وزارة الاتصالات وتقنية المعلومات

Ministry of Communications and Information Technology

Developing National Information Security Strategy for the Kingdom of Saudi Arabia

NISS, DRAFT 7

TABLE OF CONTENTS

TABLE OF FIGURES

1.0 EXECUTIVE SUMMARY

This National Information Security Strategy (NISS) for the Kingdom of Saudi Arabia (KSA / Kingdom) is in response to a Request for Proposal (RFP) issued by the Ministry of Communications and Information Technology (MCIT), dated Muharram 1432H, January 2011 as an initiative from Cabinet Resolution 82.

MCIT's NISS Objectives [1]:

1) Enable information to be used and shared freely and securely.
2) Increase the security, safety, and integrity of online information, while promoting the increased use of information technology.
3) Develop resilience in information systems.
4) Increase awareness and education of security risks and responsibility of information protection.
5) Create a set of national guidelines for Information Security Management, Risk Management and Business Continuity based on international standards and best practices.

The need for the National Information Security Strategy (NISS) is dictated by the complexity of today's interconnected computer networks. Government agencies are no longer solely responsible for the security of their information and Information Communications Technology (ICT) systems. In fact, their networks have no boundaries because of the remote connectivity that extends them throughout the world.

ICT security is now a primary driver that supports the Kingdom's growth in new areas. The NISS is a foundational element for this growth. While most countries recognize the need to better align information security with the goals of their nations, many are still struggling to translate this recognition into concrete plans of action. This NISS is a strategy for guiding the Kingdom to the needed state of information protection with secure and resilient ICT infrastructures.

The ICT changes in our increasingly interdependent world are complex and rapid. National and international interconnectivity create significant new vulnerabilities and present new types of threats to the Kingdom's economic and cultural activities. These new threats could in some cases shutdown, corrupt or even destroy critical ICT systems. In certain cases, an adversary might be able to seize control and use an ICT system to directly harm or go against the Kingdom's interests. The potential risk incurred by use of ICT systems must be adequately managed to achieve the productivity and collaborative benefits such systems provide.

The NISS priority is Information Security (IS) for all government agencies and business sector. IS requires the integration of people, processes, and technology. Each of these three (3) components should be carefully managed, considering the capabilities and limitations of the other components.

- People - This strategy suggests among other groups of people leveraging women and the Saudi youth as a key element to a successful IS deployment.
- Processes – By utilizing some of the key points here and leveraging the Kingdom's existing laws, Saudi Arabia is well positioned to implement the NISS.
- Technology – Newer and better technology will always be available. The key is to utilize the proper tools at the proper time.

When people, processes and technology are considered in total, they should provide for adequate overall IS risk mitigation.

---

[1] Request for Proposals (RFP) for Developing a National Information Security Strategy, Kingdom of Saudi Arabia, Ministry of Communications and Information Technology, Muharram 1432, January 2011.

It is widely accepted that cyber-terrorism, cyber-war, and cyber-espionage are successful due to the vulnerability of computer networks and critical infrastructures. These vulnerabilities have the potential to place the Kingdom at significant additional risk, in part because of the rapidly growing dependence of economic and financial activity on the ICT. A closer look at the relationships between computer networks and critical infrastructures, their vulnerability to attack and the subsequent effect on national security strongly suggest that the Kingdom needs to employ increased cyber and critical infrastructure protection. A full assessment of those two (2) areas is outside the scope of the NISS. A recommendation of the NISS is that separate strategies be developed for Cybersecurity and Critical Infrastructure Protection (CIP), as they are important complements to the NISS and necessary for comprehensive protection of the Kingdom's vital national interests and assets.

NISS Vision

The NISS is an integrated strategy designed to meet the Kingdom's national information and ICT security objectives. These objectives in turn support the achievement of the Kingdom's long-term plans and strategy, which depend upon a secure, reliable and resilient information infrastructure. The NISS is designed to bridge the gap from the Kingdom's current state of information security (IS) to its future IS vision, which is:

> ***The Saudi Arabian information society will have a secure, resilient foundation whose information security is supported by world-class practices and highly qualified Saudi practitioners.***

The NISS vision includes the following successes:

1) A secure, reliable and resilient national ICT infrastructure
2) A highly capable human information security resource
3) A national information security environment and management structure built upon trust, confidence, transparency and cooperation
4) A secure and dependable set of e-government services and supporting infrastructure throughout the Kingdom that meet the security objectives of the Kingdom's ICT plans and strategies
5) A flourishing and continuing IS economic sector of research, innovation and entrepreneurial activities

NISS General Objectives

The ten (10) NISS General Objectives are the guideposts for the Kingdom's on-going and future information security efforts. They were established to enable the Kingdom's information security foundation and posture to improve in a coordinated and effective manner and support national ICT goals and objectives. They also represent a top level statement of the NISS Elements and were generated using the NISS objectives set by the Kingdom, as well as various objectives in the Kingdom's national plans related to information and information security. The NISS General Objectives are listed below:

O-1 – Effective and Secure Information Security Environment

Work towards assuring that appropriate and consistent information security policies, directives, guidance, practices and oversight are achieved within the Kingdom. This process shall be responsible for the detailed implementation of the NISS objectives, and recommendations..

O-2 – Information Systems and ICT Infrastructure Enhancement

Enhance the security, reliability, availability and resilience of the Kingdom's ICT infrastructure and information systems.

O-3 – Human Resource
Improve the IS human resource and expand the capability of Saudi information security practitioners, researchers, innovators and entrepreneurs, both men and women; and establish special programs for training and awareness especially directed towards women and youth of all ages.

O-4 – IS Threat Analysis and Mitigation
Establish an IS function and analysis capability to collect and analyze vulnerabilities, all-source threats and risks to the Kingdom's ICT resources.

O-5 – Reduction of On-going ICT Exploitation
Reduce and prevent exploitation of weak points in the Kingdom's information security (IS) by employing the best international mitigation practices in local and national areas of highest IS risk.

O-6 – IS Compliance and Tracking Processes
Maximize progress toward national improvement benchmarks and goals by implementing a comprehensive compliance and tracking process, which ensures compliance with IS policies and standards and measures the progress and status of the Kingdom's information security initiatives.

O-7 – Research, Innovation and Entrepreneurship
Meet future IS needs by stimulating and directing the Kingdom's IS research and innovation programs that have high potential for commercialization and IS breakthroughs, including cryptographic interoperability, supply chain integrity, computer security and rapid and effective access control.

O-8 – Maintenance of Information Security
Ensure adequate IS protection for the Kingdom by maintaining a continuous process that supports the IS defensive posture for essential ICT infrastructures and information systems, and addresses new IS threats and vulnerabilities.

O-9 – National and International Cooperation
Achieve greater security for the Kingdom's information and ICT infrastructures by implementing new domestic ICT security coordination and information sharing processes among stakeholders and by leveraging international collaboration efforts.

O-10 – Information Security Awareness and Responsibilities
Increase in all people their awareness of IS threats and vulnerabilities, as well as their understanding of personal responsibilities to improve information security in their work environments and daily lives.

NISS Elements

The objectives of each NISS Element were independently established and compared to the NISS General Objectives for compatibility. The nine (9) Elements that compose the NISS are listed below.

NISS Elements
• Information Security Environment
• Policy and Regulation
• Risk Management and Assessment
• National ICT Infrastructure
• Human Resource
• Re-assessment and Audit
• National Cooperation and Sharing for Information Security
• International Cooperation and Sharing for Information Security
• Research and Innovation

The recommendations related to each NISS Element are as follows:

Information Security Environment

The first step is consideration of, and agreement by, the Kingdom on a secure and effective information security environment. International research from Asia, Europe and North America showed that a centrally-managed information security is the most effective and efficient way to protect their respective nations. Because of domestic political factors, few countries are able to implement an effective national organization that covers all government agencies, as well as the business sector. The current ICT environment with borderless infrastructure connectivity makes the threat, vulnerabilities and risk that one organization faces heavily dependent upon actions (or lack of actions) of other entities inside and outside the Kingdom. Such interconnection makes all systems of the government susceptible to compromise. A central national information security environment for managing information security is recommended to provide better coordination and security across the Kingdom's information and ICT infrastructure.

Policy and Regulation

This strategy recommends forming agreements, and the development and adoption of a set of national information security policies that form the IS framework for the Kingdom. This, in turn, will lead to national standards and best practices.

In addition, based upon a gap analysis, a periodic review and updating of the Kingdom's regulations and laws is recommended to take into account the constantly evolving legal challenges and situations presented by the globally interconnected internet.

Risk Management and Assessment

This strategy recommends a national framework of information security risk assessment processes and management tools to enable comparison of assessments using the same basic criteria. Managing risk is essential, as there is no longer an absolute defense against adverse events and attacks affecting information and ICT systems.

National ICT Infrastructure

This strategy recommends updating and hardening the ICT infrastructure of the Kingdom to a state of acceptable resilience. Doing so requires evolutionary security architecture and is a longer-term but vital element of the NISS.

Human Resource

The Kingdom has long recognized and supported extensive vocational, educational and professional development of Saudi citizens. The NISS extends this recognition with a specific focus on the areas of IT, ICT and ICT security. A key recommendation in this section is to identify work-ready Saudis (Male/Female) with computer skills and employ them in the near future to improve the information security of the Kingdom.

Re-assessment and Audit

The recommendation is to develop a comprehensive national assessment, re-assessment and audit framework, based upon best international practices. An Information Security Assessment is a formal, systematic process of data gathering, regarding information security measures that are in place, compared to an established set of criteria (ISO 27001), in order to determine what needs exist.

The audit portion of the framework is a review of an organization's IT systems management operation and technical controls, and the related processes, from a security viewpoint. The ultimate goal of an Information Security Audit is to assist management in understanding the relationship between the technical controls and the risks to the organization that they affect. The Information Security Audit also results in the determination of regulatory compliance, in the wake of legislation (such as the KSA privacy and crime laws) that specifies how organizations must deal with information security.

National and International Cooperation

The NISS recommends expanding internal cooperation and communication processes regarding information system attacks, threats, vulnerabilities, mitigation techniques and best practices between the Kingdom's organizations. Increased national coordination is required at all levels of the government, as well as between the government and private industry and the people. The NISS outlines several methods to enhance information sharing at the national level to include creating a centralized operations center for the collection and analysis of new ICT threats, information loss, theft and penetrations, and attempted theft and penetrations of ICT systems. The operations center should be connected to existing technical capabilities dispersed throughout the government and private industry.

There are additional benefits in having official Saudi representation in various international organizations involved with information security and cybersecurity. Topics that would benefit the Kingdom include international standards development, global ICT security policy, cybercrime initiatives and research. In addition, international strategic engagements and partnerships can strengthen the Kingdoms ICT and cyber defenses through collaboration and information sharing on emerging threats and vulnerabilities and appropriate mitigation technologies.

Research and Innovation

Research and innovation take longer to bear fruit, but the NISS has identified some initial projects, which are valuable and designed to expand the capability and success rate of researchers, innovators and entrepreneurs. These include encouragement and support through special workshops and a virtual support staff for translating ideas and research into patents. In addition, national coordination of the Kingdom’s important information security needs, and the success of designs that meet those needs, will help build a more active and relevant Saudi capability to meet the current and future needs.

Cybersecurity and Critical Infrastructure Protection

The NISS is a strategy that stands on its own. However, the Kingdom needs two (2) additional complimentary key strategies – Cybersecurity and Critical Infrastructure Protection. While all three (3) strategies have elements in common and the NISS has elements unique to each, implementation of the NISS still leaves some of the critical elements of Cybersecurity and Critical Infrastructure Protection unaddressed. Therefore, additional Kingdom strategies for Cybersecurity and Critical Infrastructure Protection must be developed and implemented in coordination with the NISS, to cover the areas the NISS does not cover. Collectively, these strategies provide the comprehensive and integrated efforts for national infrastructures required to support the Kingdom’s ICT objectives, which in turn support the Kingdom's national security and economic security objectives.

Conclusion

Upon successful implementation of the NISS, the supporting ICT security foundation should be in place to support the achievement of the Kingdom's Long Term Vision in 2024

2.0 INTRODUCTION

2.1 THE NISS PROJECT

The need for a National Information Security Strategy (NISS) is dictated by the complexity of today's interconnected computer networks. This NISS for the Kingdom of Saudi Arabia (KSA/Kingdom) is in response to a Request for Proposal (RFP) issued by the Ministry of Communications and Information Technology (MCIT), dated Muharram 1432H, January 2011.

The NISS Scope [1] includes the following components:

1) The NISS should address the security of all information in all areas of people's activities, and should enable information to be used and shared freely and securely.
2) "People's activities" includes public, private and individuals. NISS is a national strategy covering all aspects of information security as it is used and practiced in the government sector, the private sector and by individuals.
3) The strategy deals with national information security at the national level that applies to all sectors.

This strategy was researched, developed and produced by a highly experienced group of international senior consultant teamed with national consultants. Each of the consultants has personal experience in either drafting national information security strategies, implementing national security strategies or both.

[1] Request for Proposals (RFP) for Developing a National Information Security Strategy, Kingdom of Saudi Arabia, Ministry of Communications and Information Technology, Muharram 1432, January 2011.

2.2 NISS VISION

The Saudi Arabian information society will have a secure, resilient foundation whose information security is supported by world-class practices and highly qualified Saudi practitioners.

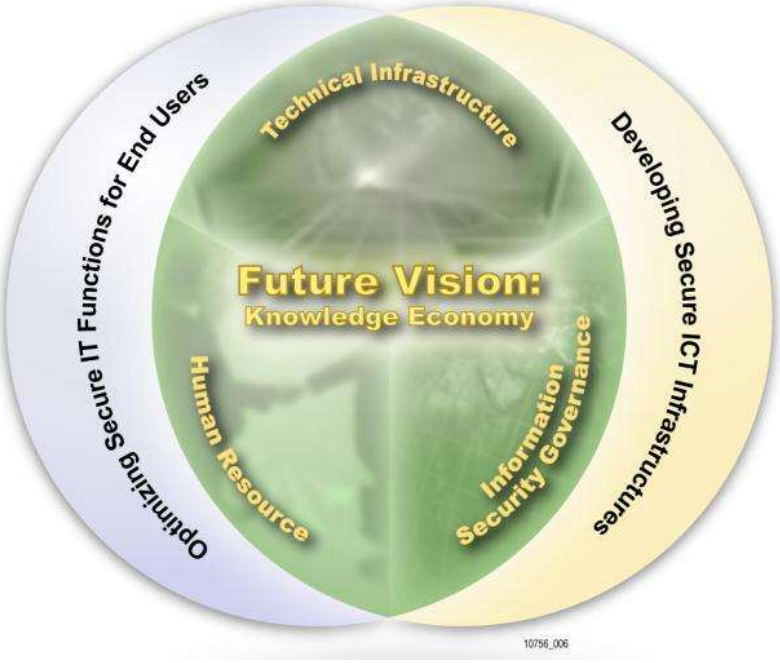

Figure 2.2-1 Achieving the Kingdom's Future Vision
The NISS vision supports the IS goals of the Kingdom's future vision.

The NISS vision includes the following successes:

1) A secure, reliable and resilient national ICT infrastructure
2) A highly capable human information security resource
3) A national information security environment and management structure built upon trust, confidence, transparency and cooperation
4) A secure and dependable set of e-government services and supporting infrastructure throughout the Kingdom that meet the security objectives of the Kingdom's ICT plans and strategies
5) A flourishing and continuing IS economic sector of research, innovation and entrepreneurial activities

2.3 NISS MISSION

The NISS is the means to advance the security and resilience of the Kingdom's ICT elements, as well as advance the capability of the Saudi Human Resource needed to accomplish the national ICT goals.

The Mission of the NISS is to produce the following:

- An effective and secure national Information Security environment
- A highly effective, skilled and increasingly Saudi human resource
- A secure and resilient national ICT infrastructure that supports the national plans
- A harmonized national framework of policy, regulations, standards and processes
- A culture of national and international IS cooperation and information sharing
- A national framework for IS risk assessment and management
- A national framework for system assessment and audit
- National IS support for IS elements and activities within the Kingdom
- Recognition throughout the Kingdom that IS is the shared responsibility of all persons
- Confidence throughout the Kingdom that online and e-government services are reliable and secure
- Expanded IS research and innovation focused on specific needs
- A growing entrepreneurial IS sector focused on high-potential commercial projects

2.4 APPROACH TO THE NISS

The initial task in creating the NISS was to research existing international information security strategies, approaches and guidelines and best practices for what would be the best approach for the Kingdom. This task also included determining the current state of information security activities and challenges faced by government agencies. The Kingdom's major national plans and strategies were reviewed and the objectives relevant to each NISS Element were identified.

The status of the Kingdom's information security was determined through intensive efforts with strong support by Ministry of Communications and Information Technology (MCIT) in the form of documents about the Kingdom's information security activities. Input from the NISS organizational and national data collection efforts from the recent data call by the minister of MCIT have been considered. The Arabic Survey sent out with the minister's letter and the online multiple choice NISS survey results have been reviewed.

The consultants used their experience and various evaluation criteria to determine the best analytical approaches for developing each NISS Element. Next, top level NISS general objectives for the Kingdom were developed and made consistent with the Kingdom's objectives contained in national plans and strategies. Specific objectives were developed for each NISS Element. Strategies to achieve each NISS Element objective were then developed and supported by a set of Implementation Initiatives.

The relationship between the NISS General Objectives and the NISS Element Objectives is illustrated in section ***3.0 NISS General Objectives***, *Figure 3.0-2 Relationship of Each NISS General Objective to the Objectives of Each NISS Element*.

2.5 Summary of Findings of KSA's Current Information Security Posture and Activities

- A set of centralized information security policies and standards is not evident.
- Each organization has implemented ICT security in their own manner with little or no consistency of architecture, policy or communication across organizations.
- The national architectural standards and requirements that Yesser has developed for connection to the Government System Backbone are an exception, but only extend to the organization's connection point and not inside the enterprise ICT infrastructure.
- IS risk assessment and management is not under a common national framework, so results from various ministries and organizations cannot be compared on the same scale for senior management decisions.
- A large unmet need exists for qualified IT, ICT, ICT security and cybersecurity practitioners.
- International approaches of countries such as Singapore, UAE, Malaysia, Tunisia, UK, Finland, and the U.S. show that a centrally-managed Information Security is the best approach to deal with the threats and vulnerabilities of today's distributed and boundless networks, because a ministry-by-ministry approach no longer provides effective security. A major obstacle to the government recruitment of skilled IT and ICT security persons is a compensation scale reported to be less of the private sector.
- There is no evidence of strong information security for the Kingdom's infrastructure elements that depend upon SCADA [1] based control systems, implying they could be highly vulnerable and represent a major risk to the Kingdom's critical ICT infrastructure.
- Limited emphasis on the importance of the translation of business/mission requirements to an ICT architecture, or the implementation of specified resilience requirements [2], was identified. Improved planning guidelines for Facilities Based Providers were identified; however, no equivalent guidelines for disaster recovery planning for ministry ICT and information systems were identified.

[1] SCADA systems security are usually considered under Critical Information Protection activities however, information security activities such as cryptographic key management and security patch installation fall under the NISS scope.

[2] Resilience is usually considered under Critical Information Protection activities; however, it was an objective in MCIT's NISS RFP and an important factor in creating confidence in the general public regarding the availability and reliability of the growing number of the Kingdom's e-government services.

3.0 NISS General Objectives

The set of NISS General Objectives are the guideposts for the Kingdom's on-going and future information security efforts. They were established to enable the Kingdom's information security foundation and posture to improve in a coordinated and effective manner and support national ICT goals and objectives.

The NISS General Objectives provide the national level scope necessary to cover the security requirements of the Kingdom's interconnected ICT infrastructure. This borderless infrastructure enables remote attacks and penetrations that can seek the weakest entry point from anywhere in the world.

The NISS is structured so the NISS General Objectives should be achieved by implementation of the set of NISS Elements. Each NISS Element has its own set of detailed objectives that should be achieved by applying a set of supporting Implementation Initiatives. Therefore, the NISS General Objectives would be achieved upon implementation of the Initiatives of the NISS Elements. The proposed five-year summary plan of the implementation sequence is in section ***5.1 Recommendations***, *Figure 5.1-2*.

Process and Principles for Generating the NISS General Objectives

The NISS General Objectives were generated using the various objectives in the Kingdom's national plans related to information and information security, as well as MCIT's objectives for the NISS. The objectives of each NISS Element were independently established and reviewed. The NISS General Objectives and the NISS Element Objectives were then modified to ensure both sets were compatible. A detailed flow chart of this process is included in the ***NISS Supplement***. References to the Kingdom's top ARE and ICT objectives used in this process are identified in the box below.

Long Term Strategy 2024 [1]
Vision "By the will of Allah, the Saudi economy in 2024 will be a more diversified, prosperous, private-sector driven economy, providing Rewarding job opportunities, quality education, excellent health care and necessary skills to ensure the well-being of all citizens while safeguarding Islamic values and the Kingdom's cultural heritage."

National Science Technology and Innovation Plan (1426)
Fourth Strategic Principle: 2. Directing scientific research and technological development towards securing the strategic requirements of defense and national security[2]
Tenth Strategic Principle: 5. Adopting the mechanisms required for the information security and protection[3]

National Communication and Information Technology Plan (1428) 2007 [4]
Long Term Vision Specific Objective (8): Raise the Security Level of ICT Networks and Protecting Privacy

Ninth Development Plan (1431/32 - 1435/36) 2010-2014 [5]
Future Vision (24.1.5.1) Objectives (24.1.5.2)

- Providing ICT services infrastructure of high quality, security and reliability, at reasonable prices, in all regions and to all segments of society
- Ensuring and safeguarding security of information of ICT services users
- Building a national ICT industry that will meet the demand for goods and services effectively

[1] Quoted in the Ninth Development Plan, Long Term Strategy for the Saudi Economy, Sec 3.4.2 Future Vision of the Saudi Economy, Page 52.

[2] National Science, Technology and Innovation Policy, Transforming Saudi Arabia into a Knowledge-Based Economy and Society, 2005-2025 , King Abdulaziz City for Science and Technology and Ministry of Economy and Planning, page 10 also at **http://www.kacst.edu.sa/en/about/stnp/pages/strategicbases.aspx**.

[3] Reference [2] above, Page 15.

[4] The National Communications and Information Technology Plan, The Vision Towards the Information Society, 1426H, unofficial Translation of the Arabic text, Page 40.

[5] Ninth Development Plan (1431/32 - 1435/36) 2010-2014, Ministry of Economy and Planning, Chapter 24, Page 479.

NISS General Objectives

The ten (10) NISS General Objectives are like the needle on a compass. They should help guide the Kingdom in its on-going IS efforts to develop and maintain the comprehensive foundation required to meet its long-term information and ICT goals. The NISS General Objectives were established to enable the Kingdom's IS foundation and posture to improve in a coordinated and effective manner, while also supporting national ICT goals and objectives. The NISS General Objectives were generated using the NISS objectives set by the MCIT, as well as various objectives in the Kingdom's national plans that are related to information and information security.

