT MoICT	2013-2016 2012-2015	GOU GOU	650 900	150	100 300	100 300	100 **100**
Police	To Develop investigations skills for cyber crime cases Operationalize structured security events	Team of police trained in investigation of cyber crimes Annualized event	NITA-U UPF MoICT NITA-U	2012-2015 2011-2016	GOU GOU	900 1250	300 250	200 250	200 250	100 **250**
Academic	Development and adaptation of curriculum to include information security in all institutions of learning	Curriculum on information security developed and implemented in all institutions of learning	MoICT MoES MoICT	2011-2016	GOU	250	50	50	50	**50**

Strategies	Objectives	Outputs	Implementing Agency	Timeframe	Source of Funding	Budget Estimate USD(000)

5.5 International Co-operation

Strategies	Objectives	Outputs	Resp. Agency	Timeframe	Source of		Budget Estimate USD(000)				
							2011	2012	2013	2014	**2015**
	Join international/ regional agencies created for fighting	International/ regional partnerships to developed and implemented	MoICT								
International strategy	organize an annual international event on information security	Annual international event on information security organised	MoICT	2013-2016	GOU	1250	1250	250	250	250	250
	Ratification of the Budapest Convention on Cyber Crime	High level workshops and benchmark study tours	MoICT	2012-2014	GOU	120		50	40	30	

5.6 Resource Mobilization

					Funding		2011	2012	2013	2014	**2015**
	Increase in budgetary allocations to information security	Increased budget allocation for	MoICT	2011-2014	GOU	65	25	15	15	10	

Strategies	**Objectives**	**Outputs**	**Resp.**	**Timeframe**	**Source of Funding**	**Budget Estimate USD(000)**					
						000	2011	2012	2013	2014	**2015**
Funding	Solicit development partner support in capacity building	Development partners to support capacity building programmes identified and support obtained	MoICT NITA-U	2013-2015	GOU	125			50	50	25

5.7 Securing E- Business

Establishment of a functional PKI	To provide an enabling infrastructure for e-business to thrive	a National PKI infrastructure	NITA-U	2011-2014	GOU	4650	3000	1000	500	150

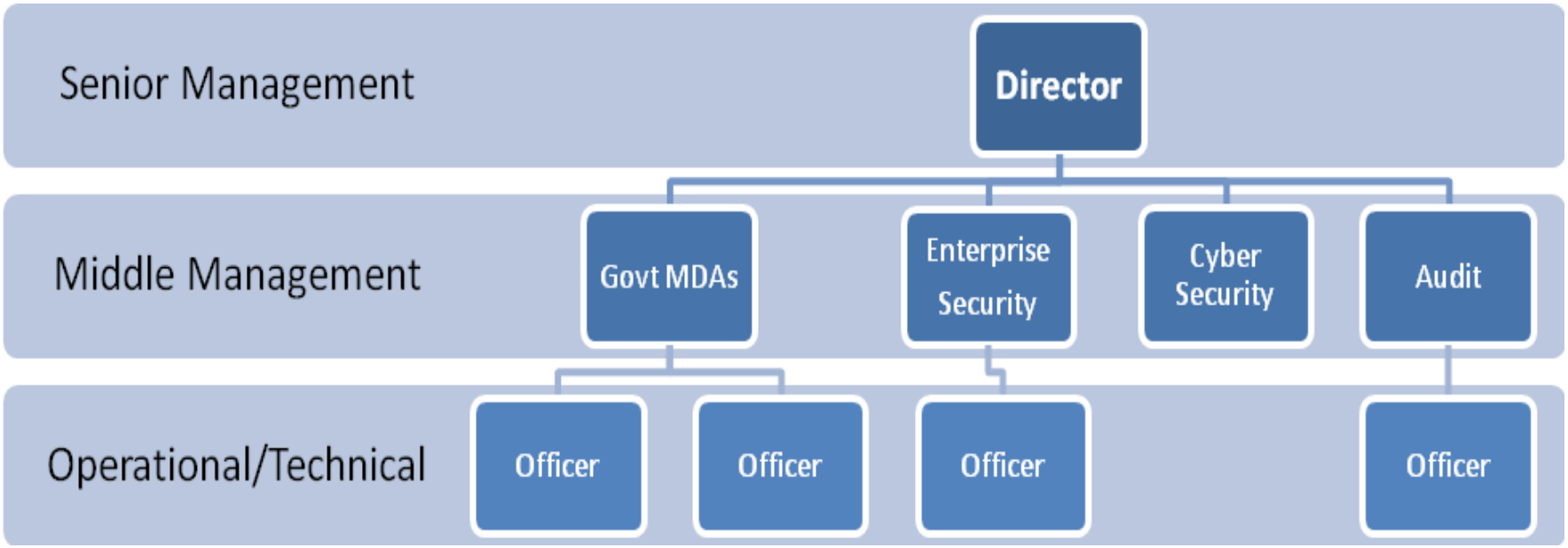
5.8 Research and Development

Strategies	Objectives	Outputs	Resp.	Timeframe	Funding	Budget Estimate USD(000)				
						2011	2012	2013	2014	**2015**
	To Develop an incentive strategy to support R&D in information security	R&D strategy to support information security	NITA-U	2011-2013		80	80	80		
Data Availability	Utilization of the national data centre to host all Government applications	Connectivity to the National Recovery center	NITA-U	2013-2015		1650		1000	500	**500**	150
Disaster Recovery	To Develop a national disaster recovery infrastructure plan for critical MDAs and national companies, utilize the NBI	National disaster recovery infrastructure plan in place	NITA-U	2013-2015		**21**00		**1500**	**300**	**200**	**100**

5.9 Data Protection

Strategies	Objectives	Outputs	Resp.	Timeframe	Source of Funding	Budget Estimate USD(000)					
							2011	2012	2013	2014	**2015**
Data Classification	To improve and optimize the confidentiality, integrity and availability of national information systems	A national data classification policy implemented.	NITA-U	2011-2014	GOU	4650	3000	1000	500	150	
Data Privacy	To safeguard data on persons collected and held by institutions and protect misuse	Legal and regulatory frameworks in place	MoICT	2012	GOU	50		50			
Copyrights and Infringements	To protect intellectual rights of individuals for their original works and promote trade	Copyright laws amendment	MoICT	2012	GOU	50		50			

Proposed structure for the Directorate of Information Security at NITA



Proposed structure and Functions for CIRT- Uganda

CIRT - Uganda				
Departments	Cyber Security Emergency Services	Cyber Security Research and Development	Outreach and Professional Development	Quality Management Services
Functions	Forensics, Investigation Laboratories, Incident Management and Help Center	Cybre security research and policy development	Professional certification and awareness creation	Maturity modeling, BCP and DRP Services, evaluation and certification services