The NISS General Objectives are listed in the table in *Figure 3.0-1* below. The table is followed by a summary description of each objective.

NISS General Objectives
O-1 – Effective and Secure Information Security Environment Work towards assuring that appropriate and consistent information security policies, directives, guidance, practices and oversight are achieved within the Kingdom.
O-2 – Information Systems and ICT Infrastructure Enhancement Enhance the security, reliability, availability and resilience of the Kingdom's ICT infrastructure and information systems.
O-3 – Human Resource Improve the IS human resource and expand the capability of Saudi information security practitioners, researchers, innovators and entrepreneurs, both men and women; and establish special programs for training and awareness especially directed towards youth of all ages and gender.
O-4 – IS Threat Analysis and Mitigation Establish an IS function and analysis capability to collect and analyze vulnerabilities, all-source threats and risks to the Kingdom's ICT resources.
O-5 – Reduction of On-going ICT Exploitation Reduce and prevent exploitation of weak points in the Kingdom's information security (IS) by employing the best international mitigation practices in local and national areas of highest IS risk.
O-6 – IS Compliance and Tracking Processes Maximize progress toward national improvement benchmarks and goals by implementing a comprehensive compliance and tracking process, which ensures compliance with IS policies and standards and measures the progress and status of the Kingdom's information security initiatives.
O-7 – Research, Innovation and Entrepreneurship Meet future IS needs by stimulating and directing the Kingdom's IS research and innovation programs that have high potential for commercialization and IS breakthroughs, including cryptographic interoperability, supply chain integrity, computer security and rapid and effective access control.
O-8 – Maintenance of Information Security Ensure adequate IS protection for the Kingdom by maintaining a continuous process that supports the IS defensive posture for essential ICT infrastructures and information systems, and addresses new IS threats and vulnerabilities.
O-9 – National and International Cooperation Achieve greater security for the Kingdom's information and ICT infrastructures by implementing new domestic ICT security coordination and information sharing processes among stakeholders and by leveraging international collaboration efforts.
O-10 – Information Security Awareness and Responsibilities Increase in all people their awareness of IS threats and vulnerabilities, as well as their understanding of personal responsibilities to improve information security in their work environments and daily lives.

Figure 3.0-1 NISS General Objectives
The NISS General Objectives were established to support national ICT goals and objectives.

O-1 – Effective and Secure Information Security Environment

This objective is based upon the need to develop a national information security environment that forms the foundation, and sets the direction, of IS activities. It is accomplished through the operational compliance of a national risk assessment framework, policy coordination, communication, monitoring and all of the factors and functions necessary to efficiently achieve and maintain an effective IS posture for all Kingdom's sector.

O-2 – Information Systems and ICT Infrastructure Enhancement

This objective envisions an evolutionary process that ensures the technology, scalable architecture and operational practices implemented are appropriate and align with the Kingdom's business/mission objectives and the requirements of the infrastructure. It will provide appropriate assurance of effective and secure disaster recovery and resilience. This includes confidence that critical e-government and business functions can continue secure operation under degradation of assets, and that the information and processing systems will recover quickly to an appropriately secure steady state.

O-3 – Human Resource

This is a key pillar of the NISS. It represents a broad set of individual objectives involving theoretical and practical IS education and training, as well as on-the-job experience with substantive evaluation of each individual's true skills and capability for growth. It has components for practitioners, managers, researchers and entrepreneurs. Special programs identify work-ready women who are capable in IT and IS and who, with focused training, can meet some of the Kingdom's immediate IS needs.

In addition, ethical unemployed youth, who have no formal credentials but have strong computer skills and hacking capabilities, can be vetted and employed – first in controlled situations, while they prove themselves.

Finally, a comprehensive program beginning in primary school identifies and encourages bright and interested children to acquire computer, analytic and IS skills. These individuals would be mentored and observed throughout their schooling and into initial employment.

O-4 – IS Threat Analysis and Mitigation

The Kingdom needs to address IS threats and exploitation attempts at the national level. This objective establishes such a capability via a national Security Operations Center (SOC), which would collect and disseminate threat and intelligence information, analyze attacks, recommend mitigation actions and coordinate a national response. The SOC would work with existing centers and capabilities to facilitate national information sharing and coordinate mitigation and incident response actions. An important element in the analysis process is the National Risk Assessment Function (NRAF). This function will establish and help implement a national Risk Process Management System that provides a common risk framework for the Kingdom.

O-5 – Reduction of On-going ICT Exploitation

The NISS establishes the SOC as a resource to assist decision makers in understanding the impacts of ICT exploitation and deciding how best to address and reduce IS risks. After an analysis of IS all-source threat and vulnerability data is provided to them via the SOC, decision makers will also be supplied with the NRAF's risk analyses and can adopt the best of international mitigation practices when faced with either a specific incident or a basic IS status review.

O-6 – IS Compliance and Tracking Processes

An effective and secure Information Security Environment requires a measurement and compliance capability to ensure progress and to identify challenges during implementation of the Kingdom's focused and coordinated IS programs. A continuous compliance process guides and enforces standards, baselines and best practices. It also ensures a uniform application of security policy across a diverse set of both governmental and critical infrastructure organizations. The project measurement and tracking component highlights the progress, or lack thereof, of the various NISS implementation initiatives.

O-7 – Research, Innovation and Entrepreneurship

This objective supports the identification and coordination of the Kingdom's future IS needs. It contains increased education and training in patenting and innovation for researchers, as well as the important areas of guiding young researchers to bridge the gap to commercialization and mentoring beginning entrepreneurs.

O-8 – Maintenance of Information Security

Information security is never an end state. It is always a continuous process because of constantly evolving threats. Effective ICT resilience and business continuity result primarily from implementation of an appropriate architecture. Achieving an adequate state of IS and maintaining that state with ever-changing technology and network configurations is a different challenge. In addition, these changes create new vulnerabilities, while adversaries work to invent new attacks. Addressing both situations demands agile and continuous attention by IS professionals.

O-9 – National and International Cooperation

Many nations have faced IS challenges similar to those the Kingdom is facing today. Several international forums provide useful IS cooperation and information sharing opportunities to address these challenges. Within the Kingdom, as in other countries, information sharing can be a major obstacle, as organizations jealously guard their territory and have limited dialogue with their neighbors. The interconnectivity of today's networked ICT environment, unlike standalone mainframes of the past, causes one organization's IS to be dependent upon the actions and security of others. The equation is simple. As the in-country cooperation, collaboration and information sharing increases, the risk of information loss and ICT systems exploitation decreases.

O-10 – Information Security Awareness and Responsibilities

All subjects, in every position in the Kingdom, need to be appropriately aware of the IS threats, vulnerabilities and risks that can affect their personal lives, as well as negatively impact business and government operations. Today's networks have no boundaries, so worldwide interconnectivity and social networks can be used to cause serious damage. Public awareness of the risks, the threat indicators (and what to do about them) and the basic IS responsibilities of each individual can result in a much stronger defense.

Relationship of the NISS General Objectives to the NISS Element Objectives

Figure 3.0-2 below demonstrates the relationship of the ten (10) NISS General Objectives listed above to the objectives of the nine (9) elements of the NISS. Each column contains links to the sets of NISS Element Objectives that support the NISS General Objective listed at the top of the column. Following the table is a list of the NISS Element Objectives.

Cross Reference Chart of Each NISS General Objective to the Objectives of Each NISS Element										
NISS General Objectives / NISS Elements	O-1 Effective and secure Information Security Environment	O-2 Information Systems and ICT Infrastructure Enhancement	O-3 Human Resource	O-4 IS Threat Analysis and Mitigation	O-5 Reduction of Ongoing ICT Exploitation	O-6 IS Compliance and Tracking Processes	O-7 Research, Innovation and Entrepreneurship	O-8 Maintenance of Information Security	O-9 National and International Cooperation	O-10 IS Awareness and Responsibilities
Information Security Environment	G-1 G-2	G-5	G-4 G-5	G-1	G-5	G-2 G-3	G-1	G-3		G-5
Policy and Regulation	P-1 P-2	P-1				P-1 P-2 P-3		P-2 P-3		
Risk Management and Assessment	K-1	K-2	K-1 K-3	K-1	K-3	K-3		K-2		
National ICT Infrastructure		T-1 T-2 T-3		T-2	T-2	T-2		T-2		
Human Resource	H-1	H-1 H-3	H-1 H-2 H-3 H-5	H-4 H-5	H-1 H-3 H-4 H-5	H-1	H-1	H-5	H-1 H-2 H-3 H-4 H-5	H-1 H-2 H-3 H-4 H-5
Reassessment and Audit	A-1	A-1 A-2 A-3			A-3	A-1 A-2 A-3		A-1 A-2 A-3		
National Cooperation		N-1 N-2 N-3		N-2	N-2	N-1 N-3	N-2		N-1 N-2 N-3	N-1 N-2 N-3
International Cooperation		I-1			I-2	I-1	I-3	I-3	I-1 I-2 I-3	I-2
Research and Innovation			R-3 R-5			R-4	R-1 R-2 R-5	R-1 R-5		

Figure 3.0-2 Relationship of Each NISS General Objective to the Objectives of Each NISS Element
The objectives of each NISS Element support one or more of the NISS General Objectives.

NISS Element Objectives	
G-1	Work towards having a secure and effective National Information Security Environment (NISE), incorporating all IS stakeholders in the Kingdom.
G-2	Establish a policy and requirements structure for the issuance of top-level IS national directives.
G-3	Ensure that the NISE has the ability to monitor and enforce compliance with national policies, directives and standards.
G-4	Oversee, support and recommend programs for the development of the required set of IS and cybersecurity people to meet the Kingdom's short and long-term human resource (HR) needs.
G-5	Provide expanded IS awareness, guidance, coordination and technical assistance to various entities of the Kingdom, including appropriate elements of the private sector.
P-1	Ensure that the owners and operators of KSA's infrastructures have designed, implemented, manage and operate ICT infrastructures with appropriate information security and resilience practices for their systems and operations.
P-2	Ensure appropriate coverage of information security by current regulatory elements, as well as the capability to cover requirements for future technological developments, by establishing a process for overall review and possible modification, augmentation or creation of the Kingdom's laws, regulations and acts.
P-3	Ensure all regulations and laws have accompanying policies, and vice versa, by establishing a policy gap analysis process.
K-1	Create and establish a National IS Risk Assessment Function (NRAF) under the National Information Security Environment (NISE)
K-2	Develop and implement national Risk Process Management System (RPMS) that establishes information security environment and compliance through national policies, procedures and guidelines.
K-3	Conduct a macro IS risk assessment to establish a risk baseline for the Kingdom's major ICT systems.
T-1	Ensure that the owners and operators of KSA's critical infrastructures evolve their ICT architecture, and implement, manage and operate ICT infrastructures with appropriate information security and resilience practices for their systems and operations.
T-2	Establish a KSA common evaluation process that permits owners and operators of ICT infrastructures and information systems to uniformly identify an appropriate risk tier level that reflects their ICT infrastructure and system information security and resilience requirements.
T-3	Institutionalize a cross-ministry effort that goes beyond e-Government systems to evaluate and assure that each ministry has well-defined processes to address documented security and resilience requirements for their ICT infrastructure and systems.
H-1	Increase the availability and number of educated, trained and skilled Saudi Information Communications and Technology Security (ICTS) professionals and managers to fill current and future key ICTS positions.
H-2	Develop a program to improve the quality and availability of IS education at all levels to produce the comprehensive Human Resource needed in the various fields of information security.
H-3	Develop a program to increase the number of skilled IS professionals who have hands-on training in simulated or real world conditions.
H-4	Develop and maintain awareness of the threats and defenses involving online applications.
H-5	Develop approaches to foster IS responsibility among all sectors of the Kingdom, with emphasis on the importance of the individual's role.

NISS Element Objectives	
A-1	Provide a Kingdom-wide harmonized ICT methodology for a system assessment, re-assessment and audit process that is customized to the Kingdom's environment. The process should be based on the principles of international standards such as ISO 27001 and 27002, as well as generally accepted best practices, guidelines, procedures and policies.
A-2	Develop a minimum baseline IT security standard for internationally accepted security configurations. This provides the standard that trained information security professionals can use to produce and conduct assessments, audits and certifications, as well as accreditation of existing and new systems.
A-3	Establish an assessment and audit framework to ensure the security and confidentiality of system records and information, to protect against any anticipated threats or hazards to the security or integrity of such records and to protect against unauthorized access to or use of such records or information.
N-1	Enhance information sharing capabilities of the following principal interfaces: Ministry-to-Ministry, Government-Private Partnerships and Government-to-Public.
N-2	Enhance the following information sharing areas that require inter-governmental structures and processes for cooperation and coordination: ICT Security Standards and Policies, Research and Development, Security Operations Center (SOC), Vulnerability and Threat Information Sharing, National IS Incident Response Process.
N-3	Create a National Information Security and Cyber Exercise Program to enhance national coordination and cooperation of activities related to information security.
I-1	Strengthen the Kingdom's national technical capabilities through increased international cooperation and sharing.
I-2	Combat cybercrime .
I-3	Expand research and innovation through international cooperation.
R-1	Develop a national research and innovation human, technical and commercial infrastructure.
R-2	Develop an analysis and review capability for research and commercialization proposals.
R-3	Provide appropriate internal and external encouragement to all team members.
R-4	Adopt project and program planning, management and measurement tools and systems.
R-5	Develop a strong marketing capability for the products ready for production.

4.0 NISS ELEMENTS

The following NISS elements are the foundation of the NISS and are designed to achieve the NISS General Objectives described in section 3.0 above. The sequence for implementation has some flexibility, but the overall approach to implementation is described in section ***5.1 Recommendations.*** Each of the NISS elements is described in a separate section below.

Each NISS Element section contains the following sub-sections:

- Element Description
- Relationship To Kingdom's Top ICT Objectives
- Element Objectives

Each Element Objective contains the following sub-sections:

- Approach
- Implementation Initiatives
- Challenges and Issues
- Measures of Progress

4.1 INFORMATION SECURITY ENVIRONMENT

The NISS information security environment element is a national configuration of information security authorities and functional responsibilities that cover the entire scope of IS and information assurance activities.

The entire Kingdom's (and, in fact, any nation's) Information Communications Technology (ICT) infrastructure is interconnected. This can create exponentially increasing risks of successful attacks and damage, as more of the Kingdom's important functions migrate to e-government. For example, the expanding skills demonstrated in all types of IS exploitation create an increasing number of vulnerabilities to the vital sectors of petroleum, communications, electricity and water, whose control is via networks.

No matter how IS measures are employed within a single government agency, an effective defense today depends upon the coordinated actions and defenses of other entities connected via networks. This is the reason for establishing national IS structure policy, standards and guidelines. In addition, each organization must implement its own appropriate procedures and initiatives, which will be coordinated at the national level through National Information Security Environment Functions.

Detailed objectives, approaches and initiatives for this element are described below.

4.1.1 ELEMENT DESCRIPTION

The proposed information security function is best achieved through a secure and effective National Information Security Environment (NISE). The NISE has an information security functions whose responsibilities cover all areas of IS. These functions are illustrated below in *Figure 4.1-1 NISE and Functions*. The NISE also has an administrative function and a support function for the various NISE Functions. These Functions are composed of members from different government agencies. They can also include appropriate representation from the private sector. It is in the Functions where the coordination and cooperation are developed, which are necessary for effective execution of the Kingdom's IS programs, projects and actions.

The NISE line organizations provide centralized technical functions of expertise and focus for the various IS functions and capabilities. Existing activities and functions could be incorporated or closely allied with the new functions to prevent duplication of effort. Examples of new activities and functions include cryptographic design and evaluation, key management, IS risk assessments, threat

and vulnerability collection and analysis. Functions such as IS awareness and outreach should be coordinated with and supportive of ongoing efforts.

The current system of IS management must evolve into a national system where IS is the responsibility of everyone and all organizational elements, not just the IT components. Such evolution will allow the Kingdom's vital ICT areas to be managed in a collective and comprehensive manner for the benefit of all.

4.1.2 Relationship to Kingdom's Top ICT Objectives

The following two relevant objectives are identified in the KSA Ninth Development Plan in Chapter 24, Information and Communication Technology[1]:

- Providing ICT services infrastructure of high quality, security, and reliability, at reasonable prices, in all regions and to all segments of society
- Ensuring and safeguarding security of information of ICT services users

The Ministry of Communications and Information Technology (MCIT)'s objectives [2] for this NISS Element include the following:

- Transform the Kingdom of Saudi Arabia into an information-secure society, enabling information to be used and shared freely and securely.
- Increase the security, safety, and integrity of online information while promoting the increased use of information Technology.
- Develop resilience in information systems.
- Increase awareness and education of security risks and responsibility of information protection.
- Create a set of national guidelines on Information Security Management, Risk Management and Business Continuity based on international standards and best practices.

The NISE should provide the centralized technical means of coordination and cooperation for the IS activities to achieve the above objectives and provide an effective and secure foundation for the Kingdom's evolution to a knowledge economy. The NISE will also prioritize, stimulate and track implementation of the Kingdom's IS initiatives and, when necessary, recommend course corrections or alternatives. Appropriate transparency is critical, as is cooperation, coordination and collaboration among the Kingdom's IS stakeholders. The Kingdom's long-term ICT security objectives are important components in achieving the vision of a knowledge economy. The NISE is the structural foundation for achieving these ICT security objectives.

4.1.3 Element Objectives

4.1.3.1 Objective G-1: Work towards having a Secure and Effective National Information Security Environment (NISE)

Work towards having a National Information Security Environment (NISE) by incorporating all IS stakeholders in the Kingdom. Its national management structure will consist of the NISE functions. It will be based upon the best international practices of nations such as Singapore, UAE, Malaysia, Tunisia, UK, Finland, the U.S. and others. NISE shall be responsible for the detailed implementation of the NISS objectives and initiatives.

---

[1] Ninth Development Plan (Eng), Chapter 24, Section 24.1.5.2, page 479.

[2] Request for Proposals (RFP) For Developing a National Information Security Strategy, KSA Ministry of Communications and Information Technology, Muharram 1432H, January 2011 page 9.

4.1.3.1.1 Approach

The appropriate authority in the Kingdom shall decide which entities and sub-entities to establish. The specific roles for existing government agencies concerned with information security need to be determined. The approach taken in proposing the NISE Environment and Functions, illustrated in figure 4.1-1 was to identify the functions to be performed and principles to be followed, but not to attempt any assignment of these functions to existing, combined or new organizations.

4.1.3.1.2 Implementation Initiatives

1) Identify the Components of the NISE

The proposed detailed NISE is shown below in *Figure 4.1-1 NISE and Functions*. The diagram represents the functional composition and structure of a national information security environment, based on best international practices and includes all IS stakeholders in the Kingdom.

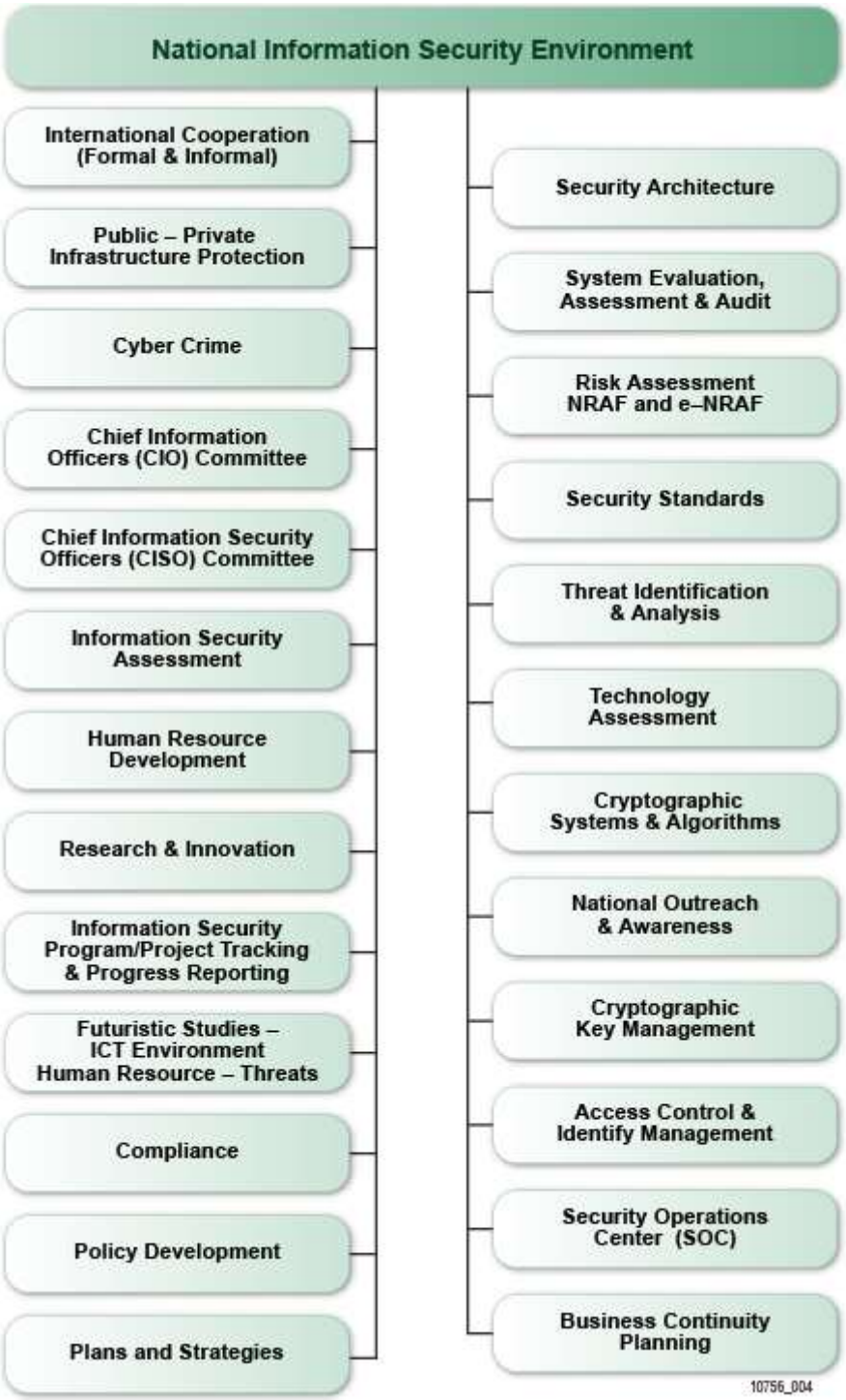

Figure 4.1-1 NISE and Functions
The proposed elements of the Kingdom's national IS management structure include the primary functions areas needed for IS.

Many countries have or are working toward a secure and effective national IS environment. Globally, countries are increasing their use of ICT infrastructure to support:

- Government operations
- Private sector economies
- Citizens' dependence on e-government services and personal use

This global trend requires improved security and resilience. A small sample of countries and their national IS environment are listed in the table in *Figure 4.1-2* below.

Sample of Countries With National IS Environment			
Country	**Top Level Charter or Latest Policy**	**Senior Organization Responsible**	**Primary Coordinating Body For Initiatives and Implementation**
Singapore	Infocomm Security Masterplan 2 (MP2)	National Infocomm Security Committee	Infocomm Development Authority
UAE	UAE National ICT Policy	National Electronic Security Authority	Board of directors, formed by a decision by the chairman of the Supreme National Security Council
Malaysia	Malaysian ICT Security Policy 2012	Ministry of Science Technology and Innovation	CyberSecurity Malaysia
Tunisia	Tunisian Law	Ministry of Communication Technologies	National Agency for Computer Security
UK	A National Information Assurance Strategy	Official Committee on Security	Information Assurance Policy and Program Board
Finland	National Information Security Strategy	National Information Security Board	Numerous Ministries and Organizations
U.S.	Homeland Security Act of 2002", Title X, Information Security	Department of Homeland Security	Office of Management & Budget Federal CIO Council National Institute of Science and Technology (NIST) US-CERT

Figure 4.1-2 Sample of Countries With National IS Environment
Many countries are working toward a national IS environment.

2) Obtain a Consensus from the Kingdom's Top Leadership

A consensus of the Kingdom's top leadership is vital to provide the support and agreement needed to effectively implement this national level IS environment. The approach suggested is based in part on the already approved elements in existing Cabinet Resolutions and include the following:

- The assessments, initiatives and planning need to be coordinated across the Kingdom under a common framework ("to achieve universality across the Kingdom")
- An independent group that provides a consistent framework and independent approach ("to achieve … an objectivity")

4.1.3.1.3 Challenges and Issues

1) Because neither a Kingdom-wide IS environment nor a national set of security policies and standards has ever been identified, each ministry has developed and operates their own security systems as they see fit. It will be a major challenge to have each government agencies agree to create the National Information Security Environment(NISE).

   The standardization and support a national environment provides will benefit both the Kingdom and each ministry, since operating in isolation no longer provides the security required. A centralized national information security environment will provide much greater support and assistance to those organizations that need it the most.

4.1.3.1.4 Measures of Progress

1) To plan and monitor the progress of each NISE related project and program, government agencies can use the appropriate elements of ISO 27001 and 27002 as management guidelines, along with a NISE management information system.

4.1.3.2 Objective G-2: Establish a National IS Policy and Directive Issuance System

Establish a policy and requirements structure for the issuance of top-level IS national directives.

4.1.3.2.1 Approach

Ensure that the charter of the NISE contains adequate authority for the issuance of national directives, instructions, manuals and any other items required to implement IS.

4.1.3.2.2 Implementation Initiative

1) Develop Requirements and Guidance

The NISE should develop the following types of requirements and guidance:

- NISE Directives (NISEDs) are "big picture" issuances to establish NISE policy, assign responsibilities and delegate authority to NISE components. NISEDs do not contain procedures.
- NISE Instructions (NISEIs) are usually signed by an NISE division or function head to establish or implement policy.
- NISE Manuals (NISEMs) implement or supplement policy established in a Directive or Instruction and usually focus on procedures or best practices for managing activities or systems.
- Administrative Instructions provide guidance on administrative matters related to implementing policy established in NISEDs or NISEIs that focus on administration of the NISE throughout a particular government agency.

4.1.3.2.3 Challenges and Issues

1) Implementing this new national environment system will take training and a knowledgeable staff to draft issuances and could require extensive coordination for implementation approvals.

4.1.3.2.4 Measures of Progress

1) A plan with milestones for drafting, approval and final issuance will be established and tracked as a key performance measure for the efforts of the NISE.

4.1.3.3 Objective G-3: Establish NISE IS Compliance Function

Ensure that the NISE has the ability to monitor and enforce compliance with national policies, directives and standards.

4.1.3.3.1 Approach

Incorporate this objective into the NISE charter.

4.1.3.3.2 Implementation Initiative

1) NISE Charter Approval

Have the NISE charter formally approved and officially established with responsibilities and deadlines.

4.1.3.3.3 Challenges and Issues

1) Utilize outside organizations to assist and monitor assessments, as well as progress on IS initiatives.
2) If status and assessments are restricted to the senior group and viewed as necessary for the Kingdom's future welfare, addressing and mitigating the areas of highest risk will be the most

effective strategy for both the Kingdom as a whole and each individual Government entity, since they are all linked.

3) Lack of progress is often due to lack of resources and not the will or capability of management to proceed faster. Such deficiencies should be identified and appropriate resource adjustments made.

4.1.3.3.4 Measures of Progress

1) Providing the NISE with accurate and timely information on the status of each organization's implementation initiatives, as well as the annual status of their IS posture, is important. If this is done in a transparent manner and is restricted to those within the national structure with a need to know, then areas of highest risk can be identified and prioritized for appropriate mitigation actions and initiatives.

4.1.3.4 Objective G-4: Establish and Expand Programs for Development of the IS Human Resource (HR)

Oversee, support and recommend programs for the development of the required set of IS and cybersecurity people to meet the Kingdom's short and long-term human resource (HR) needs.

4.1.3.4.1 Approach

Utilize both international and Kingdom experts to identify national IS needs and qualifications and initiate a program with education, training, certification and practical experience to meet the needs. At the top university level, a Kingdom IS certification program can be established with uniform and stringent certification standards for both teachers and curricula. This can be combined with foreign universities. Exchange and internship programs with national companies and friendly foreign companies and governments can be instituted. Establish a process of tracking the quality and skill level of the people entering and graduating, along with an evaluation of their operational capabilities, as opposed to paper credentials. This involves several ministries, including the Ministry of Communications and Information Technology (MCIT), National Security Council (NSC), Ministry of Higher education (MOHE), Ministry of Education (MOE), Ministry of Labor (MOL), Ministry of Interior (MOI), Ministry of Civil Service (MCS) and Ministry of Defense (MOD). The number of ministries required is the reason an oversight and advisory group is required at the national level.

4.1.3.4.2 Implementation Initiative

1) Establish and Formalize HR Requirements and the Measurements and Tracking System

Establish the IS HR requirements and the measurement and tracking system within NISE and make them available for all government agencies.

4.1.3.4.3 Challenges and Issues

1) The challenge of identifying the true state of capability of the HR has always existed and is important to address. Support and mentoring should be provided to people who lack the required training and skills, yet have the desire to succeed and advance in the field of IS. Experienced and qualified people should be enlisted to assist in this role.

4.1.3.4.4 Measures of Progress

1) The number of qualified IS professionals in place, along with what should be a growing number and percentage of Saudis in these positions, is the key performance indicator.

4.1.3.5 Objective G-5: Establish NISE Outreach and Awareness Function and All Remaining Functions

Provide expanded IS awareness, guidance, coordination and technical assistance to various entities of the Kingdom, including appropriate elements of the private sector.

4.1.3.5.1 Approach

Require the NISE to be the lead organization responsible for this effort. Leverage this function by coordinating, collaborating with and enlisting other people or organizations within and outside the Kingdom. Coordinate and expand the ongoing outreach and educational and awareness efforts – for example. MCIT's Caravans, and CERT-SA. In addition, the ongoing efforts within each government agencies should be encouraged, supported and coordinated with the efforts of other entities to create and maintain synergy.

4.1.3.5.2 Implementation Initiative

1) Establish NISE Functions

Establish each of the NISE functions. For example, establish the National Outreach and Awareness function within the NISE. This function should have both direct responsibility and the ability to coordinate, collaborate and enlist other organizations in the Kingdom. Their charter covers the IS in all sectors.

4.1.3.5.3 Challenges and Issues

1) Establishing the NISE will require a set of high-level and skilled IS practitioners. During the initial implementation phases, HR may need to be augmented with international consultants and non-Saudi practitioners.

4.1.3.5.4 Measures of Progress

1) The number of people involved in national IS outreach and support
2) The number of people reached by the individuals in measure #1 above

4.2 POLICY AND REGULATION

The Policy and Regulation strategy element will help the MCIT develop and set the framework for meeting the objectives of the National Communications and Information Technology Plan. This framework will define goals for national standards that reflect International Standards Organization (ISO), Information Technology Infrastructure Library (ITIL) and industry best practices.

Policy development, regulation and compliance are vital aspects of any National Information Technology framework. The development, issuance and maintenance of regulatory requirements by the government help to ensure that standards are met which, in turn, support the safety, productivity and economic development of the country.

The Anti-Cyber Crime Law (8 Rabi1, 1428 / 26 March 2007) provides a good base for prosecuting those that attack, steal or damage a network or computer. However, this law does not cover prevention, education and collaboration. The Electronic Transactions Law provides a good basis for controlling, regulating and providing a legal framework for electronic transactions and signatures, but is not as comprehensive as a full strategy. These laws were reviewed, along with the Telecom Act (1422 / 03 June 2001) as the foundation for the NISS.

NISS development approach included the review and gap analysis of existing policies and regulations. We mapped any gaps that were noted to ISO, ITIL and other industry best practices and developed our element objectives and recommendations based on that mapping. The table in *Figure 4.2-1* below lists at a national level selected regulations, policies, standards and procedures that are required by an organization to comply with International Standards Organization (ISO) 27001, 27002. The ISO series of security standards provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System. The following high-level gap analysis is based, in part, upon a review of KSA laws, regulations, policies and procedures provided to the NISS team. It can be useful in developing a framework for defining the goals of a KSA national standard that adheres to International Standards Organization (ISO) 27001, 27002; Information Technology Infrastructure Library (ITIL); and industry best practices.

High-level Gap Analysis of National Level Policies, Laws and Regulations

Compliance Requirement	National-Level Considerations	Corresponding KSA Law or Regulation	Suggested Action
Risk Management Framework (RMF)	A national framework that incorporates both quantitative and qualitative considerations for risk	• The National Communications and Information Technology Plan • The Vision Towards the Information Society • National Science, Technology and Innovation Policy Transforming Saudi Arabia into a Knowledge Based Economy and Society	The current policy, plan and vision should be consolidated to address a national level RMF that all industries, as well as government agencies, can set as their minimum requirements.

High-level Gap Analysis of National Level Policies, Laws and Regulations			
Compliance Requirement	**National-Level Considerations**	**Corresponding KSA Law or Regulation**	**Suggested Action**
Information Classification of Data	Information labeling and handling standards across military, intelligence and critical infrastructure, which facilitates information sharing among peers in ministries	• Cabinet Resolution No 141	The current resolution can be better articulated to provide guidance, as well as define various classifications of KSA data.
Information Security Policy	National level policy that enables the use of common criteria and supports standards such as ISO, COBIT, and ITIL	• None provided. If no such policy exists, then it should be created.	A national level regulation on Information Security should be developed. It will be used as the minimum requirement for all KSA systems.
Roles and Responsibilities	Defines "lanes in the road" for governmental organizations	• Cabinet Resolution No 194	Update resolution to reflect new roles and responsibilities as they pertain directly to Information Assurance and Cybersecurity.
Awareness, Education, and Training	National standard for assessments, to identify where security knowledge is insufficient and to provide adequate training	• None provided. If no such training exists, then it should be created.	A national level public awareness campaign should be developed to address the importance of Information Assurance and Cybersecurity within KSA.
Physical and Environmental Security	National level baseline security requirements upon which minimums for physical and environmental security are built	• Cabinet Resolution No. 82	Implement the recommendations that are outlined in Cabinet Resolution No. 82.
Information Exchange Policies and Procedures	Important in order to exchange information and approach a common understanding between Nations. (e.g. League of Arab States, and United Nations)	• None provided. If no such policies and procedures exist, then they should be created.	KSA regulation on information exchange needs to be defined.
Electronic Commerce	Standardization and interoperability for technologies and process	• Electronics Transactions Law	The law has not been updated in over 5 years. It should be updated to reflect current technologies and business practices.
On-line Transactions	Minimum protection	• Electronics Transactions Law	The law has not been updated in over 5 years. It should be updated to reflect current technologies and business practices.
Monitoring System Use	Balancing privacy, intelligence, law enforcement, and operational equities at a national level	• None provided. If no such law exists, then it should be created.	Law on the parameters and regulations of monitoring system use needs to be developed.

High-level Gap Analysis of National Level Policies, Laws and Regulations			
Compliance Requirement	**National-Level Considerations**	**Corresponding KSA Law or Regulation**	**Suggested Action**
Information Security Incident Management	A methodology for information security management that is intended as a common basis and practical guideline for developing organizational security standards and effective management practices	• None provided. If no such documentation exists, then it should be created.	National KSA CERT program needs to be better defined and disseminated for all KSA agencies to utilize as a centralized databank for incident management.
Compliance With Legal Requirements	Information from international and regional organizations on their efforts to promote peace and security in cyberspace are important in order to exchange information and approach a common understanding. (i.e. League of Arab States, and United Nations)	• None provided. If no such framework exists, then it should be created.	National Framework on information security environment, Risk, and Compliance needs to be developed.
Data Protection and Privacy Of Personal Information	National level minimum data protection standards	• Protection of Personal Data Law	Develop a national guideline for a risk-based approach to protecting the confidentiality of PII. Define what is considered PII within KSA, i.e. Name, passport number, national identity number, photos, etc.
Compliance With Security Policies and Standards, and Technical Compliance	Compliance must come with enforcement; and penalty guidelines for offenders could aid ministries to develop penalties that are more meaningful for offenders.	• None provided. If no such framework exists, then it should be created.	National Framework on information security environment, Risk, and Compliance needs to be developed.
Continuous Monitoring	National level dashboard to “roll-up” consolidated reporting	• None provided. If no such regulation exists, then it should be created.	KSA regulation for continuous monitoring needs to be defined.
Audit And Accountability Policy and Procedures	Configure systems to record more detailed information about system access	• None provided. If no such policies and procedures exist, then they should be created.	KSA regulation for audit logs and non-repudiation needs to be defined.
Record Retention Laws	Minimum retention timeframes for logs and other records (e.g. E-mails)	• None provided. If no such laws or regulations exist, then they should be created.	KSA regulation for records retention needs to be defined.

High-level Gap Analysis of National Level Policies, Laws and Regulations			
Compliance Requirement	**National-Level Considerations**	**Corresponding KSA Law or Regulation**	**Suggested Action**
Contingency Planning Policy and Procedures	Nationalizing of "cyber" resources during times of cyber war, conflict and natural disaster	• Regulatory Framework for Disaster Recovery Planning for the ICT Industry	Define and identify the policies & procedures that need to be executed during a cyber-event. Ensure all personnel that have a need to know, are on the distribution list for these procedures.
Incident Response Policy and Procedures	Baseline incident response procedures involving national level reporting (e.g. National Level Incident Reporting Database)	• Cabinet Circulate 16-5-1432	Define and disseminate incident reporting of cyber-events to a National level database. Ensure data is shared throughout KSA agencies to prevent attack, or reduce impact of an attack.
The Arab League Convention To Combat Cyber Crimes	Adherence to and participation in the International Cyber Crimes Convention	• Anti-Cyber Crime Law	Ensure cyber-crime laws are consistent with international standards, and that cooperative agreements are in place with other Nations to ensure cyber criminals are captured and brought to justice.

Figure 4.2-1 High-level Gap Analysis of National Level Policies, Laws and Regulations
A gap analysis can be useful in developing a framework for defining the goals of a KSA national IS standard that adhere to international standards and best practices.

4.2.1 ELEMENT DESCRIPTION

Well-written policies and procedures allow individuals and employees, as well as agencies and other organizations within the Kingdom, to understand their roles and responsibilities within predefined limits. Essentially, policies and procedures allow management to guide operations without constant management intervention.

Government development and issuance of regulatory requirements help to ensure that standards are met, which leads to greater safety, productivity and economic development. Information systems and networks, as well as the information they contain, are essential assets of a nation and must be appropriately protected and regulated.

A framework for such regulation includes policies, procedures and the ability to assess regulatory compliance. The critical components of policy and regulation framework are outlined below as part of the strategic roadmap for the KSA Policy and Regulation initiatives.

4.2.2 RELATIONSHIP TO KINGDOM'S TOP ICT OBJECTIVES

The Kingdom has identified several initiatives that address the need to combat cybersecurity crime, establish enhancements and promote awareness. While the establishment of policy and regulation governance will provide the Kingdom with the ability to assess regulatory compliance, it is also crucial to the success of all strategies implemented.

4.2.3 ELEMENT OBJECTIVES

4.2.3.1 Objective P-1: National Policy Framework

Ensure that the owners and operators of KSA's infrastructures have designed and implemented, as well as manage and operate, ICT infrastructures with appropriate information security and resilience practices for their systems and operations.

4.2.3.1.1 Approach

Ensure that all Kingdom policies and regulations are tailored to suit the unique organizational and operating circumstances found within the national environment and at the ministerial level.

4.2.3.1.2 Implementation Initiative

1) Define and Design a National Policy Framework

Establish a Policy Development Function under the NISE with cooperation from all Kingdom IS stakeholders.

Having a framework provides the foundation to allow all subsequent policy writing tasks to be more efficient and focused.

4.2.3.1.3 Challenges and Issues

Because of the sensitive nature of information within each ministry, development of a trusting environment to share specific information about vulnerabilities, incidents and practices will require strong collaboration. The following issues must be addressed with that spirit of cooperation:

1) Establishment and definition of the ways in which ministries intend to express information security policies
2) Identification of the audiences to whom policies will be addressed
3) Definition of the style and format in which policies will be written, the system for numbering and naming policies and the linkages between policies and other management directives, such as procedures and standards

4.2.3.1.4 Measures of Progress

1) Identification of policy risks
2) Evaluation of policy risk potential
3) Selection of the best policy risk management techniques to mitigate or manage risks without unduly curtailing or modifying activities necessary to overall national security objectives
4) Monitoring, measuring and evaluation of the results

4.2.3.2 Objective P-2: Policy Maintenance

Ensure appropriate coverage of information security by current regulatory elements, as well as the capability to cover requirements for future technological developments, by establishing a process for overall review and possible modification, augmentation or creation of the Kingdom's laws, regulations and acts.

4.2.3.2.1 Approach

Develop a dynamic policy and risk management process that provides the capability to effectively manage information system related security risks in a diverse environment of complex and sophisticated cyber threats and increasing system vulnerabilities. Policy risk management includes the evaluation and/or establishment of all regulations and practices designed to mitigate or eliminate losses to which the Kingdom may be exposed. This function will work closely with the National Risk Assessment Function, which is a under the NISE. The NRAS will communicate the types and origins of risks identified in assessments and communicate them to Policy Development to determine if modifications to policies or regulations should be proposed.

4.2.3.2.2 Implementation Initiatives

1) Information Policy Development Process

Define and design an Information Policy Development Process. Guidance on this complex process is essential to ensuring a comprehensive and consistent policy program. This process includes:

- Writing and editing policies, obtaining management approval, communicating policies, and implementing controls to meet policy requirements
- Management instructions indicating a predetermined course of action, or a way to handle a problem or situation
- High-level statements that provide guidance to workers who must make present and future decisions
- Generalized requirements that must be written down and communicated to certain groups of people inside and, in some cases, outside the organization

2) Policy Reviews

Establish a Function to conduct reviews of policies.

4.2.3.2.3 Challenges and Issues

1) Coordinating with various groups from across the Kingdom to ensure an all-encompassing approach may present a challenge.
2) The Function must be granted the authority to complete the established objectives.

4.2.3.2.4 Measures of Progress

1) Establishment of a Policy Development Function
2) Increased level of policies being issued
3) Increased level of policies being updated

4.2.3.3 Objective P-3: Gap Analysis

Ensure all regulations and laws have accompanying policies, and vice versa, by establishing a policy gap analysis process.

4.2.3.3.1 Approach

Selected laws and regulations are being analyzed for gaps and deficiencies, regarding handling and use of digital information and the systems that transport, process, allow access to and store it. The NISS will establish capabilities to conduct gap analyses, utilizing risk assessments and Business Impact Analysis (BIA) to correlate specific system components with the critical services they provide. Based on that information, the consequences of a particular policy, standard or procedure to the correlated system components will be characterized.

1) Policy Development Team

The Policy Development Function should conduct a policy gap analysis comparing existing and internally published policies with the ISO 27001, 27002, ITIL and Control Objectives for Information and Related Technology (COBIT), as well as any other standard deemed necessary. They should assist the various government agencies and other Kingdom organizations in this effort.

2) Security Policy Review

Review all currently available Kingdom security policies, including the following activities:

- Identify the regulatory considerations, i.e. ISO, Certification and Accreditation (C&A), PCI or others.
- Produce a gap analysis.

3) Regulation Review

Review the main Kingdom framework of information regulations and laws, including the following activities:

- Identify the legal and regulatory considerations, e.g. ISO, Certification and Accreditation (C&A), PCI and the physical location of the laws and regulations or others.

- Produce a gap analysis of the legal and regulatory areas as they pertain to Information Security.

Recommend the appropriate changes to update protection requirements and penalties in current laws and regulations dealing with the use, handling, collection, release and storage of digital electronic information. These updates are vital in today's cyber and networked world, with the high mobility of data and ease of theft or loss.

4.2.3.3.2 Challenges and Issues

1) Emerging threats against the Kingdom's critical infrastructures and key resources will expand gaps against intended security objectives, as well as the policies and laws put into place to close those gaps.
2) Constant monitoring of new threats against in-place and emerging policy issues is essential to maintaining a secure environment. Coordinating with various groups from across the Kingdom to ensure a unified approach may present a challenge.

4.2.3.3.3 Measures of Progress

1) Delivery of a policy gap analysis
2) Establishment of a policy repository containing policy objectives, as well as the data for the policies implemented to solve those objectives

4.3 RISK MANAGEMENT AND ASSESSMENT

Risk Management and Assessment (RMA) is a dynamic, iterative and harmonized set of processes for managing and assessing risk. These particular processes, and their implementation structure, compose the Risk Process Management System (RPMS) and a national risk framework.

A national framework is needed for dealing with the Kingdom's Information Security (IS) risk because today identical information can be stored and processed in multiple places, and the various ICT systems and infrastructure are networked. Without a consistent risk assessment process across the Kingdom's various elements, what one organization may evaluate as a high risk, another may identify as low risk because each used different criteria. The problem for senior management is obvious when they must evaluate and make high-level risk mitigating decisions on issues that cross traditional ministry or organization boundaries. A common risk assessment framework is needed to enable senior management to make informed decisions involving risk in the context of current and future priorities, finite resources and global complexity.

The approach is to establish a national IS Risk Assessment Function (NRAF) within the National Information Security Environment (NISE). It will be staffed with trained persons who will develop and adapt the Risk Process Management System (RPMS) for the Kingdom, based on international standards such as ISO 31000 and NIST SP 800-37. It should be noted that no publication covers all situations and that the judgment of trained risk assessment persons is also required to produce the most accurate and relevant assessments.

The RPMS is designed to ensure a secure National Integrated Information Infrastructure (N3i). This term is defined as the broad set of components required to operate an enterprise ICT system. It includes the information systems, such as hardware, software and communications interfaces; support entities, such as power, cooling, facilities and disaster recovery sites; operating policies, performance standards and procedures; and the people with the required skills to operate, maintain and meet the service requirements. The term N3i can also be applied to infrastructures at different levels. At the top level, it can mean the entire Kingdom’s ICT system. It could refer to that of a particular ministry or a national component such as the Government Secure Bus. The fundamental concept is that the term encompasses everything needed by, and associated with, a particular ICT infrastructure.

The RPMS is the management system that is adaptable to the culture, environment, objectives, security needs, processes, size and structure of government agencies and the private sector. It provides a consistent framework for the requisite tools, processes, policies, procedures and resources, including IS risk assessments for the various N3is of the Kingdom.

Detailed objectives, approaches and initiatives for this element are described below.

4.3.1 ELEMENT DESCRIPTION

Risk is the uncertainty of loss, damage, theft or compromise of critical assets of any form. RMA is the set of processes that enable the identification and analysis of critical information and ICT assets and consider their vulnerabilities and the current and potential threats facing them. It can be used to determine the degree to which an entity is organized to deal with risk. RMA also provides a framework for sound decision making by senior management. The cycle of standard RMA activities is illustrated below in *Figure 4.3-1 Risk Assessment and Management Cycle*.

The major elements of the national risk framework are the NRAF, the Risk Process Management System (RPMS), an online e- National Risk Assessment Function (e-NRAF) and, when operational, a comprehensive Risk Assessment Baseline of the Kingdom's Information, ICT assets, IS systems, people and practices. The target of many risk assessments is often some element of the N3i, which requires some of the staff to have strong ICT backgrounds.

The **NRAF** is the organization in the NISE that focuses on IS risk, risk assessment and risk management.

RMA is the set of processes for managing and assessing IS risk.

The **RPMS** is the implementation of the RMA, including the combination of risk management assessment procedures and the people and organizational structure responsible for applying them. These individuals ensure that the RPMS is up to date and adequate for the assessment of the ever-evolving environment and current threats and vulnerabilities associated with the ICT and information environment. The RPMS can also provide risk mitigation and incident guidance, and control information to management. The RPMS will provide a framework that enables an organization to establish risk governance and compliance, using a set of national policies, procedures and guidelines adapted to its unique environment and resources.

The **e-NRAF** is an online repository of risk and risk mitigation information, references, training material and program and project status. Items such as risk assessments have access restricted by special security controls.

N3i is defined as the human resources, processes, practices, procedures, tools, facilities and technology that deal with information and ICT infrastructure throughout their lifecycles, and that involve national interests. The N3i designation can apply to a particular organization's systems, those of an entire government agency or a private organization, including utilities – or at the top level, the entire Kingdom.

Figure 4.3-1 The Risk Assessment and Management Cycle
The NISS provides a national risk assessment framework that allows for adaptation to each organization's requirements

4.3.2 Relationship to Kingdom's Top ICT Objectives

Risk and Risk Management are involved in each objective and project in the boxes below, as they are designed to reduce and manage risk of loss, damage, theft or compromise of critical assets of any form. Creating the framework for reducing loss, damage, theft or compromise, and applying the appropriate framework elements, effectively contributes to each of the objectives and projects in the boxes below.

Projects of the National Communications and IT Plan[1]:
Project P-2-8-38: Setting up Regulations for Information, Computers and Internet Crimes
Project P-2-8-39: Protecting Privacy
Project P-2-8-40: Setting up a Special Unit for Monitoring and Investigating ICT Networks
Project P-2-8-41: Setting up a National Advisory Center for ICT Networks Security

Ministry of Communications and Information Technology (MCIT) objectives for the NISS[2]:

- Transform the Kingdom into an information-secure society, enabling information to be used and shared freely and securely.
- Increase the security, safety, and integrity of online information while promoting the increased use of information technology.
- Develop resilience in information systems.
- Increase awareness and education of security risks and responsibility of information protection.
- Create a set of national guidelines on Information Security Management, Risk Management and Business Continuity, based on international standards and best practices.

4.3.3 ELEMENT OBJECTIVES

4.3.3.1 Objective K-1: Establish the National IS Risk Assessment Function (NRAF)

Create and establish a National IS Risk Assessment Function (NRAF) under the National Information Security Environment (NISE).

4.3.3.1.1 Approach

The approach is to educate and increase the awareness of the stakeholders and decision makers regarding the vulnerabilities, threats and associated risks the Kingdom must deal with today, so that they approve the implementation of the NRAF. The interconnectivity of information systems requires threats and vulnerabilities to be assessed using a sufficiently broad risk-based approach to assess, prioritize and manage IS activities.

4.3.3.1.2 Implementation Initiatives

1) Create and Establish the NRAF

Create and establish the NRAF, consisting of selected, risk-educated and trained senior-level KSA executives. The NRAF will have the authority to oversee information security risk assessments of the various N3i elements within the Kingdom.

2) Create and Formalize the NRAF Charter

Charter the NRAF to:

- Serve as RMA advocates and a source of risk information to senior decision makers.
- Design and implement collaborative information security risk workshops and seminars to encourage the participation of N3i managers in implementation of national, regional and local risk assessment activities.
- Develop collaborative, cross-functional, resource sharing and inter-departmental interchanges regarding IS risks.

[1] The National Communications and Information Technology Plan, KSA Ministry of Communications and Information Technology, 1426H - Unofficial English Translation, pages 68, 69.
[2] Request for Proposals (RFP) For Developing a National Information Security Strategy, KSA Ministry of Communications and Information Technology, Muharram 1432H, January 2011, page 9.

3) Support National Education and Training Efforts

Support KSA national education and training efforts involving risk, risk assessment and risk management.

4) Create an e-NRAF Function

Create an e-NRAS Function in the NRAF that will provide a comprehensive electronic information security reference library, and will function as the central electronic reporting structure for risk that is related to KSA N3i elements. The e-NRAF mandate is to promote outreach, awareness, education, transparency and trust amongst KSA entities, and should include extensive risk references in Arabic.

4.3.3.1.3 Challenges and Issues

1) Encouraging N3i senior management to collaborate on NISS risk issues may be a challenge, as it can expose organizational weaknesses. Specialized workshops should be designed to develop and encourage open dialogue and establish mutual trust, which can serve as the vehicle to build a cohesive non-fragmented national effort. This will require seasoned, experienced management personnel to function as workshop designers and instructor-facilitators, preferably from the NRAF.
2) Establishment of a web interface and extensive background database with a user-friendly search capability (a search capability and query answer designed for non-ICT professionals)

4.3.3.1.4 Measures of Progress

1) Published, signed and implemented RMA Policy
2) Employment of project tracking and scheduling tools critical path, resource management tools and KSA National Risk Process Management Performance Measurement tools, to track and measure the progress of risk assessments throughout the Kingdom.

4.3.3.2 Objective K-2: Establish the National Risk Process Management System (RPMS)

Develop and implement a national RPMS that establishes information security environment and compliance through national policies, procedures and guidelines.

4.3.3.2.1 Approach

The approach here is identical to that for K-1. Convince the senior leadership of the importance of the implementation of this objective, so they will approve the NRAF and this RPMS.

4.3.3.2.2 Implementation Initiatives

1) Develop and Implement RPMS

Develop and implement a national level RPMS that provides for the protection of KSA assets in any form and against any threat, while recognizing that each of the asset forms are interrelated, interconnected and inter-operative (at least with one another), and that an incident affecting one affects at least one other, and most likely more.

2) Develop a Process Mapping Tool

Develop a process mapping tool (or acceptable facsimile) to review, evaluate and analyze the processes and/or method(s) by which an entity operates, and determine where in that process or processes management control points: (1) Exist or do not exist, (2) Are needed or may be required or (3) Require enhancing, refining or eliminating.

3) Integrate Safety, Security, Risk Management, Insurance and Claims Functions

Integrate the Safety, Security, Risk Management, Insurance and Claims functions into the RMA to ensure a more broadly based and risk-focused IS risk management approach.

4) Create Custom Policies and RPMS' at the Operations Level

Require that each manager of a N3i element adopt the National Risk Policy and RPMS as the foundation for creating their own custom RPMS and policy, along with procedures and guidelines.

5) Require Certified NRAF Assessment for Interconnecting Elements

Require those entities wanting to interconnect to a Kingdom N3i to supply a risk assessment certified by the NRAF before connecting, as well as whatever other technical requirements might be placed upon them.

6) Establish Policy and Document Revision Standards

Require all policies to be reviewed, signed and published at least annually, and when major changes occur that are or should be formalized. Procedures and guidelines must be reviewed in accordance with policy requirements and with change management, which is a required component of the RPMS.

7) Certify Basic RPMS Components of Operational Organizations

Certify that each organization's RPMS is based on the National RPMS and contains components with performance standards that include continuous and iterative reviews of internal policies, procedures and guidelines.

4.3.3.2.3 Challenges and Issues

1) Information Security Environment and compliance are the foundation for the RPMS and must be established as integrated, interrelated management functions. Without such a foundation, the Kingdom's Risk Management and Assessment Strategy would become merely a paper exercise program leaving KSA's critical assets vulnerable.

4.3.3.2.4 Measures of Progress

1) Publish online, through the e-NRAF Function, all gap analyses, risk maturity model evaluations and project plans, progress and schedules. This will enable tracking of the status of the NISS implementation, and ongoing risk assessments of various N3i elements using the RPMS. In addition, it will enable NRAF and N3i management to utilize the output of the risk assessments to manage the risks that have been identified.

4.3.3.3 Objective K-3: Conduct IS Risk Assessments of Major ICT Systems for a Kingdom Baseline

Conduct a macro IS risk assessment to establish a risk baseline for the Kingdom's major ICT systems.

4.3.3.3.1 Approach

Convince the key decision makers and stakeholders of the damage and very high risk of NOT establishing a baseline of the risk that the various entities and elements are currently facing. Ignorance of the current risks and not addressing them now carries a much greater risk of loss or damage in the future.

For example, it is a certainty that the Kingdom's information assets are under continuous surveillance and selected attack. This requires a dynamic and centralized organizational framework to assess the associated risks and supply management with quality data for decision-making.

4.3.3.3.2 Implementation Initiative

1) Conduct Initial and Periodic Risk Assessments

Trained personnel will conduct an initial, and subsequently periodic, risk assessment to establish baselines that: (i) Determine the degree to which KSA and its organizations are prepared and organized to deal with Risks, (ii) Determine the adequacy of current RMA programs and if they meet National Risk Process Management System criteria or current best practices and (iii) Enable senior N3i management to determine the next best steps to be taken to manage identified risks.

2) NRAF Risk Management and Assessment Staff

Develop criteria for selecting the Risk Management and Assessment staff in the NRAF. They will be educated and trained in Risk Management and Assessment and then certified as Senior Risk Managers. They will serve as resources and coaches/mentors to N3i senior management and as the foundation for future N3i educators, trainers and coaches/mentors. They will also certify trained N3i risk management staff and others who meet the established criteria.

3) RMA-Trained Staff from Key Organizations

NRAF staff will help select, educate and train personnel from key organizations, including the defense sector if they want this training. The selected personnel will be RMA trained and certified to conduct risk assessments. It is preferable that the RMA certified personnel should not be the only ones directing the risk analysis for the infrastructure with which they are or may be affiliated. The objective is to ensure an accurate and impartial assessment that identifies existing weaknesses, strengths, vulnerabilities and threats.

4) RPMS Measurement Tools

NRAF will analyze its risk assessment findings using RPMS measurement tools.

5) N3i Senior Risk Managers

RMA-certified personnel will serve as future N3i senior risk managers

6) National Information Security RMA Training Program

NRAF staff will design and manage the National Information Security RMA Training Program.

7) Continuing Education

NRAF will establish, through its NRAF senior risk managers, mandated initial and continuing RMA Training Programs, which will certify graduates and require ongoing education, training for re-certification.

8) Discuss Assessment Findings with Appropriate Personnel

Do NOT publish, but discuss with the NRAF and each N3i member's senior management the Initial Risk Assessment findings. Have the NRAF and the senior N3i management determine the next best steps to resolve any negative findings and a strategy to do so, including timelines.

4.3.3.3.3 Challenges and Issues

The following challenges and issues are the same as those in K-1 and K-2.

1) Encouraging N3i senior management to collaborate on NISS risk issues may be a challenge, as it can expose organizational weaknesses. Specialized workshops should be designed to develop and encourage open dialogue and establish mutual trust, which can serve as the vehicle to build a cohesive non-fragmented national effort. This will require seasoned, experienced management personnel to function as workshop designers and instructor-facilitators, preferably from the NRAS.
2) Information Security Environment and compliance are the foundation for the RPMS and must be established as integrated, interrelated management functions. Without such a foundation, the Kingdom's Risk Management and Assessment Strategy would become merely a paper exercise program leaving KSA's critical assets vulnerable.

4.3.3.3.4 Measures of Progress

1) Create an RPMS tool to measure the effectiveness of an organizations current risk assessment process and to determine if the RPMS is adequately implemented and integrated into and throughout the organization and their processes.
2) The RPMS will address high frequency/severity/impact real or potential threats, including those in transition from uncertain threats to certain definite threats. Definite threat means there is no question a current threat exists such as from foreign attacks against the Kingdom's ICT systems.

What may be unknown is the severity and potential damage from the threat and the risk that it creates. The number and scope of credible Risk Assessments is a good measure of progress.

3) Establish the e-NRAF website. Measure and analyze online usage and page hits.

4.4 National ICT Infrastructure

This section of the NISS identifies objectives and approaches to strengthen the information security and resilience of the KSA ICT infrastructures, specifically with respect to required design, implementation, management and operational functions and processes.

The National Information Communications and Technology (ICT) infrastructures and information systems of the KSA must be protected and prepared to respond to internal and external events that could adversely affect their overall security and availability, and affect the homeland and its people. A review and analysis of available KSA information identified both a need to and a collective awareness for greater consistent application of national-level information security requirements, guidelines and processes similar to those implemented by mature information societies of other countries.

KSA initiatives already underway to augment and improve infrastructure security and resilience efforts should be continued and are incorporated into the approaches described in this section. Several essential technical approaches and initiatives are detailed in this section to achieve better and more consistent results. They are to be implemented together with the policy directions, risk management, governance, organizational and process development and implementation discussed in other sections of the NISS.

4.4.1 Element Description

When developing strategic directions and initiatives for the information security of national ICT infrastructures and information systems for the NISS, it is important to understand them in the context and relationship to critical infrastructures within the KSA. Only the current e-Government initiatives show evidence of the application of a consistent risk assessment methodology, an enterprise level architecture and a business/mission requirements analysis to drive the application of information security controls and practices commensurate with systems posing similar risks.

Within many societies today, ICT infrastructures and information systems provide critical functions and services that affect the operations of a nation's security systems, government organizations and private enterprises. As operational dependency on the ICT and electronic systems increases, the management of information security risks becomes more critical. Information security is not only an essential enabling function for most services, but must also provide countermeasures to vulnerabilities that can be exploited.

In addition, the implementation of ICT information systems, applications and operational processes affects the availability, reliably and sustainably of critical functions and services in the face of disruptive events. One of the overarching NISS goals is to provide KSA a strategic direction, in order to achieve an appropriate and sustained level of ICT security and *infrastructure resilience*.

> ***"Infrastructure resilience" is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive event.***

Laws/acts, policies, regulations and directives establish the key direction, requirements and expectations to be pursued. However, the actual design, implementation, management and operational practices will yield the resulting security and resilience performance that ICT infrastructures and systems must achieve. The performance and effectiveness of the implementation and operation of an ICT information system or infrastructure is determined by four key aspects – people, process, culture and technology.

Management of the environment of national ICT infrastructures and information systems must be consistent with an incident response and crisis management system that is applicable to a business/mission environment. *Figure 4.4-1* displays the integration of these activities in the context of this section of the NISS.

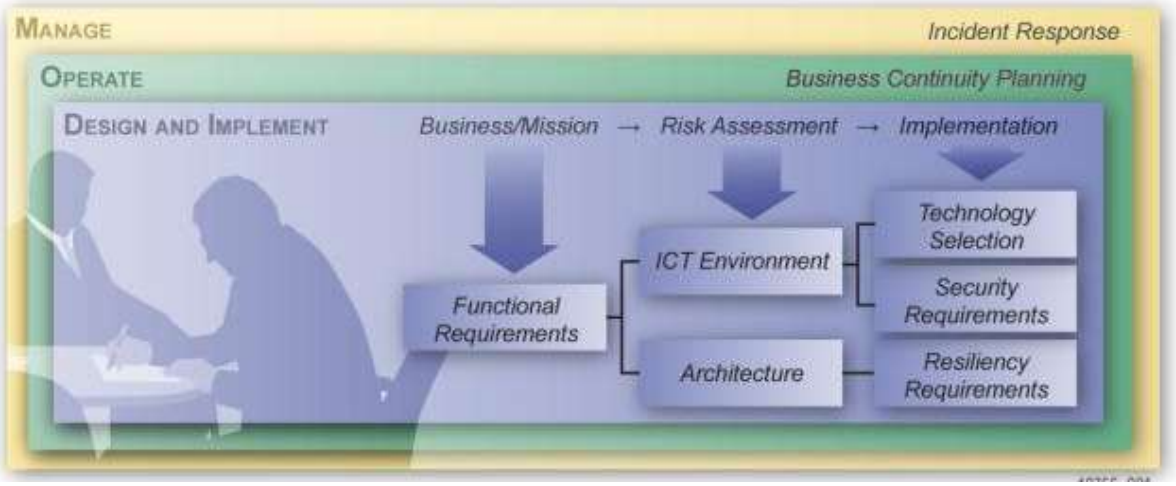

Figure 4.4-1 Design, Implement, Operate and Manage
These efforts must be accomplished as parts of an integrated process.

The challenge for those addressing complex ICT infrastructures and information systems is assuring there is a framework that aligns the business/mission objectives and requirements with the appropriate technology architecture and operational practices. The internationally accepted definition of architecture is "The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution."[1] For KSA e-Government initiatives, the YESSER Consulting Group has properly identified the importance of this relationship and has established architectural assistance services to guide the transition of ministries to e-Government services. Similar collaboration and information sharing would be beneficial among critical infrastructure owners and operators. Similarly, government and private sector organizations need to have a stronger partnership focus, sharing information and practices in ICT and information systems architecture development and analysis.

Therefore, the NISS must assure that those with responsibility for advancing the KSA transformation adopt a culture that values and adopts a strategy with a focus on enterprise architectures – a culture biased toward the adoption of open architectures and standards, and well-developed resilience approaches based on risk mitigation requirements. National-level direction, principles, objectives and requirements established through a NISE structure described in the NISS can advance and foster the required culture.

Applying these principles requires an architectural framework. An architectural framework is a structure for developing a range of architectures. The Open Group Architecture Framework (TOGAF) is one such broadly accepted, internationally developed framework that is used for developing enterprise architectures.

Leading industrialized countries have been addressing information security and ICT infrastructures security and resilience for many years, along with the efforts of international standards bodies and numerous institutes and organizations. The body of knowledge and lessons learned provide a rich array of strategies, objectives and practices to address similar challenges faced by all organizations within the Kingdom.

[1] ISO/IEC 42010:2007, Systems and software engineering -- Recommended practice for architectural description of software-intensive systems

4.4.2 RELATIONSHIP TO KINGDOM'S TOP ICT OBJECTIVES

The KSA *Ninth Development Plan (Eng.), Chapter 24, Information and Communication Technology*[2] identifies two important objectives most relevant to this section of the NISS:

- ICT services infrastructure should provide high quality, security, and reliability, at reasonable prices, in all regions and to all segments of society and
- ICT infrastructures and services should ensure and provide safeguards for the security of user's information.

The NISS National ICT infrastructure objectives in this section are constructed to complement existing efforts within the KSA and to further ensure several key strategic outcomes essential to KSA's transformation to an information society are achieved. The key ICT infrastructure outcomes to be achieved are:

- An internationally recognized Kingdom-wide technical strategy, culture and practices that further strengthen security and resilience for ICT infrastructures and information systems that affect the national security and economic security posture of KSA
- Assurance and confidence in the security and resilience design and implementation of ICT and information systems across the Kingdom
- Accelerated adoption of appropriate internationally accepted security and resilience standards, processes, controls and practices, such as ISO/IEC, ITIL, CoBIT and TOGAF; as well as the evolution of improved security technology across the ICT and information system life cycle
- Increased levels of trust by the Kingdom's businesses, government organizations and people using online services and applications for daily activities

4.4.3 ELEMENT OBJECTIVES

International standards bodies (e.g. ITU, and ISO/IEC) and other recognized leading IT and security organizations (e.g. COBIT, ITIL, TOG, ISACA and the U.S. National Institute of Standards and Technology (NIST)) have mature frameworks, best practices and standards developed by well-established national and international communities. These address essential processes for IT Governance, Enterprise Architectures and Frameworks, IT Service Management, Information Security Management Systems, Security Control Domains, Security Standards and Best Practice Guidance.

YESSER efforts for e-Government demonstrate the type of structured endeavor that is needed for ICT systems to provide and achieve the coordination, guidance, business process focus, architectures and standardization for more integrated information security capabilities, and to capitalize on the value that modern ICT can provide.

Analysis of NISS data collection documents and responses to questions identified a range of information security efforts for ICT and information systems environments that are at various stages of maturity, among the responding ministries. Through a more consistent application of generally accepted international best practices and adoption of more mature information security management processes, information security efforts within ministries can be elevated. Key objectives for the National ICT Infrastructure are identified in this section. Specific strategies for achieving these objectives are also provided, along with a list of implementation initiatives to improve the information security and resilience posture for participating organizations and critical ICT infrastructure components.

[2] Ninth Development Plan (Eng.), Chapter 24, Section 24.1.5.2, page 479.

4.4.3.1 Objective T-1: ICT Infrastructure Evolution, Architecture, Implementation, Management and Operations

Ensure that the owners and operators of KSA's critical infrastructures evolve their ICT architecture and implement, manage and operate ICT infrastructures with appropriate information security and resilience practices for their systems and operations.

4.4.3.1.1 Approach

Create a national program to assure the physical protection and security of the information systems within critical infrastructures. ICT infrastructures must be protected and designed to operate in the face of failures and threats commensurate with their critical national and economic security operational functions, dependencies and interdependencies. Capitalize on lessons learned from similar efforts of other countries. Include within the program the adoption of the NISS, and require KSA infrastructure organizations to develop an infrastructure dependency and interdependencies analysis. To further support information security goals, structure both formal and informal capabilities and processes that will foster and enhance information sharing and cross-organizational coordination among infrastructure owners and operators.

4.4.3.1.2 Implementation Initiatives

1) Collaboration Between The Public Sector and Infrastructure Operators

Establish a combined effort of representatives from public sector organizations with mission responsibilities for infrastructure and the owners/operators of those infrastructures. They will undertake the development of a national program that results in consistent risk assessments, application of internationally recognized best practices, security controls and countermeasures for similar infrastructures. Such results can be shared through the appropriate NISE Functions, such as the Security Operations Center (SOC), establishing broader information sharing and incident response/management and coordination.

The national program should be designed to:

- Ensure that the ICT and information systems that underlie critical national and organizational infrastructures have implemented proactive protective and resilient technological strategies, architectures, implementations and processes to meet critical levels of services. These strategies, architectures, implementations and processes should be based on both dependency and interdependency analyses and an operational risk assessment.
- Leverage international standards, partnerships, alliances and collaboration through participation in international security bodies and organizations to identify state-of-the-art practices and technology.
- Utilize CERT-SA and any other IS and cyber threat and incident centers and establish a Function comprised of government and private sector technical representatives from critical infrastructure areas. These representatives will establish responsibilities and processes for the expanded sharing of operational situation awareness (incident, threats and vulnerability), coordinate security and resilience practices, develop the necessary capabilities for cyber-incident analysis and creation of secure processes for sharing information and situational awareness for operators and decision makers. This could evolve into an all-source Security Operations Center under the NISE and should support KSA national-level crisis management efforts.

2) Partnership with Telecommunications Providers

The Government's Telecom Regulator shall ensure a long-term partnership effort is undertaken with telecommunications providers to assess and improve telecommunications/network security and resilience. This is a necessary effort to support the increased dependency and interdependency that will result as the Kingdom transforms into an information society and digital economy. Consider formation of a private sector National Security and Emergency Preparedness Telecommunications

Advisory Committee, comprised of senior members of key telecommunication and internet service providers, to assist in the effort and progress reviews.

3) IS Business Continuity and Disaster Planning and Management

Due to the importance of electric power for the operation of most ICT and information systems, conduct an analysis to assure that SCADA, and other systems required to maintain and recover operations of vital electric power system components, have implemented required ICT and information system asset protection and security measures. Ensure that such measures are regularly monitored, evaluated and audited for effectiveness. Ensure business continuity plans and disaster management and restoration plans are established and regularly exercised. It should be recognized that to provide adequate IS business continuity many supporting areas must be addressed to assure effective backup and restoration in the event of a disaster

4.4.3.1.3 Challenges and Issues

1) Though each critical infrastructure organization is responsible for its own operation's security and resilience, the national government must ensure that those organizations are implementing practices commensurate with the importance of the services, as well as their potential to impact KSA's national and economic security.
2) Telecommunication dependencies affect all other critical infrastructures. Historical relationships and independence must transform to an increased transparency that increases confidence and assurances of service.
3) Because of the sensitive nature of information about these infrastructure operations, development of a trusting environment to share specific information about vulnerabilities, incidents and practices will require strong collaboration among owners and operators. Specific recommendations for sharing this type of information are highlighted in ***National Cooperation and Sharing for Information Security,*** section ***4.7ن***

4.4.3.1.4 Measures of Progress

1) The extent of the willingness of leaders to encourage collaborative efforts and methodically measure progress and accountability on implementation initiatives is a key indicator leading to success.
2) Service quality and outage metrics should be standardized and reviewed by MCIT with infrastructure owners and operators to identify issues to be addressed.
3) Identify key service metrics, to include service restoration goals. Exercises and test of recovery and restoration plans and processes should be conducted on a regular basis to identify *after action* areas of improvement. Track and test after actions to assure proper implementation and changes in processes.

4.4.3.2 Objective T-2: Technical Frameworks for ICT Infrastructures and Information Systems

Establish a KSA common evaluation process that permits owners and operators of ICT infrastructures and information systems to uniformly identify an appropriate *risk tier* level that reflects their ICT infrastructure and system information security and resilience requirements.

4.4.3.2.1 Approach

As guidance to owners and operators of ICT and information systems, develop a set of common technical frameworks for security and resilience approaches and practices, to be applied to systems based on the risk assessment methodology discussed in section ***4.3 Risk Management and Assessment***.

4.4.3.2.2 Implementation Initiatives

1) ICT Security Standards and Policies

Establish a well-publicized national program to lead, coordinate and establish initiatives among the national security, ministries, critical infrastructure sectors and private sector organizations to assess and improve the security and resilience of critical infrastructures utilizing a common risk framework.

2) Risk Tier Standards

Establish risk tier standards, controls and metrics for assuring consistent security and resilience application by ICT and information system owners and operators by adapting the U.S. National Institute of Standards and Technology (NIST) 800 series process as the basis for developing such an approach for KSA.

4.4.3.2.3 Challenges and Issues

1) Elevating the priority of the technical challenge and the importance of collaborative efforts to KSA is essential, especially to attract the best technical talent to this difficult endeavor.
2) Due to the very complex nature of the ICT and information systems, KSA should capitalize on existing developed frameworks, guidelines and standards; for example, the U.S. NIST approach and documents. They can serve as a way of accelerating adoption of the required framework.
3) Inter-networking of information systems and networks requiring different levels of risk management must be explicitly addressed, especially as cloud architectures are adopted.

4.4.3.2.4 Measures of Progress

1) Developing the KSA technical framework should be a priority effort. Specific milestones should be established and tracked during development of the framework.
2) Metrics for the adoption levels by organizations can be carried out through annual surveys and should be used as a key performance indicator of progress.
3) Continuous monitoring of critical sensitive interconnections can be applied to measure and demonstrate compliance with requirements

4.4.3.3 Objective T-3: Government ICT Infrastructures

Institutionalize a cross-ministry effort that goes beyond e-Government systems to evaluate and assure that each ministry has well-defined processes to address documented security and resilience requirements for their ICT infrastructure and systems.

4.4.3.3.1 Approach

Provide an increased national focus on current implementations to identify any security and resilience gaps. Develop remediation or technology migration plans to meet the transformational aspirations of the KSA.

4.4.3.3.2 Implementation Initiatives

1) Cadre of Expertise

Develop a cadre of expertise familiar with current architectural analysis and development processes and tools to enhance capabilities and promote the importance of these specific skills and expertise.

2) Workshops and Opportunities for Expanding Information Sharing and Collaboration

Create workshops and opportunities for expanding information sharing and collaboration among government, private sector and academic organizations about enterprise architectures. Include a special focus on wireless and *cloud* based services/infrastructures.

3) Government Enterprise Architecture (GEA)

Adopt, and require ministries to follow, a Government Enterprise Architecture (GEA) and identify international security standards, practices and common technology configurations to be applied to the GEA.

4) Compliance Monitoring Practices

Develop compliance monitoring practices using continuous monitoring methodologies for evaluating the state of compliance to adopted standard configurations.

5) Engagements with International Activities

Increase the number and frequency of engagements with international activities such as The Open Group, standards bodies and consortiums that are leaders in security and resilience for existing and emerging technologies.

4.4.3.3.3 Challenges and Issues

1) Strong leadership among Chief Information Officers (CIOs) within ministries or agencies will be required.
2) Developing a common vision and mission among the diverse ministries will take time, unless there has been a prior focus on architecture methodologies. Similar broad efforts have taken years to reach maturity.
3) Those that share a common network and do not comply with the architecture and practices can place the security of others at great risk. Some have found that penetration testing by expert companies in this field can be effective in demonstrating existing issues, which then precipitates greater collaboration and a willingness to share information and practices.
4) Emerging use of more automated compliance monitoring capabilities has shown objective levels of improvement. New techniques require sufficient resources and time for adoption.
5) Technology and security threats and capabilities change rapidly. Very active engagement with those facing similar problems and issues is essential.

4.4.3.3.4 Measures of Progress

1) Tracking of the number of new certified individuals and experience levels with architectural analysis tools and processes within each ministries CIO office
2) Establishment of a plan and timeline for development and transition to common architectures, standard products and shared services and infrastructures
3) Tracking and publishing of milestone accomplishments
3) Compliance audits and testing of each ministry on a regular periodic basis, and providing them with *scorecards*, can serve to monitor and demonstrate continuous improvements in these critical areas.
4) Identification of organizational responsibilities for selected international engagements; Levels of information sharing resulting from those engagements with colleagues in other ministries

4.5 HUMAN RESOURCE

The Human Resource (HR) element of the NISS is focused on expanding the number of Saudis qualified and willing to work for the government in the field of IS security. Five interrelated and interconnected HR elements require integrated and overlapping approaches involving Human Infrastructure (Human Resource in specific jobs), Education, Training, Awareness and Shared Responsibility.

Increasingly rapid changes in technological, economic, cultural and occupational spheres have radically increased the risks to information and ICT systems. Most of the Kingdom's organizations that responded to the NISS data collection questionnaire cited lack of qualified ICT security staff as a major issue. Without qualified staff, the appropriate defense cannot be implemented and ongoing penetration attempts and successes may not even be noticed. This situation could place such elements as the Kingdom's major financial and investment strategies, the petroleum delivery systems and the nation's political deliberations at risk of exposure or exploitation due to weak IS practices.

The approach is to first identify work-ready Saudis who, with minimum of training, could be quickly employed based on their true (not paper) qualifications. Second, it has been reported that government compensation for Saudi employment in IT and IT security positions is neither competitive with private industry nor equivalent to that received by some professionals from neighboring countries. Instituting a premium compensation scale to raise Saudi compensation is proposed so the current unfilled need can be met. The third approach is to greatly expand IS education and training. Detailed objectives, approaches and initiatives for this element are described in the sub-sections below.

4.5.1 ELEMENT DESCRIPTION

The HR element of the NISS focuses on the broad range of information security and ICT security requirements that involve the following five areas.

Human Infrastructure is defined as the human resources in individual positions of leadership, employment or functional responsibility. For example, a brilliant researcher who is not a manager and an excellent manager who is not a researcher compose a human resource. One assignment creating a human infrastructure would be the researcher in a research position and the manager in a managerial position. Another assignment could be the reverse with the researcher in the managerial position and the manager in the research position. It is clear that the value to the Kingdom of the second human infrastructure assignment is much less than the first.

Education is a broad concept involving the entire spectrum of both formal, self-taught, on line, professional and job based schools, institutes, workshops, special courses, programs and opportunities to equip human resources with the knowledge, learning capability, thinking , language, analytical and problem solving skills needed for success in the 21st century's ICT and information environment. At the top university level, a Kingdom IS certification program can be established with uniform and stringent certification standards for both teachers and curriculum. This can be combined with foreign universities in exchange of both teachers and students.

Training is intended to provide and continually update the mental and physical skills, language proficiency and functional knowledge required for productive employment today and into the future. This includes the development of technical capabilities and strategic thinking, as well as individuals who can manage, supervise and make sound security decisions in the context of their organizations' missions and available resources.

Awareness is the understanding of the threats and vulnerabilities in today's government, private sector and consumer online systems and the consequences of poor security in each. Technology, innovation and growth sectors require HR ICT security awareness. It is the responsibility of each individual to protect information in any form, from its creation to its eventual destruction, regardless of who owns the information. This is accomplished through initiatives and the use of creative approaches to ensure that ICTS awareness, education and training are available to all people.

Shared Responsibility is the concept that each person has a responsibility to act appropriately in protecting the information and ICT systems belonging to them and their organization, as well as each ICT system with which they are involved. It is important for the leadership, government and private sector managers and employees, as well as the public, to understand that the actions or lack of correct actions, by even one person can create high risk to the security and privacy of information and the security of ICT systems that are remote but interconnected.

4.5.2 Relationship to Kingdom's Top ICT Objectives

The Kingdom's HR is a major element of each of the national plans, with emphasis depending upon the objective of the plan. Some national objectives relevant to the HR Element of the NISS are listed in the boxes below**.**

National Communications and Information Technology (NCIT) Plan[1]

- …. It is expected that ICT will greatly facilitate the effective employment of women and utilization of their capacities.
- Raising the percentage of university students in ICT specializations Transformation to information society requires the promotion and development of educational curricula, teaching and learning methods, as well as dissemination of new constructive concepts and values in the society that encourages innovation, invention, creativity, work perfection, productivity, raising initiatives and acceptance of failure.

Ninth Development Plan
Human Resources Development[2]

The Plan highlights a range of issues and challenges facing the Kingdom in its drive towards attaining higher international competitiveness rankings. These include:

- The need to raise the educational level of the workforce, towards a well-qualified workforce, capable of absorbing new technologies, is one of the cornerstones of competitiveness.

4.5.3 Element Objectives

4.5.3.1 Objective H-1: Increase Number of Saudi IS Practitioners and Managers

Increase the availability and number of educated, trained and skilled Saudi Information Communications and Technology Security (ICTS) professionals and managers to fill current and future key ICTS positions.

4.5.3.1.1 Approach

The approach consists of a series of both short and long-term initiatives that utilize current information security human resources and are aimed at increasing the size of the future ICT and ICTS Saudi HR.

The short-term strategy is to:

- Eliminate the current disincentives for skilled people to accept ICTS government jobs.
- Increase the utilization of women in ICTS.

[1] The National Communications and Information Technology Plan, The Vision Towards the Information Society 1426H, unofficial Translation of the Arabic text.
[2] Development Plan (1431/32 - 1435/36) 2010-2014, Ministry of Economy and Planning, Chapter 24.

- Recruit, train and employ work-ready but underutilized ICTS skilled Saudis in the Kingdom's provinces.
- Repatriate skilled Saudi teachers, researchers and practitioners currently overseas for both temporary and permanent assignments in ICTS.
- Revaluate the skills, qualifications and performance effectiveness of those in senior ICTS positions for eligibility for premium compensation, as well as for being retained in that critical position.
- Review civil service's job descriptions and HR regulations that pertain to ICTS positions.

The longer-term strategy is to:

- Create a process for early identification of talented children and youth to be trained for key ICTS positions in the Kingdom.
- Create a national ICTS development program.
- Create cooperative programs with friendly international countries and institutions.
- Establish continuous and current professional training for ICTS teachers, researchers and practitioners.

4.5.3.1.2 Implementation Initiatives

1) Upgrade Salary Scale

Develop a scale for ICTS government jobs that is comparable in wages and benefits with industry compensation for qualified persons.

2) Employ qualified women

Employ qualified women in ICTS positions, some of which could be in all female locations. Identify and establish a cadre of skilled Saudi female ICTS practitioners and teachers with appropriate training and competitive salaries.

3) Hire Skilled Saudi ICTS Persons

Encourage the Kingdom's provinces to hire skilled Saudi ICTS persons so the regional and municipal ICT systems and disaster recovery infrastructure meet information security objectives.

4) Establish Salary and Benefits Incentives

Establish an incentive program of salary and benefits to encourage Saudis qualified in ICTS who are new graduates, or are currently working in the private sector, to accept government positions. It is important to establish a compensation program for new graduates that provides mentoring, helps them to understand the organization and job requirements and rewards them with a view of a positive career path for successful performance. For the more experienced persons from industry, it is important that their introduction into government service be positive. They should be informed of appropriate career training and advancement opportunities, as they demonstrate their competence. In this case, a more senior mentor or advisor can help to make the transition smoother and reduce the natural stress of a major job change.

5) Identify and Train Talented Students

Have the Ministry of Education (MOE) and Ministry of Higher Education (MOHE) investigate and establish a coordinated program to identify talented students and also provide practical training such as Mawhiba program.

6) Create a Companion Program for Young 'Hackers'

Create a companion program for those young *hackers* who thrive outside an academic setting. Supply initial funds to establish this program from those organizations whose operations depend, for example, upon SCADA control systems. After appropriate vetting and training these people can help to provide real world assessments of the information security status of critical ICT systems. Enlist the support of

such organizations as the Ministry of Commerce and Industry, Ministry of Labor, Ministry of Higher Education, along with major companies and some of the midsize and smaller specialized companies. The purpose is to create real world, but controlled, information security and cyber labs and facilities. Here the Kingdom's youth can exercise both their hacking and defense skills, learn and improve their capabilities, while in a real work environment. At the same time, they can be positively recognized for their talents.

7) Develop a National Education and Training Program

Develop a coordinated national education and training program utilizing both formal education, internships in government and industry, and extensive and continuing professional education in the fields of ICTS allowing for an upward career path.

8) International Cooperative Exchange

Utilize educational, government and private sector resources and cooperatively exchange ICTS activities with countries such as the GCC, and other countries friendly to the Kingdom.

9) Enlist International IS Professionals

Enlist top international IS persons on a temporary or permanent basis to provide training, teaching and workshops to both Saudis and other compatible nationalities. This will combine the benefits of having the best teachers and professionals with the networking benefits generated by the students and attendees.

10) Utilize Existing Scholarships Toward Promoting Qualified IS Professionals.

NISS Information security environment structure shall utilize existing scholarships programs to promote qualified skillful students abroad who are supported through KSA financial assistance and studying IS , and encourage them to continue IS professional education and training..

4.5.3.1.3 Challenges and Issues

1) There is currently a shortage of qualified KSA citizen human resources with the requisite skills to fill current and future information security positions due to employee retention problems and salary and benefit inequities. Correcting these issues will require some changes in government compensation and career planning for employees in the information security fields.
2) The salary for Saudi qualified persons has been reported to be low in comparison with other professionals elsewhere. . While loyalty and dedication are a function of the individual, such unfairness is a breeding ground for disgruntled people who believe they are being treated unfairly. The insider threat has traditionally been the most dangerous. Reducing or removing such unfairness in compensation for qualified persons may be a challenge, but not addressing it can create major risks to the Kingdom.
3) Another challenge to meeting this objective is convincing the Kingdom's ministries that the substantive improvement required in information security, dictated by the risks from the ICT environment, is worth the extraordinary steps, cooperation and new approaches required to increase the ICTS component of the Kingdom's human resource.

4.5.3.1.4 Measures of Progress

1) Reduction in percentage of vacant ICTS positions
2) Increase in percentage of ICTS positions filled by qualified Saudis

The following HR objectives (H-2 through H-5) have the same Approaches, Implementation Initiatives, Challenges and Issues and Measurement of Progress, which are described under *Objective H-5: Promote and Emphasize the Concept of Shared Responsibility*.

4.5.3.2 Objective H-2: Increase and Improve Information Security Education

Develop a program to improve the quality and availability of IS education at all levels to produce the comprehensive Human Resource needed in the various fields of information security.

4.5.3.3 Objective H-3: Increase and Improve Information Security Training

Develop a program to increase the number of skilled IS professionals who have hands-on training in simulated or real world conditions.

4.5.3.4 Objective H-4: Expand and Improve Information Security Awareness

Encourage, support and coordinate the expansion of current programs in the Kingdom that are devoted to increasing information security awareness of the threats and defenses involving online applications.

4.5.3.5 Objective H-5: Promote and Emphasize the Concept of Shared Responsibility

Develop approaches to foster IS responsibility among all sectors of the Kingdom, with emphasis on the importance of the individual's role.

4.5.3.5.1 Approach

The approach is to expand IS education, training, awareness and responsibility under coordination and direction from the NISE Human Resource Development Function and the NISE National Outreach and Awareness Function.

4.5.3.5.2 Implementation Initiatives

1) Establish Continuing Awareness and Instruction Campaign

Establish a continuing awareness and instruction campaign regarding how to safely, securely and confidently utilize KSA e-government and its online applications.

2) Establish Educational Baseline

Establish an educational baseline that determines current ICTS education and training initiatives and adequacy, and identifies areas to refine or enhance current initiatives.

3) Integrated ICTS Educational System

Refine, enhance or create an integrated ICTS educational system that focuses on developing HR skills and a talent development framework. This educational nurturing will occur from earliest education through Primary, Intermediate, Secondary and Higher Education schools, and graduate school through employment.

4) Partner with Business for Technical Education

Expand and continue to encourage enhanced ICTS technical education and training initiatives through partnerships with KSA companies and international companies.

5) Enhance Early ICTS Curricula

Develop and enhance appropriate ICTS curricula, beginning in the early grades through graduate levels. Include coursework in Decision Making, Critical and Strategic Thinking and Planning, Risk Management, Technology Management, Information and Cybersecurity, Information Technology and Individual Responsibility. The importance of each individual's role in and contribution to national, organizational and personal security and privacy should be emphasized.

6) Early Identification of Leaders and Researchers

Identify, beginning in early grades, both potential leaders and researchers for additional training in relevant disciplines related to their ICTS aptitude.

4.5.3.5.3 Challenges and Issues

1) Coordinating programs across ministries and with industry can be a challenge. That is the reason for the -NISE Human Resource Development Function.

4.5.3.5.4 Measures of Progress

Create a qualification and testing system, including both practical real world situations and formal learning to determine, analyze and evaluate if the information security development programs are meeting the goals set for producing the number of qualified Saudis.

4.6 RE-ASSESSMENT AND AUDIT

The Re-Assessment and Audit strategy element includes outlining and developing an approach to a common framework for security assessment, re-assessment and audits, which is based upon national and international best practices, guidelines, procedures and policies. In addition, this element will assist in the development of an approach to the certification and accreditation of new systems prior to being placed into operation.

Protective security, including physical, personnel and information security are key enablers in constructing and maintaining a productive and robust KSA Information Society and Economy. Security risks must be managed effectively, collectively and proportionately to achieve a secure and confident working environment.

Implementation of the strategic drivers described in this section is important to the success of the Re-assessment and Audit strategy and will facilitate the development of associated action plans. Detailed objectives, approaches and initiatives for this element are described below.

4.6.1 ELEMENT DESCRIPTION

The Kingdom recognizes that dependence on information technology and the information systems developed from that technology to successfully carry out missions and business functions is prevalent in today's digital age. Integral components of an information system can include a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. The need to assess and audit these systems and their components is an essential aspect of the risk management process.

A national level strategy for re-assessment and audit will help to:

- Determine the most efficient and effective mechanisms to obtain strategic warning, maintain situational awareness and improve incident response capabilities
- Improve the security posture of critical infrastructure systems
- Determine the need to update or replace existing policies and technologies
- Evaluate new technology
- Uncover fraudulent or other illegal activities
- Reinforce and strengthen internal controls

Assessments and Audits are ultimately aimed at studying processes for their improvement, but there are distinct differences.

Assessments help to collect and analyze information and also present recommendations for decision-making. An Information Security Assessment is a formal, systematic process of data gathering, regarding information security measures that are in place compared to an established set of criteria (ISO 27001), in order to determine what needs exist. In other words, it is systematic analyses of the way things are and the way they should be. Typical methods for conducting an Information Security Assessment include:

- Surveys
- Interviews
- Standards
- Statistics
- Record reviews

The assessment looks at the completeness of the security initiatives or program. By conducting the assessment first, the organization can remediate any significant shortcomings before a security audit is

performed, which is a formal record of the security status of an organization as measured against a specific standard.

Audits examine if the results of quality activities are in compliance with planned arrangements or stated processes. Audits also check if the planned arrangements are effective enough to meet the objectives for which they were set. An Information Security Audit is a systematic evaluation of the security of the Kingdom's information system, which is accomplished by measuring how well it conforms to an established set of criteria that results in a factual record. Audit activities typically focus on measuring the security of the system's operations, configuration and environment, software and information handling processes, as well as user practices. The Information Security Audit also results in the determination of regulatory compliance in the wake of legislation (such as HIPAA and Sarbanes-Oxley in the U.S., and eCrime laws in Saudi Arabia) that specifies how organizations must deal with information. Typical methods for conducting a security audit include:

- First hand (independent) observations
- Custom designed testing of security controls
- Independent monitoring of security controls
- Placing historical information under scrutiny
- Evidentiary collection via forensic analysis

The audit strategy must be specifically organized to provide a risk-driven methodology and framework for tackling the enormous task of designing a national enterprise security validation program.

The ultimate goal of the audit is to assist management in understanding the relationship between the technical controls and the risks to the organization/business affected by these controls. The findings, threats and vulnerabilities are explained and documented in a report, based on validated information from evidence gathered and examined during the audit.

This brief description of audits is consistent with major certifying bodies such as the Information Systems Audit and Control Association (ISACA), which is the international organization that issues certifications for Certified Information Systems Auditors (CISA) and the Institute of Internal Auditors.

4.6.2 Relationship to Kingdom's Top ICT Objectives

KSA has identified several initiatives that address the need to combat cybersecurity crime, establish enhancements and promote awareness. The establishment of a re-assessment and audit initiative, to include certification and accreditation of all systems and a focus on critical infrastructure systems, will provide KSA the ability to assess cyber threats, as well as information security enhancements. System hardening guidelines become critical to ensure the success of all strategies to be implemented.

4.6.3 Element Objectives

4.6.3.1 Objective A-1: Assessment and Audit Methodology

Provide a Kingdom-wide harmonized ICT methodology for a system assessment, re-assessment and audit program that is customized to the Kingdom's environment. The methodology should be based on the principles of international standards such as ISO 27001 and 27002, as well as generally accepted best practices, guidelines, procedures and policies.

4.6.3.1.1 Approach

The assessment and audit approach to be developed by NISE's information security National Risk Assessment Function (NRAF) includes a number of security controls and consists of the following steps:

1) Identify and quantify risks to critical assets.

   Critical assets are those systems, processes or people any given service relies upon for normal, sustained operation. Risk is defined as the potential that a threat will take advantage of a vulnerability identified in a critical asset, thus impacting the continued operation of the associated service.

2) Identify and quantify possible response to identified risks.
3) Select appropriate responses for implementation.

4.6.3.1.2 Implementation Initiatives

1) Evaluate the Security Controls

Evaluate the security controls established by the NISE NRAF using appropriate assessment procedures. This evaluation determines the extent to which the controls are implemented correctly, operating as intended and producing the desired outcomes, with respect to meeting the security requirements for any system. A properly conducted assessment and re-assessment (continuous monitoring) will help to:

- Ensure that managing information system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy established by the senior leadership through the risk executive function.
- Ensure that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development lifecycle processes.
- Support consistent, well-informed and on-going security authorization decisions, transparency of security and risk management-related information and reciprocity.
- Achieve more secure information and information systems within the Kingdom through the implementation of appropriate risk mitigation strategies.

4.6.3.1.3 Challenges and Issues

1) There are several dependencies in developing a re-assessment capability at the national level.
2) Documents that describe the Certification and Accreditation (C&A) requirements, responsibilities, processes and authorities must be developed.
3) For KSA critical infrastructures, information must be developed that will assist in developing analysis and identification of known issues and gaps in policies, procedures and practices, as well as incentives affecting infrastructure preparedness and resilience.

4.6.3.1.4 Measures of Progress

1) Continuous monitoring will be measured by the ability of system owners to provide system related risks that will feed up to the top of each ministry.
2) Policies and procedures to cost-effectively reduce information technology security risks to an acceptable level will be implemented, which will, in turn, will be measured through structured reporting.

4.6.3.2 Objective A-2: Baseline Security Standards

Develop a minimum baseline IT security standard for internationally accepted security configurations. This provides the standard that trained information security professionals can use to produce and conduct assessments, audits and certifications, as well as accreditation of existing and new systems.

4.6.3.2.1 Approach

Provide a minimum baseline security standard that establishes and defines the approved configuration documentation for a system at a milestone event or at a specified time. Configuration baselines represent:

- Snapshots that capture the configuration or partial configuration of a system at specific points in time
- Commitment points representing approval of a system at a particular milestones in its development
- Control points that serve to focus management attention

4.6.3.2.2 Implementation Initiatives

1) Baseline Inventories and Configurations

Establish and maintain baseline inventories and configurations of organizational information systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.

2) Security Configuration Settings

Establish and enforce security configuration settings for information technology products employed in organizational information systems.

3) Reviews and Update of the Information System Baseline Configuration

Establish reviews and updates of the baseline configuration of the information system at specified intervals, whenever required by defined events and as an integral part of information system component installations.

4) Automated Maintenance Mechanisms

Employ automated mechanisms to maintain an up-to-date, complete, accurate and readily available baseline configuration of the information system.

4.6.3.2.3 Challenges and Issues

1) Creating an enterprise asset database with systems and data about the systems is challenging to conduct at the national level because of the daunting amount of data and the need to develop a culture of trust among all participating entities.
2) Automating baseline configurations on an enterprise level from the ground up is a major undertaking.

4.6.3.2.4 Measures of Progress

1) Establishment of a configuration baseline for identified major platforms
2) Establishment of a baseline reporting system

4.6.3.3 Objective A-3: Assessment and Audit Framework

Establish an assessment and audit framework to ensure the security and confidentiality of system records and information, to protect against any anticipated threats or hazards to the security or integrity of such records and to protect against unauthorized access to or use of such records or information.

4.6.3.3.1 Approach

NISE Provides the certifier and accreditor with a structured process to perform a Certification and Accreditation of a system, based upon a series of standardized assessment and planning templates. (Templates for system security plans and system risk assessments are provided in the supplement section.)

4.6.3.3.2 Implementation Initiative

1) Develop Templates

Develop IS assessment and audit templates, which are based on the principles of ISO 27001, 27002, ITIL and Control Objectives for Information and Related Technology (COBIT).

4.6.3.3.3 Challenges and Issues

1) C&A will require each KSA ministry to develop, document and implement a ministry-wide information security program to support the confidentiality, integrity and availability of ministry operations and assets.
2) Each organization must document and provide evidence to executives and auditors that appropriate plans and controls are in place, tested and monitored for effectiveness.
3) C&A is a labor intensive, complex and costly process that challenges even the most efficient organization.

4.6.3.3.4 Measures of Progress

1) Establishment of draft audit templates

4.7 National Cooperation and Sharing for Information Security

This element of the NISS explores new processes to enhance internal coordination procedures. In order for any country to realize the goal of becoming an information-secure society, all components of the nation must work cooperatively toward a set of common goals. Achieving this across the many sectors of the Kingdom will require new internal cooperation and coordination processes. Current information security efforts are uneven between different ministries, across critical infrastructures, the private sector and among the people.

In discussions with many nations across the globe, one of the essential requirements identified to achieve an effective national approach to information security was the need for close and focused internal coordination and communication processes. Experience has demonstrated that a country can develop more uniform policies and emergency response procedures when all facets of the government and private sectors work in a cooperative manner. This is especially true for information and cyber security, where standardization, coordination and agility are vital components of a world-class capability.

The approach to increase internal cooperation and information sharing is simple. The NISS focuses its recommendations on specific sectors and specific issues that should form the basis of improving national information sharing and coordination. Finally, this section proposes the creation of a program that will both further enhance and test national information sharing initiatives, especially during crises. Detailed objectives, approaches and initiatives for this element are described below.

4.7.1 Element Description

The national information security or cybersecurity strategies of many nations have identified as key goals better cooperation and coordination between government sectors and between the government and private sectors. Each ministry has unique capabilities, authorities, responsibilities and sector insights that, when brought together in a collaborative manner will make the Kingdom stronger and create a more secure environment to execute government operations and conduct business.

One example where internal information sharing processes were effective is the case of Estonia. One of the keys for success in combating the Estonian cyber-attacks during May 2007 was the continuous cooperation between the executive, civilian, national security, and private sector communities within Estonia. Denmark is another example of a national coordination process that includes both multi-ministerial components and the telecommunications sector.

When combined with the other strategies outlined in the NISS, and executed through the implementation initiatives outlined below, the Kingdom can also achieve this national imperative.

4.7.2 Relationship to Kingdom's Top ICT Objectives

The Kingdom has already identified many goals, such as those outlined in the *Ninth Development Plan*, the *National Communication and Information Technology Plan*, the *Long-term Strategy 2024* and other strategic national documents and initiatives. Through these documents and initiatives, the Kingdom has set the foundation for its vision and ICT direction, creating opportunities to develop the IT industry, while being mindful of the need for a strong security foundation.

4.7.3 Element Objectives

The objectives outlined below are intended to enhance the Kingdom's governmental and private sector coordination process, to identify specific areas for improved coordination and collaboration and to propose a method for testing and evaluation of coordination processes.

4.7.3.1 Objective N-1: Enhance Information Sharing Capabilities

Enhance information sharing capabilities of the following principal interfaces:

- Ministry-to-Ministry

- Government Sector-to-Private Sector
- Government-to-People

4.7.3.1.1 Approach

The approach to achieve this objective is to create new coordinating positions and collaborations to facilitate the sharing of information, including cybersecurity information.

4.7.3.1.2 Implementation Initiatives

1) Ministry-to-Ministry

In this section the term Ministry-to-Ministry refers to any of the Kingdom's governmental organizations.

The NISS proposes the creation of two new coordination bodies – a Chief Information Officer (CIO) Function and a Chief Information Security Officer (CISO) Function. The CIO Function is intended to be a forum where government ministries can address emerging IT issues, which will allow each ministry to discuss and coordinate common concerns and challenges, to receive insight into potential solutions and capabilities and to leverage the knowledge of each ministry. Such collaboration will result in the development of a set of best practices and standards that will lead to reduced costs and better efficiencies.

The CISO Function will focus more specifically on ICT security threats to information systems and cybersecurity matters. The CISO Function will be a critical capability to ensure ministries are aware of new threats being detected within the Kingdom. The CISO will facilitate the transfer of threat information, while being a resource for each individual ministry to gain knowledge on how to address or mitigate threats.

By establishing these two national level Functions, the Kingdom will ensure it has the processes in place to smartly grow and protect its governmental IT systems. The exact composition and charter for each Function will be determined during the implementation phase of the NISS. However, a suggested organizational structure is the NISE described in section ***4.1 Information Security Environment***.

2) Government Sector-to-Private Sector

Government-Private partnerships are a critical step in the evolution of a national strategy to address information and cybersecurity at the national level. These partnerships must occur at both the national level and within all regions of the Kingdom. Section ***4.4 National ICT Infrastructure*** identifies models that have succeeded elsewhere and recommends a national strategy be developed. The NISS approach is to leverage the work already being done within some sectors, for example energy and banking, and to extend the outreach to other critical sectors with more involvement from the regional governments. This will require new processes to encourage collaboration between regional governments and industries, to develop trust and a true partnership, to minimize costs and to achieve the goal of a more secure national economy and infrastructure.

The NISS recognizes that additional collaboration opportunities must be created between the government and private sectors at both the national and regional levels. The national government should create information sharing mechanisms to collaborate with local industry on security issues facing industry, collect specific threat information detected by industry and provide national threat and policy guidance to industry. The exchanges should be based on trust and established on a regular periodic basis for maximum benefit.

3) Government-to-People

The third area for cooperative focus is informing the public about home and individual user responsibilities for information security. Home users are often the most vulnerable, which has led to infected digital devices, theft of personal information by cyber criminals, attacks launched from compromised home systems and theft of financial data and banking information.

The NISS proposes tying public outreach with several other new initiatives under the NISS. First, is a public outreach program run by the proposed National Information Security Environment (NISE). This organization will create an office responsible for public outreach and awareness. Next, the new national information security training initiatives, detailed in section ***4.5 Human Resource***, will teach schoolchildren about information security and cybersecurity and how to behave responsibly on the internet. Lastly, a sub-component of the National Cyber Exercise Program, described in section ***4.7.3.3 Objective N-3*** below can involve local training and exercises in which citizens can participate. By unifying these efforts for public training and awareness, the Kingdom can become a global leader in addressing the difficult problem of bringing cybersecurity into the home.

4.7.3.1.3 Challenges and Issues

1) Inadequate or non-existent coordination processes
2) Uneven security requirement development processes
3) Inadequate threat and vulnerability detection and information sharing mechanisms
4) Different ICT security standards and policies
5) Stovepipes between sectors
6) Uncoordinated or undocumented authorities and responsibilities

4.7.3.1.4 Measures of Progress

1) Creation of the position of CIO across the ministries and implementation of the CIO Function
2) Creation of the position of CISO across the ministries and implementation of the CISO Function
3) Creation of Public-Private Advisory Functions (PPAF) within each region
4) Establishment of an office responsible for Public Outreach and Awareness within the new Information Security Organization

4.7.3.2 Objective N-2: Focus National Cooperation and Coordination

Enhance the following information sharing areas that require inter-governmental structures and processes for cooperation and coordination:

- ICT Security Standards and Policies
- Research and Development (R&D)
- Security Operations Center (SOC)
- Vulnerability and Threat Information Sharing
- National IS Incident Response Process

4.7.3.2.1 Approach

In addition to the Functions recommended in Objective N-1 above, the NISS identifies several specific areas of cooperation that will greatly enhance national and organizational information security efforts. By focusing on the topics of this objective first, the Functions will achieve more rapid and uniform standards and capabilities.

4.7.3.2.2 Implementation Initiatives

1) ICT Security Standards and Policies

NISS section ***4.2 Policy and Regulations*** addresses the creation of new IT security policies and laws. The CIO and the CISO will play vital roles in deciding what new standards and policies should be adopted, how they should be written, to whom they apply and when they should be updated or discontinued. Many policies will be created by the national information security functions that will be applicable to the national security sectors, so their unique perspectives, insights and participation are necessary.

2) Research and Development (R&D)

It is vital for the Kingdom to further develop its own domestic capabilities in the area of ICT and cybersecurity. This will help grow a domestic industry vital to the security of the nation and create exciting job opportunities for university graduates. In order to achieve this result, research and development activities require additional focus and oversight.

Creating a technology roadmap for research is one way of beginning this effort. Led by research centers with requirements inputs from both the civil and national security communities, the roadmap will shape the future research activities in information security for the Kingdom. In addition, creating a centralized funding advisory capability for research will ensure the roadmap is implemented in accordance with strategic goals and requirements.

To this end, the NISS proposes the creation of a Research and Innovation Function that will, in coordination with King Abdulaziz City for Science and Technology (KACST), have oversight of a program to provide research grants and funding for specific security developments.

3) Vulnerability and Threat Information Sharing

Sharing vulnerability and threat information is specifically identified as one area of cooperation that requires special attention. The CISO Function will be one primary mechanism utilized to share this type of information across the government. A Public-Private Advisory Function (PPAF) will be a similar mechanism for industry. KSA's Computer Emergency Response Team (CERT-SA) can also play a role. Finally, the national Security Operations Center (SOC) will be used to share more immediate or urgent threat information. In the past, there has been a reluctance to share this type of information.

However, trusted mechanisms to share the information do not exist. Countries that have overcome these barriers have also had the most success in developing processes to mitigate threats across the government. The NISS recommends that the Kingdom put into place mandatory reporting policies for sharing cyber vulnerability and threat information.

4) National Incident Response Process

No matter how well the Kingdom is prepared to detect and defeat cyber threats, the threat of a large-scale cyber incident within a ministry or across multiple sectors is real. In order to address such threats, the NISS proposes the creation of a National Cyber Response Plan (NCRP). See section ***5.2 Recommendations Outside the NISS Scope But NISS Related***. The plan will include such elements as national coordination responsibilities for the incident, individual ministries and private sector roles and responsibilities, technical analysis and mitigation planning, an alert and notification process, international collaboration and media coordination.

4.7.3.2.3 Challenges and Issues

1) Unclear authorities and responsibilities
2) Potential lack of trust between institutions
3) Competing resources
4) Inadequate existing coordination processes.

4.7.3.2.4 Measures of Progress

1) Effectiveness of the CIO and CISO Functions issuing national ICT security policy and guidance
2) Creation of a NISE Research and Innovation Function
3) Development of a National Research and Development Technology Roadmap
4) Creation of a centralized R&D funding mechanism for ICT security
5) Creation of a national Security Operations Center (SOC)
6) Integration of the telecommunications sector with SOC operations
7) Creation of a policy that mandates the sharing of ICT security threat and vulnerability information

8) Creation of a National Information Security and Cyber Response Plan

4.7.3.3 Objective N-3: Create a National IS and Cyber Exercise Program

Create a National Information Security and Cyber Exercise Program to enhance national coordination and cooperation of activities related to information security.

4.7.3.3.1 Approach

Information security does not belong to one group or sector, but can be felt across all aspects of life in the Kingdom. The NISS is proposing many new responsibilities and capabilities for information security throughout the Kingdom. In order to achieve the maximum benefits of these capabilities they must be tested through simulated cyber exercises. The final strategic objective in the NISS to enhance national coordination and cooperation is the creation of a National Information Security and Cyber Exercise Program.

4.7.3.3.2 Implementation Initiative

1) Implementation of IS and Cyber Exercises

This program will test some of the new capabilities and processes created by the NISS and are intended to be flexible. That is, individual exercises can be customized to test and evaluate the entire Kingdom's IS and cyber response capabilities or can be targeted to individual segments of the response process. The types of participants (called players) and processes to be tested are national policy makers and ministries, authorities and responsibilities, coordination processes, technical teams, private sector outreach, citizens, international partners and media.

Many countries have successfully tested and improved their processes by using exercises to evaluate capabilities and improve processes in a cyber-crisis. The Kingdom must quickly develop appropriate responses to such attacks. Creating a national information security and cyber exercise program and integrating it into all sectors of society will greatly improve the Kingdom's chances to withstand a significant attack via remote means and involving the Kingdom's ICT assets.

4.7.3.3.3 Challenges and Issues

1) Experienced personnel who have designed and participated in similar exercises are needed.
2) Willingness by government and other sectors to participate realistically in the exercises is mandatory.
3) Specific goals for each exercise must be developed and measured.

4.7.3.3.4 Measures of Progress

1) Creation and execution of the first national IS and cyber exercise
2) Expansion of the program to include additional institutions and players

4.8 International Cooperation and Sharing for Information Security

This element focuses specifically on areas where the broader international community has significant efforts underway and where specific international engagement at the governmental level is required.

Although most national information and cybersecurity strategies identify *international cooperation* as a key objective, very few identify specific goals and objectives. Absent such concrete goals, nations often do not understand how to leverage the benefits that can be derived from effective international cooperation. It is critical that the Kingdom identify specific goals to be achieved through international cooperation and partnerships.

The approach outlined here focuses on building strong international partnerships across an array of organizations and initiatives to strengthen the Kingdom's domestic information and cybersecurity capabilities. In addition, a special emphasis on working with the international community in the area of cybercrime is highlighted. Lastly, the NISS recommends approaches to acquire leap-ahead technologies and training opportunities to enhance domestic information security research and innovation. Detailed objectives, approaches and initiatives for this element are described below.

4.8.1 Element Description

The Kingdom must recognize that information and cybersecurity are complex issues with changing technological and policy components. It is important that the Kingdom work in partnership with the international community in order to achieve success. Our networks reach outside the Kingdom and so too must our processes and relationships. International cooperation and coordination on these complex issues and evolving ICT threats is vital to our nation's information security posture and economic future, as well as the development of a robust ICT infrastructure.

In order to fully realize KSA's goals in information security, we must work more collaboratively, and across a broad range of areas, with the international community. The NISS recognizes that the field of information security and cybersecurity is exploding globally and is a major concern for all nations. The Kingdom can improve its own capabilities through greater participation in, and cooperation with, the many initiatives underway around the world. Other sections of the NISS also identify areas where the Kingdom can benefit from greater international partnerships and collaboration.

4.8.2 Relationship to Kingdom's Top ICT Objectives

Cabinet Resolution No. 82 has identified several recommendations that address the need to combat cybercrime. In addition, other national strategies recognize the need to work with the international community and experts to improve the Kingdom's ICT security posture. A comprehensive international engagement strategy and information-sharing plan must be created in order to effectively and efficiently work with the international community.

4.8.3 Element Objectives

The NISS addresses the challenges of working cooperatively with the international community by identifying the leading international organizations that should be engaged, specific areas of international cooperation and different mechanisms to interact with other countries. The NISS calls for critical cooperation between involved ministries and it positions the Kingdom to implement an international engagement strategy that will enhance our information security posture. The objectives outlined below frame the international engagement strategy required to achieve our national information and ICT security goals.

4.8.3.1 Objective I-1: Strengthen the Kingdom's National Technical Capabilities

Strengthen the Kingdom's national technical capabilities through increased international cooperation and sharing.

4.8.3.1.1 Approach

The Kingdom must leverage the international community to advance its own efforts in the fields of information and cybersecurity. To accomplish this, it must position itself to take full advantage of opportunities to learn and acquire the appropriate capabilities for its needs, based on targeted outreach to international partners.

4.8.3.1.2 Implementation Initiatives

1) Phase I

Information gathering and sharing occurs across a wide variety of international organizations. Some are focused on specific topics, while others are much broader in scope and purpose. The NISS recognizes that new efforts are continually being created and the following list is not exhaustive, but rather representative of leading international efforts. Although some are regionally organized, and direct KSA participation may be limited, their outcomes often have global impacts on information security and cybersecurity standards and processes. In *Figure 4.8-1 International Organizations Involved in Information Security and Cybersecurity*, the leading international organizations are arranged in alphabetical order.

- Asia-Pacific Economic Cooperation (APEC)
- Association of Southeast Asian Nations (ASEAN) Council of Europe
- European Network and Information Security Agency (ENISA)
- European Union (EU)
- Forum of Incident Response and Security Teams (FIRST)
- Group of Eight (G8) (Cybersecurity/Cyber Crime)
- Gulf Cooperation Council (GCC)
- Institute of Electrical and Electronic Engineers (IEEE)
- International Electrotechnical Commission (IEC)
- International Organization for Standardization (ISO)
- The International Telecommunication Union (ITU), SG-17
- International Multilateral Partnership Against Cyber Threats (IMPACT)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Engineering Task Force (IETF)
- The Internet Governance Forum (IGF)
- INTERPOL
- Meridian
- North Atlantic Treaty Organization (NATO)
- The Open Group
- Organization for Economic Cooperation and Development (OECD)
- United Nations (UN)

Figure 4.8-1 International Organizations Involved in Information Security and Cybersecurity
Their efforts often have global impacts on information security and cybersecurity standards and processes.

Some KSA government elements are directly involved with these organizations today. However, a comprehensive and systematic approach to gain required knowledge and expertise must be initiated. The NISS recommends a top-to-bottom review and assessment of current engagement activities, appropriate ministerial involvement, strategic goals and objectives and a strategy to improve awareness, effectiveness and engagement of the myriad of policies, standards, information and outcomes from these organizations.

2) Phase II

Phase II activities include direct government-to-government interactions and information sharing activities. Phase II government engagements are intended to focus on very specific information security needs. Due to the nature of these interactions, sensitive or even secret information may often be exchanged. These engagements are integrated into larger national goals and objectives and will usually be achieved by the following mechanisms:

- Bi-lateral information sharing agreements
- Multi-lateral information sharing agreements
- Regional information sharing forums or agreements

Many countries have collaborated with key allies to significantly enhance their national cyber defense and information security postures. That is the key goal of these Phase II relationships. In order to mature the Kingdom's ability to withstand national level cyber-attacks, protect its citizens from the consequences of these attacks and further integrate technology throughout all levels of our society, targeted engagements with specific countries are required.

The greatest benefit to be derived from these types of agreements is the enhancement of the Kingdom's own defenses through the acquisition of unique capabilities and access to international experts, indications and warnings of new threats and mitigation strategies, threat awareness, incident response and mutual defense activities. Inter-ministerial participation in these engagements will reduce burdens on key technical experts and provide more breadth of experience across many domestic ministerial authorities and capabilities.

Formal information sharing agreements between governments, while initially not easy to obtain and execute, are one of the strongest mechanisms for securing the Kingdom's expanding IT and cyber infrastructure.

4.8.3.1.3 Challenges and Issues

1) International engagement in cybersecurity first requires national coordination. Effectively sharing information between ministries remains a challenge unto itself.
2) Similar to internal information sharing, external information sharing relies on trust.
3) National interests are key factors in what types of information are shared. The Kingdom must be able to identify what information of value it is seeking to acquire and share with international partners.
4) This is an area of cooperation that must be developed over the long-term, as these relationships take several years to develop and mature.

4.8.3.1.4 Measures of Progress

1) Establishment of a working-level international information security and cybersecurity forum to inform other government ministries of activities, outcomes and strategies for international engagements
2) Review participation in, and awareness of, international organizations involved in information security and develop a comprehensive engagement strategy
3) Establishment of negotiated international information sharing agreements with strategic partners

4.8.3.2 Objective I-2: Combat Cybercrime

Combat Cybercrime.

4.8.3.2.1 Approach

The detection and limitation of cybercrime has been one of the few unifying international issues upon which most nations have agreed. It is, therefore, deserving of its own specific listing as one of the international objectives for the Kingdom. By quickly aligning itself with international standards and capabilities to detect and respond to cybercrime, the Kingdom helps protect the Saudi government and economy from cybercrime and fraud.

4.8.3.2.2 Implementation Initiative

1) Assessment of Current Efforts to Align With International Cybercrime Activities

The NISS makes an important distinction between internal cybercrime laws and procedures and the requirements necessary when dealing with these issues at the international level. In order to effectively operate on the international cybercrime stage, the Kingdom may need to forego a rigid interpretation of its own legal standards and procedures and adopt a more flexible legal approach to work cooperatively with international partners.

However, the cornerstone of working internationally in cybercrime is to have national laws and procedures to combat cybercrime. Fortunately, as far back as 2007, the Council of Ministers created the first national cybercrime law named the Anti-Cyber Crime Law. The Anti-Cyber Crime Law identifies specific illegal activities and outlines punishments associated with various illegal activities. With this law, and subsequent rulings and enhancements, the Kingdom has achieved the first necessary step in working internationally to combat cybercrime.

The Council of Europe created the Convention on Cybercrime in 2001 that has been signed by nearly 50 nations and is the de facto standard on international cybercrime cooperation. However, many developing countries now wish to re-open the international cybercrime debate and standards by creating a broader internationally developed policy or treaty. The Kingdom must continue to engage this issue on the international stage and assess whether it should align itself with and ratify the Convention on Cybercrime or wait to develop a new international cybercrime document. The outcome of this legal assessment, and KSA's decision, will have impacts on national laws and capabilities.

4.8.3.2.3 Challenges and Issues

1) Domestic and international, as well as legal and cultural challenges arise when dealing with cybercrime and the interpretation of legal standards, procedures and law. Domestically, Sharia law can be applied to some forms of cybercrime. However, on the international stage, this will be more difficult. Therefore, it is imperative that the Kingdom engage in the international discussion of cybercrime, understand what issues or concerns need to be addressed and develop a strategy to work proactively with the international community in this area.

4.8.3.2.4 Measures of Progress

1) Creation of a legal forum that focuses on cybercrime issues, both domestically and internationally
2) Development of an international cybercrime engagement strategy
3) Review and ratification of the Convention on Cybercrime, or participation in the dialogue on re-opening the discussion of an international Cybercrime Treaty

4.8.3.3 Objective I-3: Expand Research and Innovation Through International Cooperation

Expand research and innovation through international cooperation.

4.8.3.3.1 Approach

The final focus that the NISS highlights in international cooperation is research and innovation. The primary approach is to undertake activities to grow domestic information security capacity. Outside academic circles, real innovation is being achieved within smaller technology companies. This provides many opportunities for the Kingdom to expand its own domestic capabilities in the rapidly expanding and evolving cyber security and information security community.

4.8.3.3.2 Implementation Initiatives

1) Attendance at Specific Trade Shows and Trade Fairs

Trade shows for information security provide opportunities to view the latest mature technologies in the market, as well as allow attendees to understand what is driving future requirements and needs. The Kingdom needs a strategy to identify which trade shows should be attended, by whom, and how the knowledge gained is fed back into government and private sector research projects on information security. The Kingdom should also consider hosting its own yearly conference to attract the best technology firms to display their offerings, which could increase participation by university students and researchers. The ultimate goal is to have several Saudi companies display their products at leading international trade shows.

2) Investment In, or Acquisition Of, Start-up Companies

Another area that would greatly accelerate and integrate innovation concepts and capabilities with a Saudi brand is investing in new and emerging information security and cybersecurity companies. Within the innovation community and new start-up companies, an infusion of cash is often all that is needed to elevate a great idea into the research and development phases. In addition to the prospect of investing in unproven technologies, potential acquisition of companies, although costly in the short term, is a strategy that could pay dividends to the Kingdom in the long term.

3) Integration and Coordination of Domestic and International Research Efforts

To manage the international research and innovation engagement strategy, the NISS recommends that the NISE's Research and Innovation Function be tasked with examining how to address these research and innovation initiatives. Integrating domestic research work with the international approach will generate additional capabilities and strategic guidance from this proposed board.

4.8.3.3.3 Challenges and Issues

1) Historically, government-to-government cooperation in this area has been difficult, due mainly to the issues involved in teaming on sensitive research.
2) Developing/acquiring a skilled workforce to engage the international community in cutting-edge research
3) Limited access to the world-wide innovation communities for information security

4.8.3.3.4 Measures of Progress

1) Issuance of mandate to the proposed NISE Research and Innovation Function to develop a strategy that addresses the key areas for international information security engagement
2) Identification and participation in leading international conferences, followed by the sharing of results within the Saudi R&D communities
3) Hosting of an international trade show for ICT security
4) Alignment with the innovation community

4.9 RESEARCH AND INNOVATION

The Research and Innovation element of the NISS is a strategy for creating the broad set of processes and capabilities necessary to identify, focus, research, invent, develop, protect and, in some cases, commercialize the unfilled information security (IS) needs of the Kingdom. This element includes the development and support of the human resource necessary to produce the research and development and production, as well as the entrepreneurs and marketers needed to successfully commercialize or place into operation selected technology.

There is a need to identify and frame real world IS problems for the R and D community. Unless there is need, innovation is useless. Some projects need teams with special skills and resources that require coordination across organizations. In addition, there is always a need to increase the number of inventions and patents, along with their utility and potential commercialization. Finally, to increase the commercialization rate of R and D output, more innovation is often needed.

The approach is to identify the macro elements related to the Kingdom's NISS related research and innovation objectives described in this section. In addition, the NISS Supplement contains a description of five specific initiatives that can be started immediately to begin what will become a foundation for the Kingdom's IS related research and entrepreneurial activities. In addition, specialized courses by experienced inventors on research methods, improved patent searches and patenting, advanced workshops and short courses on key areas of IS and cryptography can help stimulate and focus researchers, developers and teams on problems of potentially high payoff.

4.9.1 ELEMENT DESCRIPTION

Successful research and innovation involves an output, which establishes a tangible result no matter how modest. Building upon results in the real world becomes easier, even though the problems become more challenging, because skills, new people and increased experience improve the opportunity for success

The following five specific projects are described and analyzed in detail in the ***NISS Supplement***:

1. Counterintelligence – a mission of vigilance to detect people and actions that seek to harm the Kingdom or its citizens. We believe that a successful counterintelligence activity will require successful completion of five related innovative research efforts. The efforts are very broadly scoped and each one is expected to entail a great deal of planning, research and development effort, and integration to bring the CI activity to fruition and guardianship of the Kingdom’s data against the specific threat of an insider betraying the community trust.

2. Domains of Duty. It has been envisioned that the Kingdom will be linked together by an advanced communications network and will generate, share and use information to advance the Kingdom’s collective value, while providing great benefit to the populace. Subjects using this network and its information resources, databases and data portals will need to be allowed (and also denied) access. Further, there is a need to structure the network and its controls so that granting membership and deleting membership is done in such a way that reinforces the community aspects of a Kingdom-wide information system.

3. Steganography and Steganalysis. Because different steganography techniques are developed at such a high rate and the detection of newly discovered techniques is expected to be very difficult and take significant time, the greatest need for security is a technique that can be used to defeat steganography and not necessarily detect its presence. It is suggested that this is an ideal problem for university researchers to undertake within a security business incubator environment. The approach might be to jam any steganography that is present. This could be done by adding noise to the host elements or by overlaying a known message steganographically. Another valuable feature might be the development of a stenographic-defeating technique that would have a high probability of defeating steganography but not affect legitimate watermarking. The key to this approach may lay with advanced error correction codes.

4. Avoiding Malicious Chips. Two areas are ripe for innovation and research. First, is the question as to whether or not the KSA should invest in building a chip foundry within the Kingdom that is operated by and for the Kingdom's subjects. A foundry, and training the skilled technicians to run it, is a significant undertaking and expense. It is suggested that the question be answered with respect to the necessary scale and complexity of chips that are essential for secure functioning of absolutely critical infrastructure within the Kingdom. It is further suggested that a first foundry effort not be oriented to fabricating, using the most advanced integrated circuit technologies, but integrated circuits that can be modularly combined to provide the critical functions. Such an effort will not result in the fastest, smallest or perhaps most efficient integrated circuits, but the expectation of security may well offset any cosmetic or any performance diminishments incurred.

5. Backup Keying Variable Distribution. Much of the world's electronic security rests on public key cryptography (PKC), a remarkable development within the latter half of the last century. It presents us with the apparent ability of being able to communicate securely over an open channel without any a priori distribution of keying material. The usual method is to establish a common secret quantity between two or more correspondents and then use this common secret quantity to establish a commonly held and commonly used keying variable. Therefore, it seems prudent because of quantum computation for a modern technologically advanced e-network to consider a backup cryptography for securely conducting the nation's business. This calls for continual assessment and planning, as well as appropriately scaled build-out of fallback cryptographic methods.

4.9.2 RELATIONSHIP TO KINGDOM'S TOP ICT OBJECTIVES

The Research and Innovation element of the NISS supports several of the Kingdom's top objectives. These objectives are identified in the boxes below, including the National Science Technology and Innovation Plan, the National Information and Communications Technology Plan and the Ninth Development Plan.

National Science Technology and Innovation Plan (1426)

Fourth Strategic Principle: 2. Directing scientific research and technological development towards securing the strategic requirements of defense and national security[1]

Tenth Strategic Principle: 5. Adopting the mechanisms required for the information security and protection

[1] National Science, Technology and Innovation Policy, Transforming Saudi Arabia into a Knowledge-Based Economy and Society, 2005-2025 , King Abdulaziz City for Science and Technology and Ministry of Economy and Planning, page 10 also at http://www.kacst.edu.sa/en/about/stnp/pages/strategicbases.aspx.

Chapter 4: Follow-Up Mechanisms and Implementation Requirements

National Information and Communications and Technology Plan[2]

1- **Innovation and Creativity:** Innovation and creativity are the main drivers for development and progress. It is important to disseminate and spread concepts that encourage and promote innovation and creativity in the society, in family, school and work environment.

2- **Initiative:** The spirit of initiative proved to have a profound effect on the industrial and commercial progress of developed countries. This has been clearly reflected in the experiences of US and Malaysia. Accordingly, the spirit of initiative should be encouraged and spread in the society, and ways of utilizing this spirit to establish companies and organizations should be sought.

3- **Acceptance of Failure:** Acceptance of failure from an individual or the entity that made the attempt in a positive manner, and from the society at large, is a supporting concept for innovation, creativity and initiation and should be spread and encouraged at the family, school and work environment.

4- **Productivity and Professionalism:** Productivity and competitiveness are two of the main factors that decide the strength of countries' economies and their competitive positions. The individual's productivity and proficiency represent the major units in measuring the productivity and competitiveness of countries. These concepts should be widely disseminated and deepened in the culture of the society.

Ninth Development Plan

2.4.5 Enhancement of Competitive Capacities[3]

Limited number of business clusters, which consist of several industries, companies and institutions, with strong interlinks and interrelationships, leading to intensive interaction that contributes to increased productivity, stimulates innovation, and generates new business opportunities.

The need to promote investment in research, development and innovation, as there is a shortage of specialists in science and engineering, as well as weak linkages between the academic and the business communities.

The general objectives include:

- Moving the national economy to innovation-based competitiveness
- Improving competitiveness of national products in domestic and external markets
- Supporting competitiveness of non-oil exports and increasing their technological content
- Raising the general level of education and training and expanding scientific and technical education
- Intensifying processes of technology transfer, adaptation and indigenization in order to enhance competitiveness and keep pace with globalization of production
- Expanding establishment of business clusters with strong multiple interlinks (forward and backward linkages), and promoting merger of national companies, as well as closer collaboration with foreign companies possessing advanced technologies

4.9.3 ELEMENT OBJECTIVES

The overall approach to the Research and Innovation element is to start with five quite different, but we believe important, research projects as opposed to establishing a massive research and innovation infrastructure. This will parallel some of the on-going initiatives that have not yet been identified.

There are five pillars upholding innovation, whether it is for information security or anything else:

1. Need
2. Support
3. Innovator Reward
4. Innovation Tools

[2] The National Communications and Information Technology Plan, The Vision Towards the Information Society, 1426H, unofficial Translation of the Arabic text, Page 56.

[3] Ninth Development Plan (1431/32 - 1435/36) 2010-2014, Ministry of Economy and Planning, Chapter 2, Page 38-39.

5. Mindset

It is our assessment that the Kingdom has positioned itself well to encourage innovation by developing these pillars, but there are things that can be done to progress faster and to realize the goal sooner.

4.9.3.1 Objective R-1: Expand and Integrate IS Research Infrastructure

Develop a national research and innovation human, technical and commercial infrastructure.

4.9.3.1.1 Approach

The NISS proposes a Research and Innovation Function under the NISE, to initiate some or all of the five specific projects and to identify the on-going information security activities, capabilities and areas needing augmentation or restructuring. Specific initiatives can be created to increase the synergy and critical mass of the information security efforts. King Abdulaziz City for Science and Technology (KACST), universities and research centers should play major role in the Function.

4.9.3.1.2 Implementation Initiative

1) Prioritize and Initiate Some or All of the Five Projects

Prioritize and initiate at least some of the five projects with proper staffing and resources. The projects are described above in section ***4.9.1 Element Description***.

4.9.3.1.3 Challenges and Issues

1) The Arab culture has a unique challenge to address. It is clear that some research and some entrepreneurial activities will not be successful or, if so, perhaps not in the near future. Chapter four of the National Information and Communications and Technology Plan states, "Acceptance of failure from an individual or the entity that made the attempt in a positive manner, and from the society at large, is a supporting concept for innovation, creativity and initiation and should be spread and encouraged at the family, school and work environment."

   To achieve the Kingdom's goals, it is vital that people are not afraid to accept challenging problems or begin new business ventures. The following thought is a powerful one. *On the path to success, one will meet failure. A well-meaning effort should continue with a positive attitude and with course corrections and modifications derived from the lessons learned from the failure.* Something useful has been learned even if it is simply to approach similar problems in a different way.

4.9.3.1.4 Measures of Progress

1) Number of active projects
2) Number of active researchers
3) Number of patent applications filed with the Saudi Arabia Patent Office, the GCC Patent Office, the Patent Cooperation Treaty (PCT) and the United States Patent and Trademark Office (USPTO)
4) Number and size of self-sustaining derivative business ventures

4.9.3.2 Objective R-2: Develop a Review Process for Proposals

Develop an analysis and review capability for research and commercialization proposals.

4.9.3.2.1 Approach

The NISE Research and Innovation Function should develop the independent evaluation process for research and development ideas and possible commercial IS projects. This includes an assessment of the capability of the human resource requirement proposed and available for a successful project.

4.9.3.2.2 Implementation Initiative

1) Establish the NISE Research and Innovation Function.

Establish the National Information Security Environment (NISE) to provide the framework for the NISE Research and Innovation Function.

4.9.3.2.3 Challenges and Issues

1) A primary challenge is to assure independence, objectivity and skill in the evaluation process.

   Providing transparency and feedback to the proposer in the evaluation of the development ideas and projects, in a manner that is independent of the political/social status of the human resource, is one approach to achieving this.

4.9.3.2.4 Measures of Progress

1) Track the success or lack of success of the sponsored entrepreneurial ventures with factors such as (i) time to reach the financial breakeven point, (ii) number of people employed and (iii) gross sales.
2) Measure the analysis and selection of research projects by (i) number of papers published, (ii) number of patent applications, (iii) number of projects that proceed to the development stage and further and (iv) the total amount of outside funding that has been supplied.

4.9.3.3 Objective R-3: Support and Encourage Researchers and Entrepreneurs

Provide appropriate internal and external encouragement to all team members.

4.9.3.3.1 Approach

Create a positive environment of adequate funding, training, mentoring and incentives for those organizations and people engaged in research, development, innovation, commercialization and entrepreneurial activities.

4.9.3.3.2 Implementation Initiatives

1) Publicity Campaign

Produce a major publicity campaign, along with the establishment of the NISE Research and Innovation Function and its mission.

2) Mentor Program

Encourage successful people in the Kingdom to provide assistance and mentoring to the newer members of the human resource.

3) Reward Success

Create a program to highlight people successful in research, development, innovation and as entrepreneurs. Publicize these successes through mass media, but especially within all levels of the educational, vocational and business training institutions, clubs and professional organizations.

4.9.3.3.3 Challenges and Issues

1) Dissemination and penetration of the motivational materials into all Saudi communities, regardless of a community's location and economic standing

4.9.3.3.4 Measures of Progress

1) Conduct the Saudi equivalent of Western focus groups.
2) Develop an on line feedback means to track the change in awareness of, and attitude towards, new research ventures and entrepreneurial initiatives.
3) Measure hits and time spent on online videos of several types, some strictly publicizing the opportunities, others should be of successful, and not so successful, experiences that encourage the acceptance of reasonable risk after careful study of the proposed venture.
4) Incorporate and analyze evaluation criteria incorporated into the web site to collect viewer feedback.
5) Track mentors and mentoring efforts showing (i) the number of mentors, (ii) the number of separate activities being helped and (iii) the number of people enrolled and being supported in the mentoring program.

4.9.3.4 Objective R-4: Adopt Project Planning and Tracking Tools

Adopt project and program planning, management and measurement tools and systems.

4.9.3.4.1 Approach

Establish compatible transparent management information systems for lifecycle project tracking and management. The output is accessible to sponsors and stakeholders.

4.9.3.4.2 Implementation Initiative

1) Standard MIS Tools and Experienced People

Employ the standard MIS tools. However, using experienced people to assist with the initial planning of each project is vital for its success.

4.9.3.4.3 Challenges and Issues

1) Some do not want their progress or lack thereof exposed. In these cases, we suggest they find another profession or field of work.

4.9.3.4.4 Measures of Progress

1) Number of projects using MIS tools and the skill and experience of the various project managers.

4.9.3.5 Objective R-5: Develop a Strong Marketing Capability

Develop a strong marketing capability for the products ready for production.

4.9.3.5.1 Approach

Utilize successful companies within the Kingdom in strategic alliances to market information security products and services.

4.9.3.5.2 Implementation Initiative

1) Utilize Experience of Companies Currently Marketing IS Products within the Kingdom

Identify companies already marketing information security products within the Kingdom and GCC and contract with them to both market products and perform market research for needed products.

Encourage these companies to employ young Saudis in a training capacity.

4.9.3.5.3 Challenges and Issues

1) Information security products can be difficult items to sell. Structure contracts with appropriate incentives, especially in the beginning.

4.9.3.5.4 Measures of Progress

1) The time it takes for this venture to become profitable
2) Value of sales and sales growth
3) Number of persons marketing the commercially viable or operationally deployable IS products and services

5.0 RECOMMENDATIONS

5.1 NISS ELEMENTS AND HUMAN ATTRIBUTES

The NISS is a related set of elements that form an integrated national strategy, as illustrated by the pyramid in *Figure 5.1-1 Elements of the National Information Security Strategy*. The driving force behind the NISS implementation is the Human Resource (HR) component. With development of trust and cooperation from a base of transparency, coordination and collaboration, the implementation is designed to support the Kingdom's short and long-term ICT objectives necessary to achieve a knowledge economy by 2025.

Figure 5.1-1 Elements of the National Information Security Strategy
The strategy's success depends upon the trust, cooperation, coordination and collaboration of the human resource.

5.1.1 NISS FIVE-YEAR IMPLEMENTATION SCHEDULE

Detailed implementation recommendations are in each NISS Element section under Implementation Initiatives. The chart in *Figure 5.1-2 NISS Implementation Five-Year Timeline* shows the project progression for the first five years, and is a top-level summary of the main groupings of NISS Elements, in order of priority to begin implementation of the initiatives.

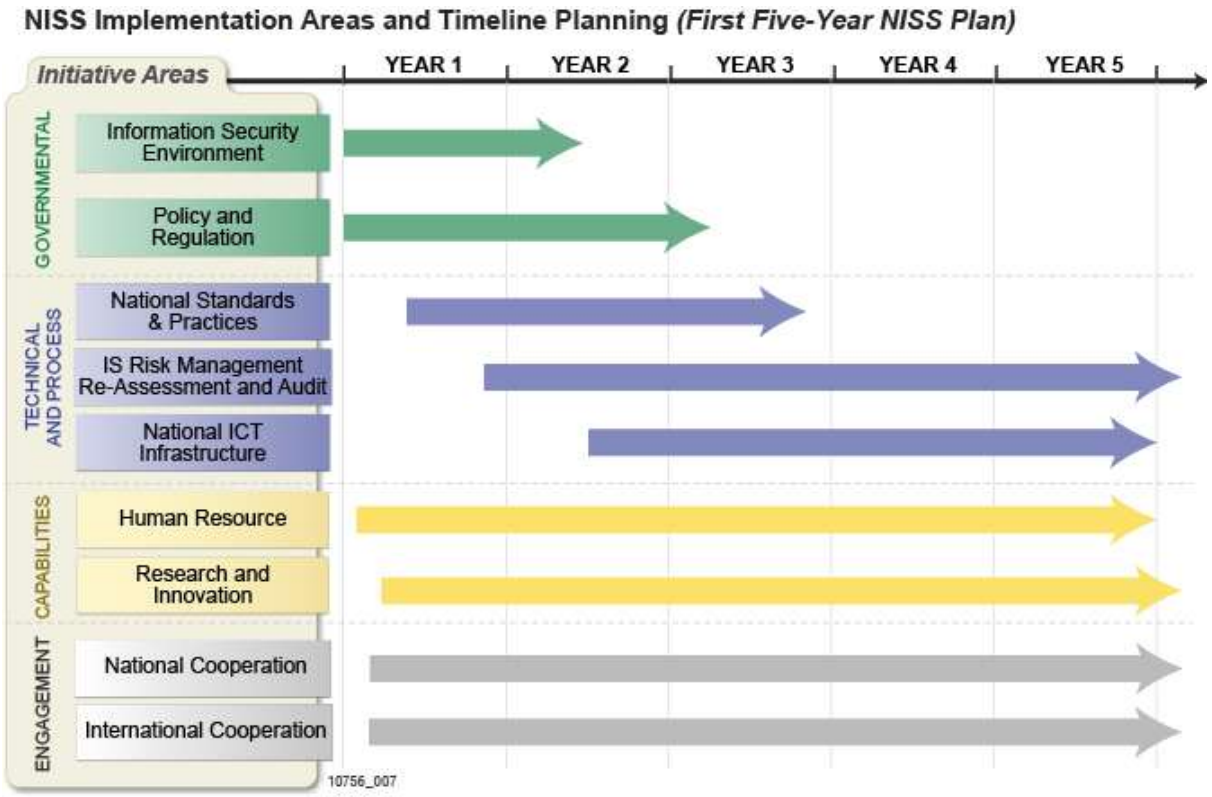

Figure 5.1-2 NISS Implementation Five-Year Timeline
The implementation sequence of the NISS Elements

5.1.2 TOP LEVEL NISS RECOMMENDATIONS

5.1.2.1 Information Security Environment

The first and primary step is consideration and agreement by the Kingdom on a secure and effective Information Security Environment. International research shows that a centrally-managed information security is the most effective and efficient. Because of domestic political factors, few countries are able to implement an effective centralized organization that includes the defense and intelligence sectors. However, most countries have or are working towards a secure and effective national information security and cybersecurity for the protection of all the other ICT infrastructure and information systems. The current ICT environment with borderless infrastructure connectivity makes the threat, vulnerabilities and risk that one organization faces heavily dependent upon actions (or lack of actions) of other entities inside and outside the Kingdom. This is why the traditional model of each organization being responsible for its own information security no longer works. A central national environment with information security oversight, guidance and monitoring of the non-military/intelligence sector on behalf of the entire Kingdom is the best means of minimizing risk and providing maximum assurance against both natural and manmade accidents, disasters, attacks and exploitation. This information security environment shall be responsible for the detailed implementation of the NISS objectives and recommendations.

5.1.2.2 Policies

The next step is agreement for, and development and adoption of, a set of national information security policies. This, in turn, will lead to national standards and best practices. Each ministry agency and organization should have the flexibility to adapt the policies and implement the standards according to their individual circumstances.

5.1.2.3 Regulations

This includes an update of the Kingdom's regulations and laws to take into account the legal challenges presented by the globally interconnected internet. The contents of a person's social network page on such sites as Facebook, Twitter, YouTube or even a personal or organization's website can be subject to unauthorized modification without the knowledge or permission of the owner. Hence, it is possible for someone whose objective is to damage the reputation of a person, organization or the Kingdom to surreptitiously plant false, inflammatory or pornographic information in an account. The defense is to minimize the vulnerabilities by employing good security measures, but ultimately a highly trained group of computer forensic specialists and investigators is needed to avoid falsely convicting innocent persons.

5.1.2.4 Risk Assessment and Management

Risk assessment and the management of risks are necessary since there is no longer an absolute defense against adverse events and attacks affecting information and ICT systems. This is because of today's network interconnectivity and extreme ease of storing and transmitting and transporting (256 GB thumb drives can store 20 million pages of text) sensitive and classified information. A companion to the risk assessment is a framework for ICT system assessments and audits to ensure the appropriate standards and policies are being met.

5.1.2.5 National ICT Infrastructure

The technical infrastructure updating and hardening to a state of acceptable resilience takes longer to achieve but is a vital element of the NISS. Again, the interconnectivity dictates a national architectural framework, since all systems today will suffer successful attacks and/or some degradation due to natural events or accidents or both. Planning and implementing measures to assure a minimum grade of service is both prudent and necessary to achieve the Kingdom's evolution to a knowledge-based ICT economy.

5.1.2.6 National and International Cooperation

Expanding the internal cooperation communication regarding attacks, threats, vulnerabilities, mitigation techniques and best practices among and between the Kingdom's organizations is essential. Today, not every ministry is connected to CERT-SA, which is an obvious starting point, but much more needs to be done as described in the NISS section on National Cooperation. External initiatives with numerous international organizations are needed for any nation, since in many cases immediate mitigation against cyber-attacks depends upon international cooperative actions.

The sharing of information and establishment of a professional dialogue and trust regarding information security and cybersecurity between friendly nations is important. This provides information and cooperative preplanned actions that can improve the national defense from attacks on the Kingdom's ICT systems and infrastructure (such as the electric, water, and petroleum SCADA control systems) and those targeting valuable and sensitive information.

5.1.2.7 Human Resource

The major foundation block of the NISS, after the Kingdom decides upon an information security environment and policy approach is the Human Resource component. The Kingdom has long recognized and supported extensive development of Saudi citizens. The NISS extends this recognition with a specific focus on the areas of IT, ICT and ICT security.

However, the NISS focus is a broader one than just an educational program and is based in part on identifying unemployed work-ready Saudis that could rapidly become important contributors to the needed IT and ICT security workforce. Two groups identified are females and skilled male hackers with no formal degree, but very strong IT and ICT security knowledge. In many cases their capability and knowledge is far beyond what is currently taught in the universities. With appropriate vetting and training, they could provide much needed augmentation to the existing information security work force.

An extensive program to identify, educate and train Saudis for upward mobile information security careers is described. It is based on one major change to a situation that the analysis has identified as a major factor in lack of skilled government IT and ICT security personnel. This situation is in part due to the very great difference in compensation for qualified IT, ICT and ICT security professionals in government positions and in private industry. The proposal is for a special compensatory premium to be paid to Saudis in government purely based on their true capabilities and qualifications in these fields. There should be no distinction based on gender or unvetted paper credentials.

5.1.2.8 Research and Innovation

Research and innovation take longer to bear fruit, but the NISS has identified some initial projects that, in themselves, are valuable but are designed to expand the capability and success rate of researchers, innovators and entrepreneurs.

5.1.3 CONCLUSION

With successful implementation of the NISS Elements, the supporting ICT security foundation should be in place to support the achievement of the Kingdom's Long Term Vision in 2024.

5.2 RECOMMENDATIONS OUTSIDE THE NISS SCOPE BUT NISS RELATED

5.2.1 NISS AND CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

KSA efforts to improve the information security of information and communications technology (ICT) and information systems (the scope of the NISS) are a fundamental and necessary national effort for achieving the Kingdom's long-term national objectives.

Figure 5.2-1 NISS Cybersecurity – CIP Relationships shows the relationship of the NISS to both Cybersecurity and Critical Infrastructure Protection. While all three have elements in common and the NISS has elements unique to each, implementation of the NISS still leaves critical elements of Cybersecurity and Critical Infrastructure Protection unaddressed. Therefore, additional Kingdom strategies for Cybersecurity and Critical Infrastructure Protection must be developed and implemented in coordination with the NISS to cover the areas the NISS does not cover. Collectively, these strategies provide the comprehensive and integrated efforts for national infrastructures required to support the Kingdom's ICT objectives, which in turn support the Kingdom's national security and economic security objectives. The following figures illustrate this.

Figure 5.2-1 identifies the different areas of the three domains and the overlaps between each pair of domains and the one area common to all three domains. *Figure 5.2.1-2 Examples of Unique and Overlapping Areas for Individual Domains* provides examples of the seven different areas and illustrates why the Kingdom also needs a Cybersecurity Strategy and a Critical Infrastructure Protection Strategy to achieve the Kingdom's long term ICT and other national objectives.

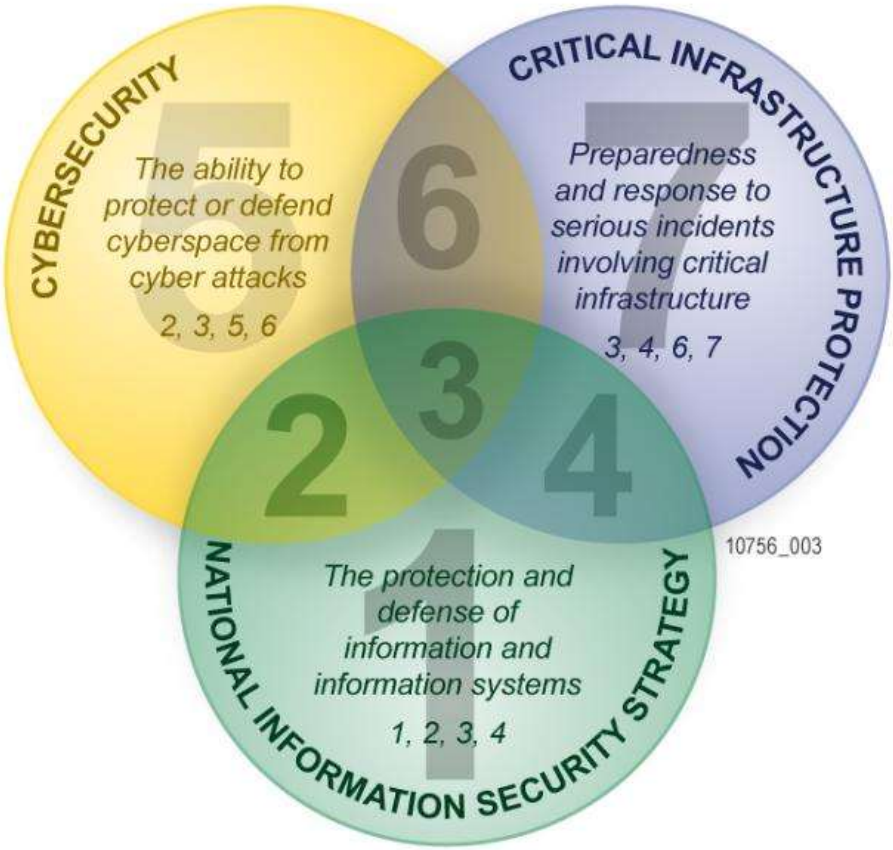

Figure 5.2-1 NISS Cybersecurity – CIP Relationships
The different areas related to security/protection and resilience intersect and overlap (see Figure 5.2-2 for examples).

Examples of Unique and Overlapping Areas from Figure 5.2.1-1		
Area #	**Domain**	**Examples**
1	NISS alone	Computer security and cryptographic policies, directives , guidance and standards for information infrastructure and information systems
2	NISS and Cyber	Cyber threat monitoring, analysis, information sharing, crisis management, computer emergency response team coordination.
3	NISS and Cyber and CIP	Protection of physical and information assets, full threat spectrum resilience and business continuity efforts for information technology infrastructures and operations personnel.
4	NISS and CIP	Risk management assessments and dependency analysis.
5	Cyber alone	National cyber operations center and response capabilities to cyber-attacks.
6	Cyber and CIP	SCADA control system security and response to full spectrum of cyber-based attacks.
7	CIP alone	Protection and response capability against physical attacks to critical infrastructure assets by terrorists.

Figure 5.2-2 Examples of Unique and Overlapping Areas for Individual Domains
These examples illustrate the need for three separate but synergistic KSA national strategies for Information Security, Cybersecurity and CIP.

The important point here is that the NISS covers areas important to both Cybersecurity and CIP. However, the NISS does not address all of the areas to sufficiently cover the security/protection and resilience for these domains. Though Cybersecurity and CIP strategies each have areas in common with the NISS, they must address unique aspects of their individual domains outside the NISS, which will complement the NISS.

5.2.2 RESILIENCE

Another feature that is most often applied to critical infrastructure protection but can be applied to all of the areas above is resilience. This is the ability to anticipate, absorb, adapt to and rapidly recover from potentially disruptive event or failure. (Note resilience is a "system or infrastructure" characteristic, which is a goal to achieve/approach depending on its criticality and type of threats/hazards you want it to be "resilient" against). To maintain and increase the confidence of the general public in the growing number of e-government services, the NISS Element of the National ICT Infrastructure addresses resilience from the NISS point of view.

5.2.3 CYBERSECURITY OVERVIEW

Cybersecurity is an increasingly important challenge faced by the Kingdom. Many of the core systems that underpin the economy and society are now enabled by information technology. While this has created tremendous benefit in terms of efficiency, it has also necessitated a more systematic approach to identifying and thwarting cyber-attacks and cybercrime. As the Kingdom's cyber infrastructure is threatened, we will need to move quickly – both bilaterally and with private sector owners of critical infrastructures. The Kingdom needs to respond jointly and effectively to any attack and that takes expertise, preparation and cooperation. Achieving a cyber-resilient ecosystem is essential.

Cybersecurity is the newest and unique national security issue of the 21st century. The shift from traditional hacker-based cyber-attacks to the use of offensive cyber weapons is the new reality. The potent nexus between threat and vulnerability makes it imperative that traditional information security strategies are enhanced but also transformed to a more resilient cyber security methodology.

A recent report by Security and Defense Agenda, "Cyber-security: The vexed question of global rules: An independent report on cyber-preparedness around the world" (dated February 2012) assesses the unprepared state of nations from a cybersecurity standpoint.

According to the above report on page 47:

- 57 percent believe an arms race is taking place in cyberspace;
- 36 percent believe cybersecurity is more important than missile defense;
- 43 percent felt that damage to critical infrastructure was the greatest threat cyber-attacks posed, with massive economic consequences; and
- America, Australia, the United Kingdom, China and Germany rank behind less populous countries when it comes to cyber-readiness.

The report noted an interesting paradox in the area of national cyber health. The largest countries with the most sophisticated internet access are the most at-risk but also are the most "cyber literate," and thus the best prepared to react if attacked. Countries with less sophisticated internet connections generally are less vulnerable to cyber attacks.

Every day Gulf Cooperation Council businesses are targeted by nation-state actors for cyber exploitation and theft. This consistent and extensive cyber looting results in huge losses of valuable intellectual property, sensitive information, and jobs for the Kingdom. Many of the same vulnerabilities used to steal intellectual property can also be used to attack the critical infrastructures. Without an immediate Kingdom initiative to develop and implement a cybersecurity policy, the Kingdom will continue to be at risk for a catastrophic attack to the nation's vital networks - networks that power essential services for continuity of national security operations and economic stability.

5.2.4 CRITICAL INFRASTRUCTURE PROTECTION

The KSA has correctly concluded that ICT will be an increasingly important underlying fabric affecting all aspects of a society and will influence its future economic prosperity. How the security and resilience functions of ICT and the information systems supporting critical infrastructures are designed, operated and monitored for threats to their operations within KSA will also influence perceptions of KSA by other nations within the international community, who are also addressing similar issues.

The NISS is focused on the information security efforts essential for protecting ICT, information systems and information. Within today's world, ICT and information systems provide critical functions and services that affect the operations of a nation's national security systems, government organizations, and private enterprises. As operational dependency on the ICT and electronic systems increases, information security risks become more critical. Information security is not only an essential enabling function but it must also provide countermeasures to vulnerabilities that can be exploited. In addition, the implementation of the ICT, information systems, applications and operational processes affects the availability, reliably and sustainably of those "critical" functions and services in the face of disruptive events. One of the overarching goals for the NISS strategy is to provide a strategy and direction for achieving an appropriate and sustained level of ICT security.

Each infrastructure operates within a unique set of requirements and collectively they contribute to national security and economic security at various levels of criticality. Most critical infrastructures, including those that perform national security functions, though generally fewer in number, perform and support the most important and fundamental role a government must exercise; namely, assuring national sovereignty and protection of its people. Government functions and services, such as emergency services, are very critical and a variety of Government services are relied upon by its people for essential services and the orderly functioning and economic wellbeing of the KSA. Many private enterprises (but not all) provide some nationally critical operations and services that underpin the effective operations of both government organizations, other private organizations' operations and a vast array of services to the people of KSA; for example, financial services.

It is important that critical infrastructure protection and resilience be considered a separate element of an overall national security strategy. A separate Critical Infrastructure Security and Resilience Strategy (CISRS) for KSA should be developed. It must focus on both the physical protection of key assets and the security of ICT and information systems used within critical infrastructures. Without a comprehensive CISRS, there can be no assurance that infrastructure security and resilience is being implemented and operated commensurate with identified national-level risks and interdependencies. The NISS only addresses the security and resilience needs for ICT and information systems. Though the analysis identified a range of specific independent infrastructure efforts related to technical and organizational infrastructure, there was no evidence of a comprehensive national critical infrastructure protection program.

APPENDICES

A. GLOSSARY OF NISS TERMS AND ACRONYMS

Glossary Term	Definition
Accreditation	Formal declaration by a Designated Accrediting Authority (DAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.
APEC	Asia-Pacific Economic Cooperation
Approval to Operate (ATO)	The official management decision issued by a DAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
APT	Advanced Persistent Threats
ASEAN	Association of Southeast Asian Nations
Asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
Audit	A review of system security (or software security) in order to provide assurance that the system's security posture is adequate. During software development, this term is often used to refer to a code review or to an architectural risk assessment. In an operational environment, auditing refers to a review of security logs or other data collected during on-going monitoring of operations to identify actual or attempted security breaches and to evaluate the quality of a system.
BADIR	BADIR-ICT, Saudi Arabia's first operational national technology incubator
C and A	Certification and Accreditation
Certification	Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
CIC	Critical Infrastructure Council
CIO	Chief Information Officer
CIP	Critical infrastructure Protection - Relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation
CISO	Chief Information Security Officer
CISRS	Critical Security and Resilience Strategy
CITC	Communications and Information Technology Commission
COBIT	Control Objectives for Information and Related Technology
COE	Council of Europe
Critical Infrastructure	System and assets, whether physical or virtual, so vital to KSA that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cyber	Of, or related to, computers and computer networks, such as the internet

Glossary Term	Definition
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks.
Cyberspace	A global domain within the information environment consisting of the interdependent networks of information systems infrastructures including the internet, telecommunications networks, computer systems, embedded processors and controllers
DTMs	Directive Type Memorandums (for time critical issues)
e-NRAF	electronic - National Risk Assessment Function
ENISE	European Network and Information Security Agency
EU	European Union
FIRST	Forum of Incident Response and Security Teams
G8	Group of 8
GANNT	A *Gantt chart* is a type of bar chart, developed by Henry Gantt, which illustrates a project schedule.
GCC	Gulf Cooperation Council
GEA	Government Enterprise Architecture
GSN	Government Secure Network
HR	Human Resource
IA	Information Assurance
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information Communications Technology
ICTS	Information Communications Technology Security
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IMPACT	International Multilateral Partnership Against Cyber Threats
IS	Information Security (The NISS uses the term IS to mean the same as IA)
ISO	International Standards Organization
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
ITNS	Information Technology and National Security Conference Dec 2007
ITU	The International Telecommunication Union
KACST	King Abdulaziz City for Science and Technology
KAI	King Abdullah Institute
KRCs	Kingdom Resident Consultants - The NISS consultants on KAI's Team
KSA	The Kingdom of Saudi Arabia

Glossary Term	Definition
MCIT	Ministry of Communications and Information Technology
MCS	Ministry of Civil Service
MOD	Ministry of Defense
MOE	Ministry of Education
MOHE	Ministry of Higher Education
MOI	Ministry of Interior
MOL	Ministry of Labor
N3i	National Integrated Information Infrastructure
NATO	North Atlantic Treaty Organization
NCDC	National Center for Digital Certification
NCITP	National Communications Information Technology Plan
NCOC	National Cyber Operations Center
NCRP	National Cyber Response Plan
NERC	North American Electric Reliability Council
NISE	National Information Security Environment
NISED	National Information Security Environment Directives (for major issuances)
NISEIs	National Information Security Environment Instructions
NISEMs	National Information Security Environment Manuals
NISS	National Information Security Strategy (for the Kingdom of Saudi Arabia)
NRAF	National Risk Assessment Function
OECD	Organization for Economic Cooperation and Development
PCI	Payment Card Industry
PCT	Patent Cooperation Treaty
PERT	Program Evaluation and Review Technique
PMC	Prince Muqrin Chair
Public (Public Sector)	Saudi Arabia's government or government related organizations
Resilience	The ability to reduce the magnitude and/or duration of disruptive events
RFP	Request for Proposal
Risk Management Framework (RMF)	A structured approach used to oversee and manage risk for an enterprise.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
RMA	Risk Management and Assessment
RPMS	Risk Process management System
SA CISRS	Saudi Arabian Critical Security and Resilience Strategy

Glossary Term	Definition
SCADA	Supervisory Control and Data Acquisition
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.
Security Policy	A set of criteria for the provision of security services. Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Security Test and Evaluation (ST&E)	Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.
SOC	Security Operations Center
STS-51-G	Space Transport System - fifth flight of shuttle Discovery 1985
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline.
TAQNIA	The Saudi Company for Technological Development and Investment
the Kingdom	the Kingdom of Saudi Arabia
Threat	An agent that exploits security vulnerabilities and risks
TOGAF	The Open Group Architecture Framework
UN	United Nations
USPTO	United States Patent and Trademark Office
Vulnerability	A defect or weakness in system security procedure, design, implementation, or internal control that an attacker can exploit.
YEFI	- A unified framework to implement e-Government
Yesser	e-Government Program in KSA

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu