هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

Information Security Policies and Procedures Development Framework for Government Agencies

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

Information Security Policies and Procedures Development Framework for Government Agencies

CERT.sa
المركز الوطني الإرشادي لأمن المعلومات
Computer Emergency Response Team

First Edition - 1432 AH

Contents

Preface

This guide has been developed by the Computer Emergency Response Team – Saudi Arabia (CERT-SA), in the Communications and Information Technology Commission – (CITC), to further its statutory responsibilities under the Council of Ministers Act, that assigns CITC / CERT-SA authority to develop and promulgate information security policies and guidelines, including minimum requirements, that shall assist Government agencies in Saudi Arabia in managing their information security risks.

Chapter 1
Information Security Policies and Procedures Development Framework

Introduction

Although the importance of information security for businesses is increasingly recognized, the complexity of issues involved means that the size and shape of information security policies and procedures may vary widely from Government Agency to Government Agency. This may depend on many factors, including the size of the Government Agency, the sensitivity of the business information they own and deal with in their marketplace, and the numbers and types of information and computing systems they use.

For a large Government Agency, developing a single policy document that speaks to all types of users within the organization and addresses all the information security issues necessary may prove impossible. A more effective concept is to develop a suite of policy documents to cover all information security bases; these can be targeted for specific audiences, making a more efficient process for everyone. This Framework examines the elements that need to be considered when developing and maintaining information security policies and procedures and goes on to present a design for a suite of information security policies and procedures documents and the accompanying development process.

It should be noted that there is no single method for developing an information security policies and procedures. Many factors must be taken into account, including audience type and Government Agency business and size, all of which are considered in this Framework. One other factor is the maturity of the policies and procedures development process currently in place. A Government Agency which currently has no information security policies and procedures or only a very basic one may initially use a different strategy to a Government Agency which already has a substantial policy framework in place, but wants to tighten it up and start to use policies and procedures for more complex purposes such as to track compliance with legislation.

This document presents an overview of the information security policies and procedure development framework developed for Government Agencies in Saudi Arabia.

Information security policies and procedures are key management tools that assist in managing information security risk being faced by an organization. Information security policies and procedures of an organization should be in line with the specific information security risks being faced by the organization.

In recent times, the government organizations in Saudi Arabia have been undergoing significant changes in terms of increasing role of information technology in supporting key business functions, provision of eServices, interconnectivity between government agencies and other organizations and other related aspects. This has resulted in significant increase in the importance of information security Government agencies in Saudi Arabia.

The purpose of this framework is to assist the Government Agencies in Saudi Arabia in development of their information security policies and procedures in quick and effective manner in line with the relevant information security risk being faced by the agencies.

The target audience of this Framework is the Government Agencies in Saudi Arabia. However, the framework can also be used by other public and private sector organizations in Saudi Arabia and Abroad.

The framework has been developed to be used by Information security and/or Information technology functions of the Government agencies that shall use this framework to develop information security policies and procedures for their respective organization.

1. Information Security Policies and Procedures Development Guide for Saudi Government Agencies

The information security policies and procedures development is initiated by Government Mandate number (81) – 191430/3/H and all Government Agencies are required to fulfill the minimum security requirements, in line with the relevant information security risk to the organization's information assets.

This development framework has been provided to the Government Agencies as a comprehensive set of guidance and tools that can be used by the management in their efforts to comply with the Government Mandate.

2. Responsibility of Saudi Government Agencies

Each Government Agency in Saudi Arabia is responsible for development of their information security policies and procedures in line with their specific needs.

Government agencies that don't currently have information security policies and procedures shall develop those by using this framework. Those government agencies that already have information security policies and procedures shall be responsible for ensuring that their current information security policies and procedures at least address the applicable policies and procedures presented in this framework.

3. Disclaimer

The information security policies procedure and standards framework has been developed by CITC/ CERT-SA to address its assigned mandate and to assist Saudi Government agencies in managing information security risks faced by them.

Each Government Agency is considered to be responsible itself to implement the framework and ensure required compliance. CITC/ CERT-SA do not have any responsibility of any Government agencies' non –compliance with this framework.

Further, it should be noted that policies, procedure and standards in this framework address the minimum security controls for specific risk level of information systems[1]. Each Government Agency is responsible for complying with the stated minimum security requirements and defining additional controls in line with specific information security risks to their information assets. CITC / CERT-SA do not bear any responsibly of non-compliance, or lack of mitigation of information security risks at any Government Agency.

[1] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

4. Acknowledgement

Approach to the development of this framework has considered input from a number of related information security international standards, Saudi laws and regulations and similar work done by other Government Agencies and input from Saudi Government Agencies, as listed below:

- US- Federal Information Processing Standards FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems.
- US-National Institute of Standards & Technology NIST PUB 80053--Recommended Security Controls for Federal IS.
- Germany- Federal Office for Information Security (BSI)Baseline Protection Manual.
- ISO/IEC 27001.
- Input for selected Government Agencies.
- Saudi Laws.
- Transaction Law.
- Crimes Law.

5. Need for Information Security Policies and Procedures in Saudi Government Agencies

5. 1. Information Security Policies and procedures Definition

Information security policies are the documented business and technical rules for protecting an organization from information security risk faced by its business and technical infrastructure. These written policy documents provide a high-level description of the various controls which the organization will use to manage its information security risks. The information security policy documents are also considered to be a formal declaration of management›s intent to protect its information asset from relevant risks.

In specific cases, the information security policies are supported by information security procedures that identify key activities required to implement relevant information security policies.

5. 2. System Specific Security Policies

Provide the specific security controls for securing an information system of a particular type.

5. 3. Information Security Procedures

Step-by-step instructions on how to perform a task based on technical and theoretical knowledge.

6. Need for Security Policies

A security policy should fulfill many purposes. It should:

Protect people and information

- Set the rules for expected behavior by users, system administrators, management, and security personnel.
- Authorize security personnel to monitor, probe, and investigate.
- Define and authorize the consequences of violation.
- Define the organization consensus baseline stance on security.
- Help minimize risk.
- Help track compliance with regulations and legislation.

Information security policies and procedures provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to. Information security policies will also help turn staff into participants in the organization's efforts to secure its information assets, and the process of developing these policies will help to define a Government Agency's information assets.

Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

7. Key aspects impacting information security policy needs of Government Agencies

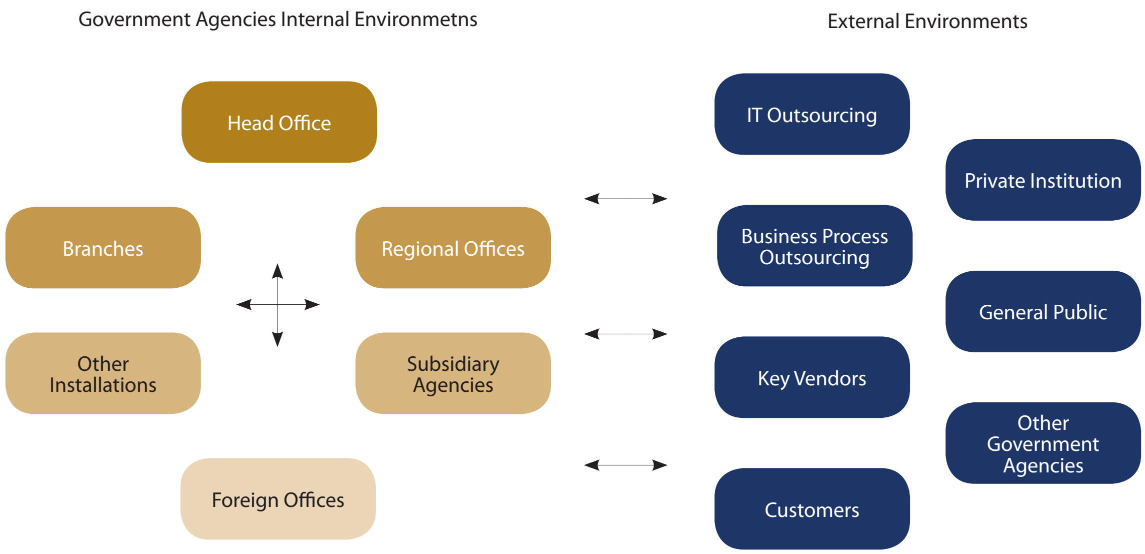
The Government Agencies in Saudi Arabia typically comprise of a large number of business function spread over a number of entities including, Head Office, Branch Offices, Regional Office, Manufacturing Facilities, Subsidiary Government Agencies etc.

As part of its operations, the Government Agencies' entities may capture, process, communicate and store or destroy Information of different sensitivity levels within the organization using various manual or automated mechanisms. A Government Agency is exposed to information security risk if confidentiality, integrity or availability of information handled within its business functions is compromised.

The Government agencies interact with a number of entities in their external environment e.g. customers, vendors, other Government Agencies, business process outsourcing provider (When Government Agency has outsourced its business processes), IT outsourcing provider (When Government Agency has outsourced its IT functions), General Public and others entities.

As part of its business operations, the Government Agencies exchange information with relevant external entities. External entitles may also receive, process, communicate, store or destroy Government agencies information. These activities are performed using various manual or automated mechanisms.

A Government Agency is exposed to information security risk if confidentiality, integrity or availability of information communicated with external entities or handled by external entities (as stated above) is compromised.



Government Agencies Internal Environmetns

External Environments

Hence, the information security risks and corresponding information security policies requirement can vary between different Government Agencies based on their business and technology environment. Some key aspects impacting information security policy requirements are stated below:

- The Organization’s business functions and internal and external relationships.
- The confidentiality, integrity or availability requirements of the information handled within the agency or with external entities.
- The manual and automated mechanisms used to capture, process, store, communicate or destroy this information.
- Other aspects applicable to the Government agencies in Saudi Arabia e.g. laws and regulations with which relevant Saudi Government Agencies are required to be compliant.

8. Approach Used in Developing the Information Security Policies and Procedures Structure

Information security risk applicable to any organization is highly dependent on its business and technology environment. Hence, identifying applicable information security risk and related policy areas for the Saudi Government Agencies requires understanding of related business and technology aspects of the Government Agencies, deriving related key information security risks aspects and based on that identifying key applicable information security policy area.

In order to comprehensively address the information security risks and related information security policy areas and development of appropriate categorization criteria, our approach has considered input from a number of related information security international standards, Saudi laws and regulations and similar work done by other Government Agencies listed below:

- ISO/IEC 27001
- CoBiT
- Saudi Laws
- Input from government agencies
- US- Federal Information Processing Standards FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems
- US-National Institute of Standards & Technology NIST PUB 80053--Recommended Security Controls for Federal IS
- Germany- Federal Office for Information Security (BSI)Baseline Protection Manual

9. Categorization of Information Security Policies Required for Managing Information Security Risks

There are different ways to represent the development of information security policies. Typically, the information security policies are categorized based on their control groups (e.g. Access Control, Compliance, Business Continuity etc) in line with international information security standards such as ISO 27001 (this types is called common information security policies in this framework). There are also specific information security policies to information systems. This framework supports both common and system specific policies information security policies development and considers the following aspects in categorizing the development of information security policies for Government Agencies:

- A repository to assist in developing sample information security policies and facilitate the development of common as well as system specific policies
- The information security needs within the Government Agencies vary in terms of significance of risk faced by them and strength of required policies
- The policies are supposed to address a wide range of audience in the organization. To facilitate their effective communication and implementation, the policies need to identify target audience

Based on the analysis of these factors above, this framework classifies the development of information security policies into:

1. Common Information Security Policies
    a. The common information security policies are categorized based on the Control Group (e.g. Access Control, Business Continuity, Acceptable use Policy etc). The Common Information security policies

address the typical information security risk applicable to most of the organizations. Further, certain Common Policies are supported by procedures to facilitate policy implementation.

   b. The Common Information Security Policies identify the specific group of target audience.

2. System Specific Policies (used to develop risk based system specific information security policies)

   a. The system specific information security standards are categorized based on specific types of systems identified in this document (i.e. Application, IT System, Networking and Physical Infrastructure). These assist the Government Agencies in developing risk based system specific policies for themselves based on the type of information systems being used at the organization and their relevant confidentiality, integrity and availability needs.

   b. Where applicable, the information security system specific policies support maximum three levels (High, Medium and Normal) of information security requirements. It should be noted that the Medium and High Level standards will include the controls of lower level standards of the same system where applicable. The Higher level standards will supplement the lower level standards by adding a few additional controls to the standard of the same system.

10. Key Benefits of the Suggested Categorization Approach

Key benefits of the suggested categorization are stated below:

1. The categorization criteria will support the suggested information security policies and procedures development process:

   a. Policy areas identified as common security policies will assist in establishing the basic security policies quickly and effectively without significant efforts.

   b. System specific policies will assist in developing risk based policies for specific information system.

2. Modular structure of system specific policies provides flexibility and scalability to update/ extend the standards repository with minimum possible efforts:

   a. New types of generic systems specific policies can be added in the existing list of standards.

   b. Standards for vendor specific technologies e.g. Microsoft Exchange Email Server, UNIX Server etc could be added to the existing list of standards. This will supplement the existing generic standards for different types of information assets.

   c. Existing standards could be modified and kept up to date with minimum or no impact on other system specific policies.

3. Identification of target audience in common policies will assist in effective communication of policies to the right audience.

11. Overview of the Framework and its Components

This Framework has been developed to be used by Government Agencies to identify their security needs and to use a risk based approach to develop their information security policies and procedures using the information security policy and standards repositories. This framework provides a flexible approach and is developed to assist the Government Agencies in quickly and effectively developing and implementing their information security policies and procedures. The information security policies and procedures development framework has the following characteristics:

- It provides alignment between the information security policies and procedures that will be developed and the business needs.
- It provides flexibility approach in developing the information security policies and procedures.
- It can be used by Government Agencies with lower or advanced security readiness status regarding information security policies development
- It can be used by Government Agencies having personnel with low or advanced security skills i.e. Does not require very high skilled resources for accomplishing major part of policy development exercise
- It can be used by Government Agencies with low or advanced security requirements
- It saves time and effort

This developed framework also assists in:

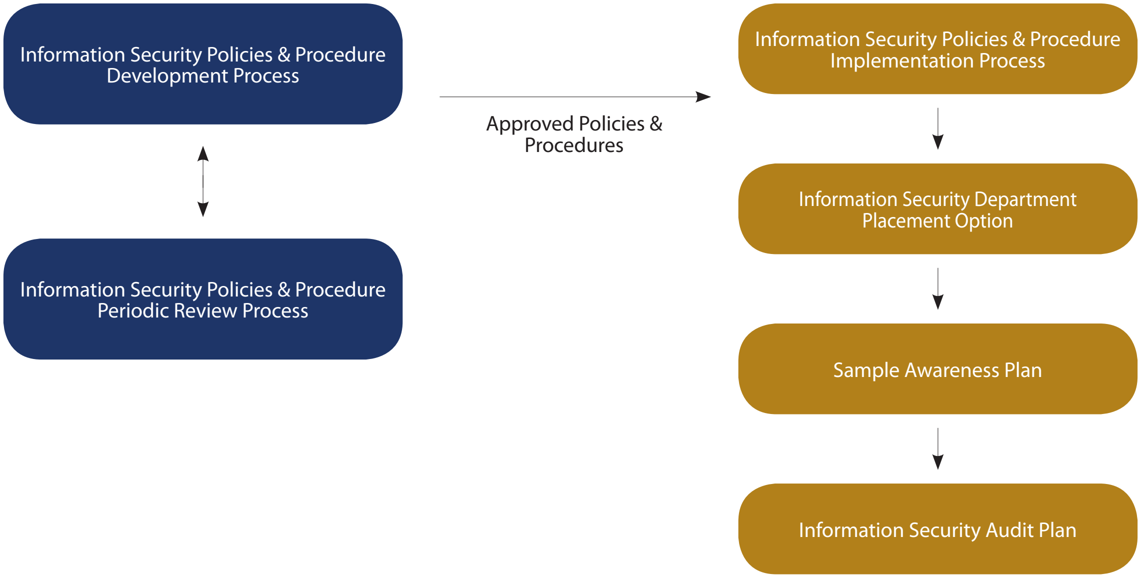
- Planning and developing information security policies and procedures
- Selecting appropriate information security department placement option
- Implementing the developed information security policies and procedures
- Creating awareness on the developed information security policies and procedures
- Identifying and classifying the information systems within the Government Agencies
- Monitoring the integrity and security of the Government Agencies information systems
- Complying with the local legislation and regulations that may have legal implication on the information security of the Government Agencies
- Auditing compliance with the developed information security policies and procedures

12. Framework Components

The developed framework has the following key components that will be used in rolling out the Government Agencies' policies and procedures:

1. Development Process for Information Security Policies and procedures Process.
   a. Repository of Common Policies.
   b. Repository of System Specific Policies.
   c. Repository of Common Procedures.
   d. Information Security Department Placement Options.
2. Implementation of Information Security Policies and Procedures.
   a. Sample Awareness Plan.
   b. Information Security Audit Process.

The following illustration depicts the different components of the Framework:


Information Security Policies & Procedure Development Process
Information Security Policies & Procedure Periodic Review Process
Approved Policies & Procedures
Information Security Policies & Procedure Implementation Process
Information Security Department Placement Option
Sample Awareness Plan
Information Security Audit Plan

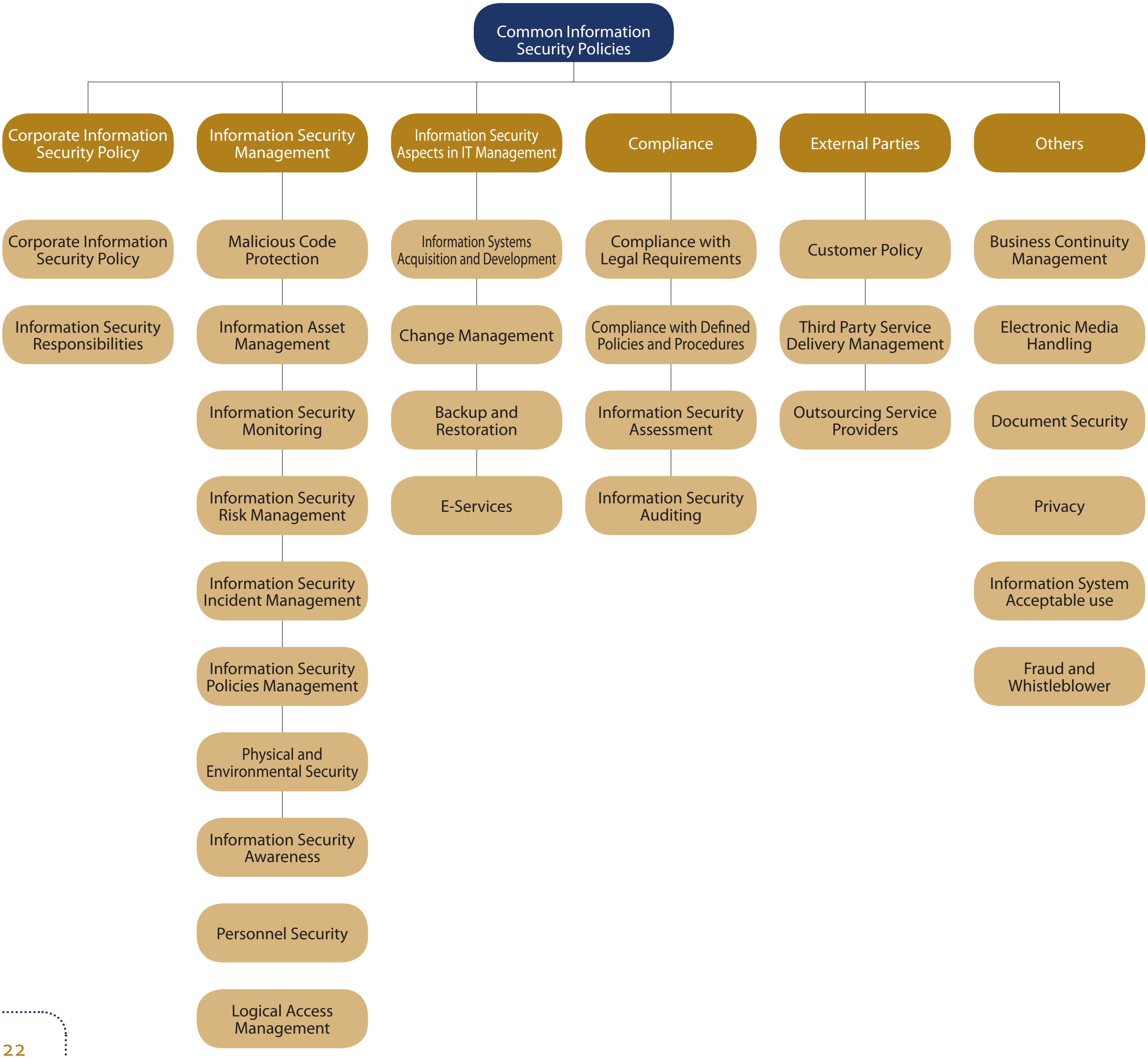
The following sections describe the Framework components and their relation.

12. 1. Development Process for Information Security Policies and Procedures

This process explains the steps used to develop risk based Information Security Policies and procedures. This process uses the sample repositories of the Common Policies and procedures to develop the Government Agencies' risk based policies, standard and procedures. More details about this process can be found in Section B.

12. 2. Sample Repository of Common Policies

A consolidated and categorized list of common information security policies that can impact the information security risk of Government Agencies is depicted in the illustration below:



- Common Information Security Policies
  - Corporate Information Security Policy
    - Corporate Information Security Policy
    - Information Security Responsibilities
  - Information Security Management
    - Malicious Code Protection
    - Information Asset Management
    - Information Security Monitoring
    - Information Security Risk Management
    - Information Security Incident Management
    - Information Security Policies Management
    - Physical and Environmental Security
    - Information Security Awareness
    - Personnel Security
    - Logical Access Management
  - Information Security Aspects in IT Management
    - Information Systems Acquisition and Development
    - Change Management
    - Backup and Restoration
    - E-Services
  - Compliance
    - Compliance with Legal Requirements
    - Compliance with Defined Policies and Procedures
    - Information Security Assessment
    - Information Security Auditing
  - External Parties
    - Customer Policy
    - Third Party Service Delivery Management
    - Outsourcing Service Providers
  - Others
    - Business Continuity Management
    - Electronic Media Handling
    - Document Security
    - Privacy
    - Information System Acceptable use
    - Fraud and Whistleblower

The above common information security policies are described in the table below:

Number	Policies Categories	Policy Areas	Description
1	Corporate Information Security Policy	Corporate Security Policy	This policy aims to communicate the management commitment and key goals for establishing risk based information security controls in Government Agencies.
		Information Security Responsibilities	This policy aims to assign responsibilities for various information security goals and objectives of the Government Agencies and to set the underlying framework for establishing a relationship between the Information Security Department and other IT/Business Functions.
2	Information Security Management	Information Security Awareness	This policy aims to provide the Government Agencies' users the appropriate information security awareness of information security threats and Government Agencies' information security policies, procedures and standards based on their specific needs.
		Logical Access Management Policy	This policy aims to control the logical access to the Government Agencies' information systems thereby ensuring accuracy, confidentiality, and availability of information.
		Malicious Code Protection	This policy aims to protect the Government Agencies' information systems from malicious software (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) into the Government Agencies.
		Information Security Incident Management	This policy aims to ensure that information security incidents related to the Government Agencies' information systems are reported, tracked, investigated and resolved in timely and effective manner.
		Personnel Security	This policy aims to minimize the chances of abuse, misuse, or destruction of the Government Agencies' information systems by verifying the integrity of personnel provided access to its information systems.
		Information Asset Management	This policy aims to ensure that all of the Government Agencies' information systems are identified, assigned to specific owners and appropriately classified considering their relevant nature and information security risk rating that would assist in defining appropriate security controls for them.
		Information Security Risk Management	This policy aims to ensure that the Government Agencies identifies information security risks for its information systems considering the relevant threats and vulnerabilities and corresponding business impact. Further the organization plans appropriate risk mitigation initiatives to address the identified information security risks.
		Information Security Policies Management	This policy aims to maintain and communicate the Government Agencies' Information Security Policies and procedures in accordance with business requirements and relevant laws and regulations in the Kingdom of Saudi Arabia.

Number	Policies Categories	Policy Areas	Description
		Physical and Environmental Security	This policy aims to establish guidelines to prevent unauthorized access and interference to the Government Agencies' premises and information systems and to protect and preserve information systems and human from the exposure to various physical threats that can produce a disruption or denial of information systems services.
		Information Security Monitoring	This policy aims to ensure that information security status of the Government Agencies' information systems is effectively monitored by planning and deploying adequate security monitoring techniques in line with the relevant risk and criticality of the information systems.
3	Information Security Aspects in IT Management	Backup and Restoration	This policy aims to ensure that backup and restoration of the Government Agencies electronic information are planned, and executed in timely, effective and secure manner based on business requirements.
		E-Services	This policy aims to ensure that the Government Agencies address risk to its information systems supporting e-Services based on applicable best practices and relevant Saudi Laws and Regulations.
		Information Systems Acquisition and Development	This policy aims to ensure that security is integrated throughout the whole lifecycle of information systems acquisitions and development in the Government Agencies.
		Change Management	This policy aims to ensure that changes to key information systems are controlled effectively in order to minimize the chances of disruption of IT services or fraud resulting from unauthorized changes to information systems.
4	Compliance	Compliance with Legal Requirements	This policy aims to ensure Government Agencies' compliance with relevant laws and regulations applicable on the organization.
		Compliance with Defined Policies and Procedures	This policy aims to ensure effective monitoring of compliance with the Government Agencies' information security policies and procedures by the Government Agencies Employees and third parties.
		Information Security Assessment	This policy aims to ensure that the Government Agencies perform security assessment on key information systems based on business requirements to identify security weaknesses on those systems and accordingly take appropriate action to resolve such weaknesses.
		Information Security Auditing	This policy aims to ensure that the Government Agencies plan and perform independent information security audits of their information systems in line with their relevant risk and criticality and take timely and appropriate actions to address observations identified as part of the audits.

Number	Policies Categories	Policy Areas	Description
5	External Parties	Customer Policy	This policy aims to ensure that the Government Agencies maintain the security of their customer information and ensure adequate security controls are implemented when providing customers access to their IT services.
		Third Party Service Delivery Management	This policy aims to ensure that the Government Agencies manage information security risk from the third parties serving the organization.
		Outsourcing Service Providers	This policy aims to ensure that the Government Agencies manage the information security risks from outsourcing service providers serving the organization.
6	Others	Business Continuity Management	This policy aims to define appropriate actions to mitigate any interruptions to business activities and to protect critical business processes/services from the effects of major failures of information systems or disasters and to ensure their timely resumption.
		Electronic Media Handling	This policy aims to protect the Government Agencies' electronic media such as (USB Memory, Portable hard disks, input/output Data Media e.g. DVDs, CDs etc) from damage, theft and unauthorized access.
		Document Security	This policy aims to protect the Government Agencies' sensitive documentation from damage, theft and unauthorized access.
		Privacy	This policy aims to maintain the confidentiality and integrity of personal information handled by the Government Agencies.
		Information System Acceptable Use	This policy aims to establish acceptable use rules for the Government Agencies' information systems.
		Fraud and Whistleblower	This policy aims to ensure that fraud or malpractice activities occurring on the Government Agencies' information systems are prevented, reported, investigated and appropriate action is taken accordingly.

For the above selected sample of the information security policies, the sample common information security policies repository:

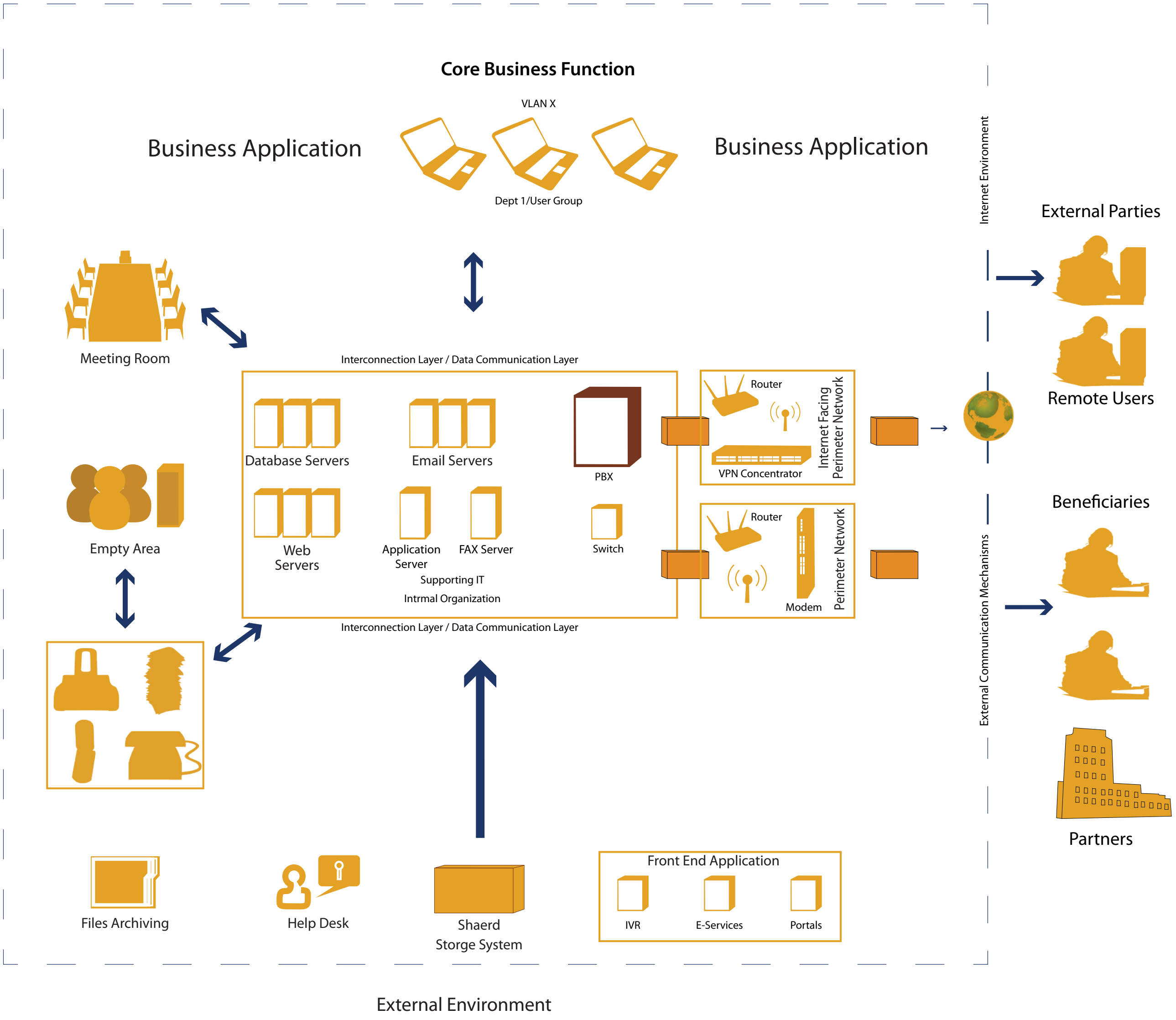
- Has the policy statement(s) required to address risks pertaining to the specific information security policy area
- (Where Relevant) has the procedure(s) required for the developed policy statement

The common information security policies have a number of supporting procedures and are used together with the information security system specific policies and other relevant security best practices to develop the Government Agencies Information Security Audit Programs and the relevant awareness security messages as part of the Awareness Plan.

For further details about the common information security policies, please refer to the Information Security Common Policies Repository.

12. 3. Sample Repository of System Specific Policies

The diagram below presents the Government Agencies' Environmental factors that may impact their information security needs:



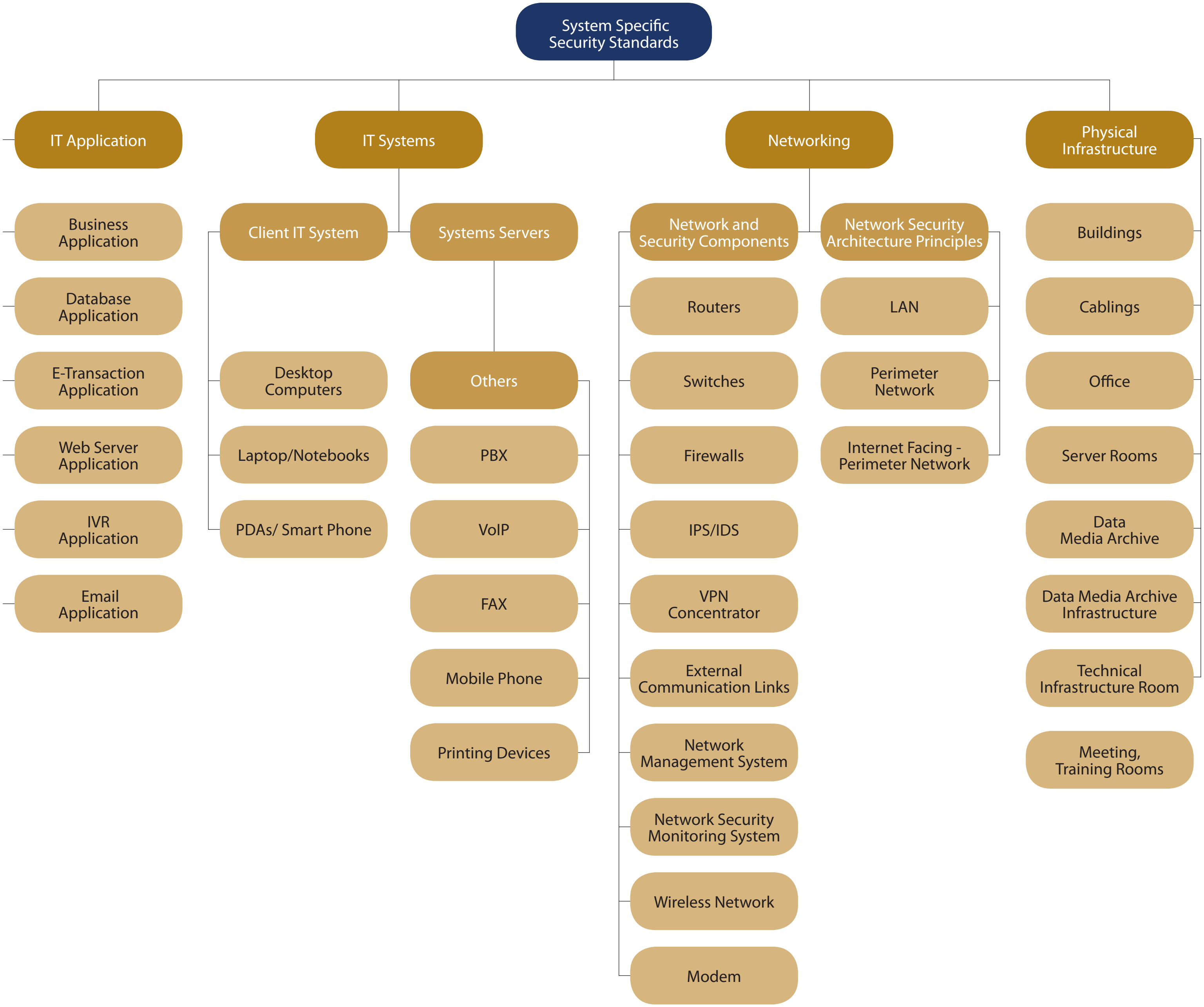
As stated in the illustration above:

- A Government Agency is supported by a set of core and supporting business functions. The business functions capture, process, store, communicate or destroy information as part of their business operations. The confidentiality, integrity and availability requirements of information handled by business functions may vary depending on the business needs.
- Information is handled by business functions:
  - By using automated means e.g. IT Applications that process information related to the business functions.
  - Or using manual methods e.g. Documents, Meetings etc.
  - Or a combination of the above
- Business information is captured and processed by different types of IT Application e.g. Application Servers software, Web Servers software. These applications are supported by IT system infrastructure.
- Information from IT Applications Servers is accessed by users using client application. The client applications would typically reside on client computing devices including Desktops, Notebooks, PDAs, etc.
- Information is stored in Database Servers, client computing devices, Centralized Data Storage/ Backup Mechanisms, Portable Storage Devices etc.
- Information from IT application services are accessed within the Government Agency through the agency's Local Area Network or Wide Area Network.
- IT application services (and supporting information) may also be accessed remotely by using different remote communication mechanisms e.g. Wireless access, Dialup access, Web based access, etc.
- Information may be captured, processed, stored or communicated by other mechanisms. E.g. Documents, Meetings, Telephone system, Fax etc.
- A Government Agency may have one or more IT departments to manage the IT infrastructure supporting its business functions.
- Core IT applications are typically situated at centralized location (Server Room, Data Center).
- A Government Agency may have one of more information security department (within or outside the IT department) to manage the information security aspects.
- The underlying infrastructure also facilitates the interaction process between various stakeholders including customers, vendors, partners, contractors, other Government agencies etc. These entities have different level of access to the Government Agencies information based on their specific role.
- Physical Environmental security aspects of the Government Agencies are normally handled by a separate department e.g. Physical Security Department, Buildings Department.
- The Government Agencies are required to comply with a number of laws and regulations, some of these have information security implications.

The Government Agencies may face information security risk from any of the sources mentioned above if their vulnerabilities are exploited by related information security threats. The information security risks and required information security policies of the Government Agencies can vary based on their type of information systems infrastructure.

Based on analyses of information provided above, the following illustration presents key types of information system involved in capturing, processing, communicating, and storing information in Government Agencies[2]:

[2] These information systems have been defined to enable a large number of the Saudi Government Agencies to map their information systems to them. However, the list can not be all inclusive. It is possible that based on their specific requirements, the Saudi Government Agencies may need additional types of information systems. The suggested approach provides flexibility to add additional types of information systems in future with their own specific risk.



- System Specific Security Standards
  - IT Application
    - Business Application
    - Database Application
    - E-Transaction Application
    - Web Server Application
    - IVR Application
    - Email Application
  - IT Systems
    - Client IT System
      - Desktop Computers
      - Laptop/Notebooks
      - PDAs/ Smart Phone
    - Systems Servers
      - Others
        - PBX
        - VoIP
        - FAX
        - Mobile Phone
        - Printing Devices
  - Networking
    - Network and Security Components
      - Routers
      - Switches
      - Firewalls
      - IPS/IDS
      - VPN Concentrator
      - External Communication Links
      - Network Management System
      - Network Security Monitoring System
      - Wireless Network
      - Modem
    - Network Security Architecture Principles
      - LAN
      - Perimeter Network
      - Internet Facing - Perimeter Network
  - Physical Infrastructure
    - Buildings
    - Cablings
    - Office
    - Server Rooms
    - Data Media Archive
    - Data Media Archive Infrastructure
    - Technical Infrastructure Room
    - Meeting, Training Rooms

For samples of system specific security standards please refer to Appendix III.

For the above selected sample of system specific security standards, the system specific security standards repository:

- Determines the control(s) required to address risks pertaining to the specific while referring to relevant common information security policy.
- Develops the standards statement(s) in line with the identified control(s).

Assigns the CIA level as (High, Medium, Normal) for each standards statement.

Some of the above sample system specific policies are linked with a specific common information security policy. The system specific policies are used together with the common information security policies and other relevant security best practices to develop the Government Agencies Information Security Audit Programs and the relevant awareness security messages as part of the Awareness Plan.

For further details about the system specific security standards, please refer to the Information Security System Specific policies Repository.

12. 4. Sample Repository of Common Procedures

Number	Procedure	Description
1	Information Security Awareness	This procedure identifies key activities to be carried out to develop and implement information security awareness plan.
2	Logical Access Management	This procedure manages user access to Government Agencies' information systems.
3	Malicious Code Protection	This procedure helps in mitigating the information security risks associated with the identified/detected Viruses/malicious code.
4	Information Security Incident Management	This procedure provides the activities for handling security incidents and all related actions including investigation, analysis and follow-up of status of incidents.
5	Personnel Security	This procedure identifies key activities to be carried out to protect Government Agencies' information systems from misuse, or destruction by employees and contractors.
6	Information Security Monitoring	This procedure identifies key activities to be carried out to monitor the integrity and security of Government Agencies' information systems.
7	Information Asset Management	This procedure defines the specific steps that Government Agencies will use to identify its information systems and classify its information systems by examining and determining risks related to these systems.

Number	Procedure	Description
8	Information Security Policies Management	This procedure identifies key activities to be carried out to manage Government Agencies' information security policies and procedures.
9	Physical and Environmental Security	This procedure identifies key activities to be carried out to ensure that necessary controls are in place to reduce the risk of theft and / or damage to information and information systems.
10	Backup and Restoration	This procedure identifies key activities to be carried out to establish the rules for the backup, storage and restoration of the electronic information.
11	Information Systems Acquisition and Development	This procedure identifies key activities to be carried out to ensure that security is an integral part of the information systems.
12	Change Management	This procedure identifies key activities to be carried out to control changes to Government Agencies' information systems in order to minimize the impact of change-related incidents upon service quality.
13	Compliance with Legal Requirements	This procedure identifies key activities to be carried out to monitor local legislation and regulations that may have legal implication on the information security of the organization.
14	Information Security Assessment	This procedure identifies key activities to be carried out to ensure that proper information security controls exist for Government Agencies' information systems (or group of information systems).
15	Information Security Auditing	This procedure identifies key activities to be carried out to ensure that proper information security controls exist for Government Agencies'information systems (or group of information systems) and services/functions.
16	Electronic Media Handling	This procedure identifies key activities to be carried out to protect Government Agencies' electronic media such as (USPs, hard disks, input/output data) from damage, theft and unauthorized access.

All of the above sample procedures are linked with the one of the common information security policies and are used to identify the steps that should be followed to ensure that the related policy statements objectives are met.

For further details about the information security procedures, please refer to the Information Security Procedures Document.

12. 5. Information Security Department Placement Options

The information security organization has evolved over the past several decades with several names, for example, data security, systems security, security administration, and information security and information protection. These naming conventions are reflection of the emerging scope expansion of the information security departments. With whatever naming convention is used within the Government Agencies, the primary focus of the information security organizations to ensure the confidentiality, availability and integrity of the information.

In today's security organizational structure, there is no "one size fits all" for the information security department or the scope of the responsibilities. The location of where the security organization should report has also been evolving a sample Information Security Department Placement Options Document has been provided to assist the Government Agencies which do not currently have an information security department to establish a department based on the principles outlined in the document. Those Government Agencies that already have an information security department should be responsible for ensuring their current information security department responsibilities are inline with Information Security Department Placement Options Document and should consider enhancing their current information security structure using this document as a guide.

The Information Security Department Placement Options Document presents different options for placing the information security department, considering their advantages and disadvantages, within the Government Agencies in Saudi Arabia. The selected information security placement option of the Government Agencies will ensure assigning the roles and responsibilities to relevant personnel/positions as per the selected information security organizational structure for the Government Agencies' information security policies and procedures.

The Information Security Department Placement Options document also includes the Information Security Audit Roles and Responsibilities of the information security audit and implementation follow-up unit (within the security department). This includes the unit's responsibility of performing follow up on the implementation of information security policies and procedures in the Government Agencies as well as conducting continuous audit for them (e.g. annual audit).

For further details about the information security department placement options, please refer to the Information Security Department Placement Options Document.

12. 6. Implementation Process for Information Security Policies and Procedures

When the security policies and procedures are all drawn up, revised, updated and agreed upon, the implementation process should be followed by Government Agencies to implement specific information security policies and procedures, however, this is usually harder than the creation of the policies and procedures, due the fact that at this stage the Government Agencies also need to coach and educate their staff to behave in a «secure» manner, following each of the core elements pointed in the formal security policies and procedures.

A proper implementation requires not only educating the staff on each of the core elements flagged as critical in the formal Security policies and procedures, but also changing their role in the effort to protect the Government Agencies' critical information systems.

Having formalized the Government Agencies' policies and procedures, each Government Agencies should start rolling out their developed policies and procedures using the information security policies and procedures implementation process. The information security policies and procedures implementation process will ensure that the Government Agencies implement the defined gaps against their formal information security policies and procedures. This process works together with the Information Security Awareness provided as part of this Framework.

For further details about the information security policies and procedures implementation process, please refer to the Information Security Policies and Procedures Implementation Guide

12. 7. Sample Awareness Plan

The Security Awareness Program can be defined as one of the key factors for the successful implementation of a Government Agency-wide security policies and procedures. The main aim is to define and outline the specific role of each of the employees in the effort to secure critical Government Agencies' information systems, as well as covering in detail each of the core elements pointed in the information security policies and procedures. The program is aimed at generating an increased interest in the Information Security field in an easy to understand, yet effective way.

The purpose of awareness is to provide staff with a better understanding of security risks and the importance of security to the daily business procedures of the Government Agency.

The procedures document has an information security procedure that provides the Government Agencies with the key steps that the Government Agencies should perform to develop and implement their information security awareness program in addition to the sample information security awareness program provided as part of this Framework.

This developed sample information security awareness program will assist the Government Agencies in implementing the developed information security policies and, and procedures by raising the awareness of its staff with regards to security and its importance. The program includes items like sample messages, means through which these messages are conveyed and frequency of the awareness messages.

For further details about the information security awareness program development, please refer to the information security procedures document and the provided sample information security awareness program document.

12. 8. Change Management Process (Included in the Implementation Guide)

The purpose of the change management process is to provide guidance and mechanisms for facilitating the employees' experiences while Government Agencies transition from current state to the desired future state as per the requirements of the information security implementation process.

The change management process addresses the people side of change associated with the implementation of the information security policies and procedures.

In support of this understanding, the change management process includes elements such as assessing and mitigating risk, building an active and cohesive change management team, managing resistance and communicating with and engaging all stakeholders. In addition, the change management process provides a central point of reference and alignment for all change management and awareness activities throughout the entire implementation of the information security policies standards and procedures.

The developed change management process will support successful implementation of the information security policies and procedures by helping to mitigate the organizational and individual challenges that could impede the implementation.

For further details about the change management aspects of implementing the information security policies and procedures, please refer to the Implementation Guide.

12. 9. Information Security Audit Process

The purpose of the information Security Audit process is to set out a baseline approach to be followed by Government Agencies in:

Planning and communicating their information security audit.

Executing their information security audit.

Reporting and following up their information security audit findings and action points their information security audit.

The procedures document has an information security procedure that provides the Government Agencies with the key steps that the Government Agencies should perform to develop and implement their information security audit in addition to the sample information security audit process provided as part of this Framework.

Having formalized and implemented the Government Agencies' policies and procedures, the Government Agencies should develop and implement their information security audit plan using the provided information security audit process. The developed information security audit programs as part of this process utilize the common and system specific policies sample repositories' controls in addition, to the best practices recommended by the technology vendors and other relevant reputed sources.

For further details about the information security audit process, please refer to the information security procedures document and the provided sample information security audit process document.

Chapter 2
Development Process for Information Security Policies, Procedures and Standards

1. Overview

As building good information security policies and procedures provides the foundations for the successful implementation of security related projects in the future, this is the first measure that must be taken to reduce the risk of unacceptable use of any of the Government Agencies' information resources.

The first step towards enhancing a Government Agency›s security is the introduction of a precise yet enforceable information security policies and procedures, informing staff on the various aspects of their responsibilities, general use of the Government Agency resources and explaining how sensitive information must be handled. The policies should also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of the information security policies and procedures is highly beneficial as it will not only turn all of a Government Agency staff into participants in the Government Agency›s effort to secure its communications but also help reduce the risk of a potential security breach through «human-factor» mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally the building process of the information security policies and procedures will also help define the Government Agency›s critical information systems, the ways they must be protected and will also serve as a centralized document, as far as protecting information systems is concerned.

Government agencies that currently do not have information security policies and procedures shall be responsible for developing their policies and procedures based on the guides lines stated in this document. Those government agencies that already have information security policies and procedures shall be responsible for ensuring that their current information security policies and procedures address the applicable policies and procedures presented in this framework.

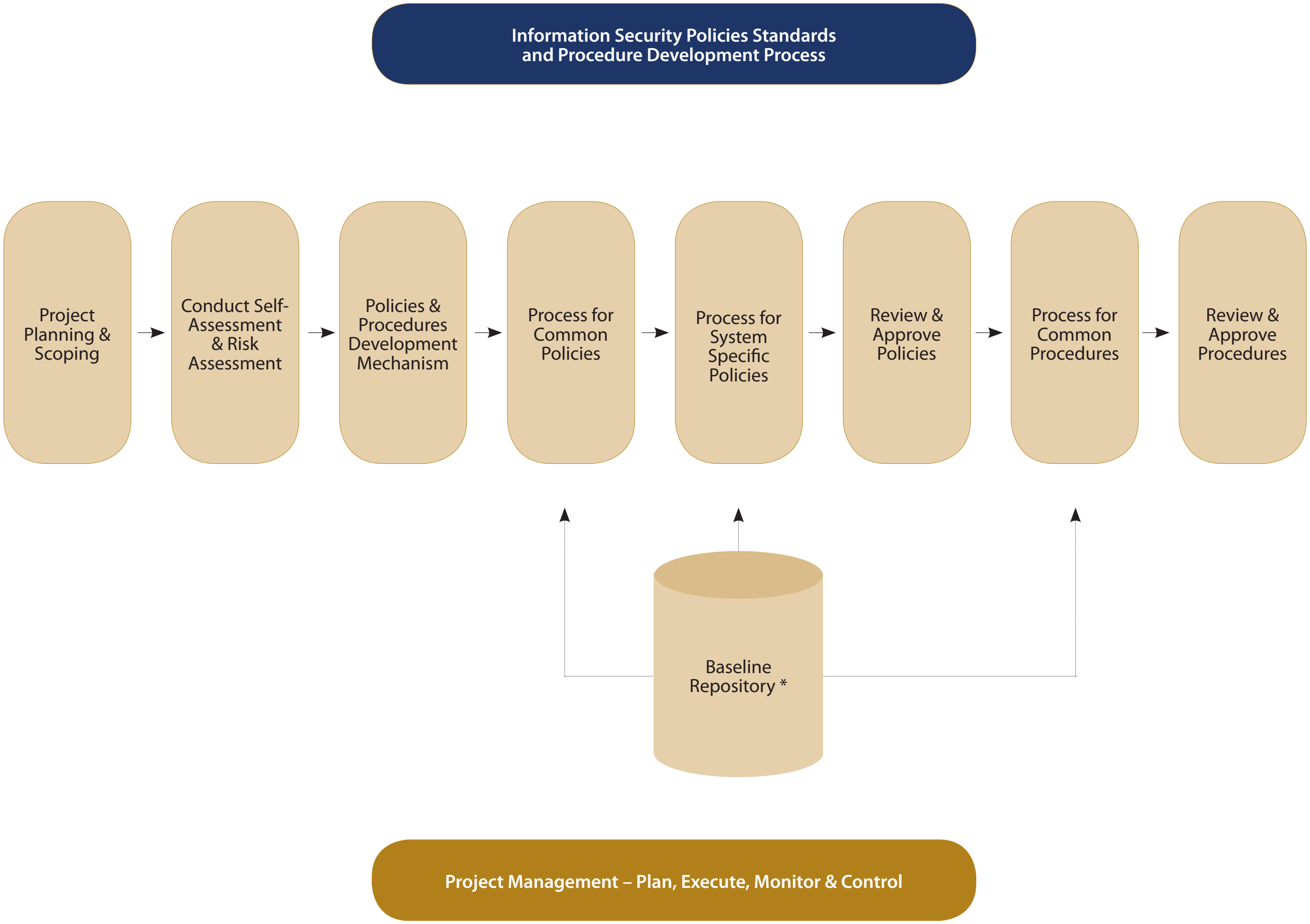
2. Objective

The information security policies and procedures developed process aims to set out a baseline approach to be followed by Government Agencies to develop appropriate policies and procedures that are aligned with the objectives of an overall information security management program within each Government Agency while ensuring that employees, contractors and third parties are aware of their responsibilities to protect valuable information systems and sensitive information.

3. Process Description

This Information Security Policies and procedures development process helps Government Agencies in developing their information security policies and procedures that are mapped to leading practices, individual business requirements, and appropriate regulations. The result is the creation and implementation of effective data information security policies and procedures, which help to establish a consistent and repeatable way to manage information security risk.

The following illustration depicts the key processes that a Government Agency should follow to develop its information security policies and procedures:



Information Security Policies Standards and Procedure Development Process

Project Planning & Scoping → Conduct Self-Assessment & Risk Assessment → Policies & Procedures Development Mechanism → Process for Common Policies → Process for System Specific Policies → Review & Approve Policies → Process for Common Procedures → Review & Approve Procedures

Baseline Repository *

Project Management – Plan, Execute, Monitor & Control

** Note: The Baseline repository comprises of the Common Policies, System Specific Standards and Common Procedures that are provided as part of the package along with this Information Security Policy, Standards and Procedures Development Framework. This repository will be used as a primary reference by the agency to determine the minimum-security requirements expected by the the agency under this framework.*

4. Project Planning & Scoping of Information Security Policies, Standards and Procedures Development

4. 1. Objective

The objective of the first step is to ensure that the information security policies and procedure development process is executed as a project. As explained in diagram above the entire process will follow the project management practices of plan, execute, monitor and control.

The Project will be initiated once the Top Management of a Government Agency.

4. 2. Establish Roles & Responsibilities

The Top Executive would be required to assign roles and responsibilities for Information Security Policies & Procedures Development Project. The following roles will be required for the Development Process:

- Project Owner: Generally, this role is assigned to the Top Executive of the Agency. The Project owner must initiate the Project and will be accountable for the project. He has the following responsibilities:
  - Champion the Project
  - Provide budget approvals for the Project
  - Accept responsibility for problems escalated by Project Manager
  - Define goals and objectives for the Project.
- Set targets on Key Performances Indicators (KPI).
- Decide who the members are of the Steering Committee.
- Steering Committee: The primary function of the Steering Committee is to provide oversight to the project management activities conducted by the Project Manager. This will include but not limited to review the requirements assessment and gap analysis reports, as well as the ongoing monitoring and review of the overall project. The Steering Committee must ensure all stakeholders are informed about the status and progress of the Project. The responsibilities include:
  - Review and approve the outputs from Self Assessment
  - Validate and prioritize risk identified
  - Review and approve risk identified
  - Review reports issued by the Project Manager
  - Review reports against targeted KPI.
- Project Manager: The Project Manager will be responsible for planning and executing the Information Security Policies and Procedure Development Project. He will have the following responsibilities:
  - Maintain the goals and objectives set forth by Project Owner
  - Assign Project Team
  - Conduct Self Assessment and produce reports for Steering Committee's review.
  - Assess the Project resource requirement
  - Assess and create an estimated budget required for the Project
  - Prioritize various phases of the development process
  - Ensure adherence to approved Project Plan
  - Ensure that resources have the required skill sets
  - Monitor and maintain the Project
  - Initiates and facilitates Top Executive meetings for major problems, reviews and endorsement.
- Project Team: The Project Team would comprise of various members from the Information Security Department and Information Technology

Department. The will have the following responsibilities:

- Conduct Self Assessment.
- Conduct Risk Assessment.
- Develop information security policies and procedures.
  - Customize information security policies and procedures.
- Execute tasks assigned by the Project Manager.

4. 3. Develop Project Charter and Project Plan

The Project Manager will be responsible for creating the Project Charter and Project Plan. Project Charter template is available in Appendix II Section and the purpose of the Project Charter is to address the following areas:

- Identify Key Stake Holders
- Define the scope of the information security policies and procedures development project. The scope of work may include one or more of the following:
- All Government Agency Information Systems or specific portion of the Government Agency Information Systems.
- Ore business functions of the Government Agency.
- The Government Agency head office.
- The Government Agency head office and its subsidiaries.
- Etc.
- Identify the steps, sequence of work, and timeframe for the defined project.
- Identify the Project Team

Further information on various aspects of Project Management including project scoping is covered under the Implementation Guide.

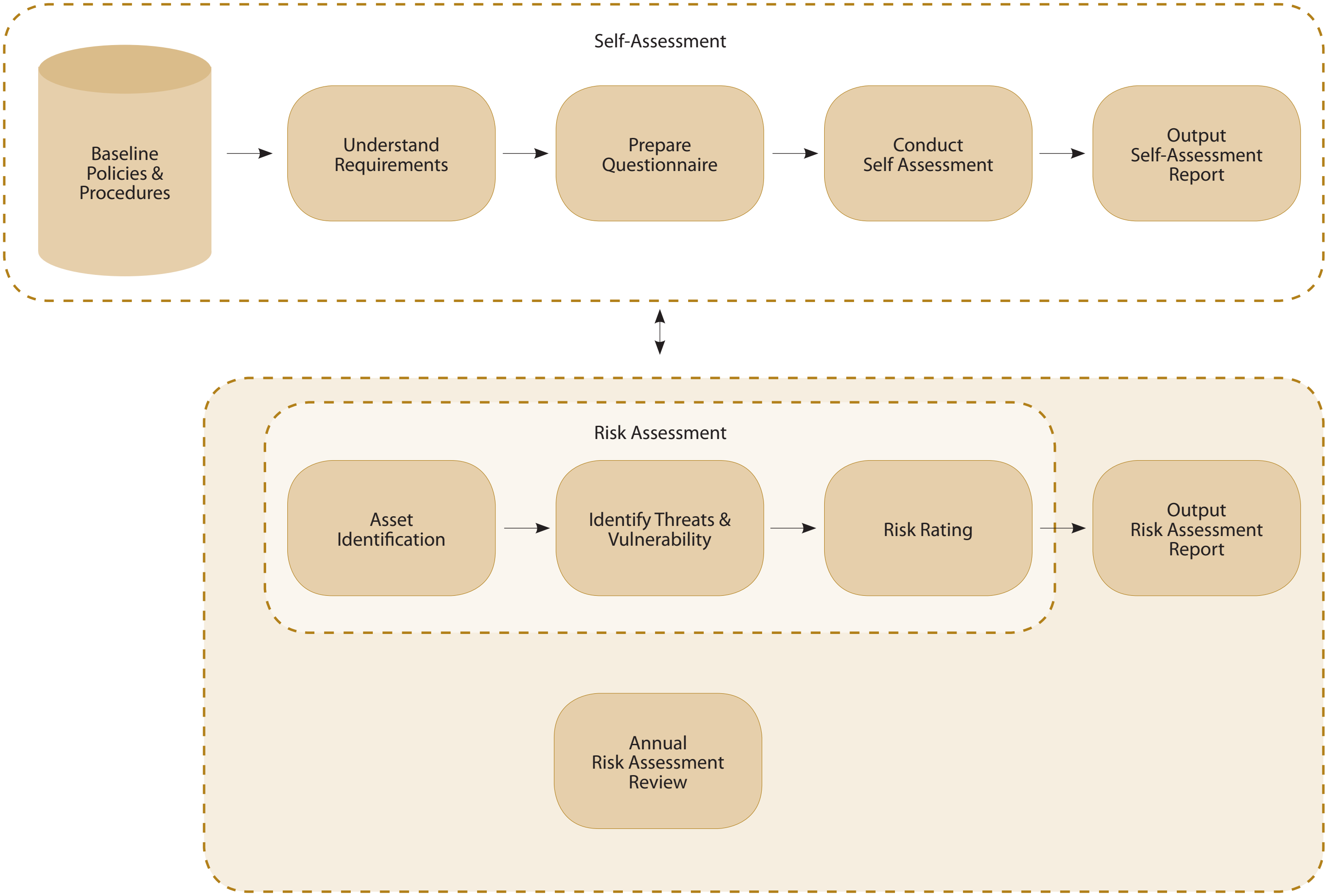
4. 4. Conduct Self Assessment and Risk Assessment

The self-assessment process is a key part of the overall Development framework. The objectives are twofold – firstly to gain an understanding of where the agency stands with respect to the baseline security policies, and secondly, to help develop or customize comprehensive policies and procedures that meet its security requirements.

The responsibility of conducting and coordinating the Self Assessment and Risk Assessment phases is with the Project Manager of the development effort. This will ideally be the Head of Information Security (Officer/Manager/Director level). In case such an official is not available in the organization, the next appropriate person to conduct these assessments will be the Head of Information Technology who should have suitable understanding and experience of the information technology setup and the business processes of the organization.

It is also noted that while the Project Manager is responsible for conducting these assessments, the source of information would remain to be the key stakeholders and business owners. Their inputs will be key for these assessments.

The whole assessment process is divided into two phases – The Self Assessment and Risk Assessment as shown in Fig 1. Each type of assessment is described in more detail in the following sections.


Self-Assessment
Baseline Policies & Procedures
Understand Requirements
Prepare Questionnaire
Conduct Self Assessment
Output Self-Assessment Report
Risk Assessment
Asset Identification
Identify Threats & Vulnerability
Risk Rating
Output Risk Assessment Report
Annual Risk Assessment Review

4. 4. 1. Understand Requirements

In order to perform a self-assessment, the Agency must first understand and recognize its obligations and requirements concerning Information security.

The project manager or one of the policy development team members will use the following mechanisms for conducting the Self Assessment:

1. Meetings with Key Stakeholders

Meetings must be held with key stakeholders to understand the business and technology drivers affecting the agency. The purpose of these meetings is to understand the processes of key business functions and of key technology services or support functions.

The persons in charge of the following key areas should be met for this purpose:

- Information Technology.
- HR.
- Administration & Facilities.
- Finance.
- Network.
- IT Support.
- Application Development, if exists in-house.
- Data Center.

2. Review Documentation

A study of the key relevant documentation will give an understanding of the processes, activities of modes of operations.

The key factors to consider are:

1) The Agency's risk evaluation factors;

The project manager must understand the environment in which the agency operates. Some of the key factors are:

- Identifying its key customers
- Identifying the number and criticality of services provided
- The number of sites it operates from
- Criticality of its assets
- Stakeholder expectations and loss of goodwill and reputation

2) Applicable laws and regulations;

Agency must identify all relevant laws and regulations applicable within Saudi Arabia. These will include statutory, regulatory requirements or any contractual agreements with other organizations.

The results of this phase can be used to prioritize the implementation of the controls in the risk treatment phase.

4. 4. 2. Prepare Questionnaire

To assist the Agency in identifying gaps in the information security framework, the development project team will prepare an assessment questionnaire. The questionnaire is a tool for performing an assessment of the controls in each policy area that exist in an organization. The questionnaire must be based upon the Policy areas listed in Table 1 and must cover the Agency's critical business functions.

1. Questionnaire Structure

The self-assessment questionnaire contains three sections: Introduction, questions about existing and/or expected controls in the policy areas under review, and additional notes. The questionnaire should have an introduction sheet requiring a description about the policy area being assessed. It also will indicate the CIA rating of the asset.

A sample of a self-assessment questionnaire is shown in Appendix IV.

The questions can be divided into two major categories depending on the policy areas to be covered: 1) Management controls and 2) Technical controls as shown in Table 1.

Table 1

Policies Areas Requiring Management Controls	Policies Areas Requiring Technical Controls
Corporate Information Security	Logical Access Management
Information Security Responsibilities	Malicious Code Protection
Information Security Awareness	Electronic Media Handling
Information System Acceptable Use	Information Security Incident Management
Document Security	Personal Security
Privacy	Information Asset Management
Fraud and Whistle blowing	Physical and Environmental Security
Information Security Risk Management	Backup and Restoration
Information Security Policies Management	E-Services
Compliance with Legal Requirements	Information System Acquisition and Development
Third Party Service Delivery Management	Change Management

Policies Areas Requiring Management Controls	Policies Areas Requiring Technical Controls
Outsourcing Service Providers	Information Security Monitoring
Customer Policy	Information Security Assessment
	Information Security Auditing
	Compliance with Policies and Procedures
	Business Continuity Management

In order to measure the effectiveness of existing controls and also to improve the effectiveness of the relevant policies in the coming years, five levels of have been defined to measure the effectiveness for every control question:

- Effectiveness Level 1 – control objective is documented in a security policy but do not contain procedures and controls are not implemented.
- Effectiveness Level 2 – security controls are documented in procedures but are not implemented.
- Effectiveness Level 3 – procedures have been implemented but have not been tested or reviewed.
- Effectiveness Level 4 – procedures and security controls are tested and reviewed periodically
- Effectiveness Level 5 – procedures and security controls are fully integrated into a comprehensive program.

4. 4. 3. Conduct Self Assessment

1. Self Assessment Responsibilities

a. The person conducting the self-assessment should preferably be a person from the IS function knowledgeable of the policy area under review. This person will be a member of the project team that is responsible for policies and procedures in line with this framework.

b. The persons in charge of the following key areas should be interviewed for administering the questionnaire:

   - Information Technology.
   - HR.
   - Administration & Facilities.
   - Finance.
   - Network.
   - IT Support.
   - Application Development, if exists in-house.
   - Data Centre.

c. Analysis of the information captured by this questionnaire is the responsibility of the head of IS function (who will also be the project manager of this policies and procedures development project). The primary aim of this analysis should be to incorporate areas of policy weaknesses or gaps into subsequent steps as defined in this framework document.

2. Administering the Questionnaire

The self-assessment questionnaire can be administered by a combination of the following methods:

- By an examination of relevant documentation;
- By meetings held with key stakeholders;
- By an examination and test of controls - For example examining Change records, active system accounts etc.

Supporting documentation detailing the tests conducted and the results of the tests add value to the assessment and will facilitate the any future reviews.

During the assessment, if parts of the questionnaire are found to be not applicable to the policy area under review, then it should be marked as "not-applicable" or "N/A" and a suitable explanation should be recorded.

For all applicable areas, the assessor must review the relevant policies, standards and procedures and make the assessment in the following sequence:

- No documented policies, standards or procedures exist (to be marked as "Do not exist")
- Documented policies and standards are in place (level 1);
- Procedures for implementing the control exist (level 2);
- The control has been implemented (level 3);
- The control has been tested and improved if found ineffective (level 4); and
- The control is part of an agency's organizational culture (level 5).

A sample questionnaire is shown in Appendix IV

3. Self Assessment Reporting

Upon completion of the self-assessment, the Project Manager must compile a Self Assessment Report and present it to the Steering committee. The report must highlight the following gaps in current state against the 29 baseline policy areas:

- The baseline policies areas that are not currently deployed in <Organization Agency Name>.
- Partial coverage and the resulting gaps in the already implemented Policy areas.
- Prioritization of gaps and missing policy areas based on assessment.

4. 4. 4. Information Security Risk Assessment

A systematic approach to information security management is necessary to identify organizational needs regarding information security requirements. Security efforts should address risks in an effective and timely manner. Information security risk assessment is an integral part of any information security management process.

Below is a typical description of the risk assessment process to be followed by <Organization Agency Name> to obtain an understanding of the risks faced by it. The outcome will be used in the subsequent stages of the Information Security Policies and Procedures Development Framework.

1. Information Asset Identification

An asset is defined as anything that has value to the agency and which therefore requires protection. For the purposes of this ISPDF, the focus of the <agency > should remain on the information assets. To facilitate the identification process, these Information Assets can be grouped in the following broad types as shown in Table 2:

Table 2

Asset Type	Description
Core Services	Key Agency activity or services rendered
Personnel	General users; Management personnel; Technical personnel
Hardware	Fixed equipments; Mobile equipments; Paper documentation; Electronic Media; Network devices
Software	Operating system; Business Application; Configuration records
Information	Information vital to Agency; Personal information; Strategic information; Electronic records;
Service Providers	Third Party service providers; Vendors;
Site	Physical location; Utility services
Intangibles	Organization reputation

Information Assets should be assigned a measure of valuation either by qualitative or quantitative means. Qualitative methods define degrees of value e.g. Very High, High, Low, Very Low, Medium whereas Quantitative methods of valuation define the value of an asset in quantifiable terms.

Of the two methods, Quantitative methods are not generally used due to practical difficulties in assigning values to individual assets.

The commonly used Qualitative method to value an asset is to determine its CIA (Confidentiality; Integrity; Availability) value. An example is provided in Table 3 below:

Table 3

Asset Type	Asset Name	Confidentiality High = 3 Medium = 2 Normal = 1 C	Integrity High = 3 Medium = 2 Normal = 1 I	Availability High = 3 Medium = 2 Normal = 1 A	Asset Value C x I x A
Hardware	Core Switch1	2	1	3	6
Information	Personal records	3	3	3	9

2. Identify Threat & Vulnerability

The threats and vulnerabilities must be identified for each of the asset types determined during the Asset Identification. This forms the basis of the risk analysis.

A threat is potential event from the external environment and has the potential to harm assets such as information, processes, and systems as well as people leading to harm to the organization. Threat sources may be determined by consulting with the asset owners, facility and administration, security specialists, specialist groups, etc.

Sources of threats care primarily external and can be further grouped into the following broad types:

Sources of threats	Examples
Human	External Hackers;
Technical	Connectivity Failure from Telecom provider
Environmental	Fire; Epidemic

After the Assets and Threats are identified the project manager must identify vulnerabilities that the threats will exploit. Vulnerabilities are defined as weaknesses existing within the organization, and can be identified in the following areas:

- Personnel.
- Organizational Policies.
- Processes and procedures.
- Physical environment.
- Information systems.
- Software.
- External Service providers.

An example of Threats and Vulnerabilities is listed in Appendix C. It must be noted that this is not a complete list of Threats and vulnerabilities and agency must further develop this table and tailor to its own requirements.

3. Risk Ratings

Once the risks are determined for different scenarios and for key assets classes of the organization, these risks are rated in terms of the following:

- Impact of Threat to the organization
- Likelihood or probability of threat occurring

The Impact of the threat and likelihood of its occurrence will determine what should be the focus of the management efforts in implementing the Information Security Policies Development Framework.

Key stakeholders are involved in assigning the impact and likelihood ratings for key risks identified for the organization. Their cumulative ratings are then compiled and an overall risk rating High, Medium, Low is assigned based on the risk. A risk-rating template with samples is provided in Appendix IV for reference

4. Overall Risk Rating for the Agency

In addition to the individual detailed risk ratings assigned in the previous step, it is imperative that the management also develops an understanding of the overall risk profile of their agency. Both quantitative and qualitative factors need to be considered.

- Quantitative: Management should compile an overall risk rating for the agency based on the overall combined average for all the individual risk ratings assigned as part of risk assessment. Normally, a simple average rating will be sufficient. However, management may also decide to give more weight to specific areas and compute a weighted average.
- Qualitative Factors to be considered:

The management will further cross-check and verify the above risk rating in line with other considerations about the nature of agency and its areas of operation within the overall context of the Saudi Government and national economy. Accordingly, the agency management may be required to increase the risk rating to a High or Medium level, if necessary.

- Importance of Agency to Government: Guidance to be obtained from the relevant ministry.
- Importance to National Security and Economy: This will be based on the industry grouping.
    - National Security:
        - National Security.
        - Foreign Affairs.
    - Civil & Public Services:
        - Civil & Public Services
        - Education
    - Finance & National Economy
    - Healthcare
    - Commercial & Others:
        - Commercial & Industrial
        - Communication & Technology
        - Oil, Gas & Minerals
        - Transport
        - Other
- Level of Public Interaction and Services Provided by the Agency

5. Risk Assessment Reporting

Upon completion of the risk assessment, the Project Manager must compile a Risk Assessment Report and present it to the IS Steering committee. The report should include an overall summary of risks faced by the organization as well as the following details for each key risk:

- Threat.
- Vulnerability.
- Asset Name.
- Asset Value.
- Risk Statement.
- Threat Impact.
- Probability.
- Inherent Risk Rating.

4. 5. Policies and Procedures Development Mechanisms

This framework requires the agency to fully comply with the Information Security requirements mandated by Saudi Government

4. 5. 1. Decision Factors

While remaining within the compliance requirements, the <Organization Agency Name> can choose to develop and update their policies and procedures on their own or decide to adopt the policies and procedures provided along with this framework with suitable customization.

Management will consider the following factors before deciding upon the mechanism to be used either as self-development customization:

1. Size of the existing Information Security Department.
2. Availability of in-house specialist skills.
3. An initial understanding of the costs involved depending upon factors such as the complexity, variety, uniqueness and/or size of the agency's operations.
4. Time constraints depending on the overall deadlines.

Based on an overall management judgment of the above factors, one of the two approaches (Self-Develop or Customize) will be adopted by the Top Management. Guidance has been provided below for both the approaches.

Furthermore, management may also choose to have a mixed approach by applying Self-Development to some selected policy areas whereas choosing to follow customization for the remaining policy areas in order to optimize the costs and reduce the total time required.

4. 5. 2. Customize the Provided Information Security Policies and Procedures

It is recognized that many <Organization Agency Name> may be faced with a strict deadline by the government or may not have the required resources or skill set available to do any self-development. Therefore, a complete set of policies and procedures have been developed and provided with this Development Framework for use by the management of the respective <Organization Agency Name> as a support to enable them to comply with the mandate.

The <Organization Agency Name> can create policies, and procedures in a short duration by customizing the policies and procedures provided with this Development Framework (which can also be considered as the baseline policies and procedures repository). For this purpose, the Information Security Officer will be assigned the primary responsibility of customizing the information security policies and procedure. The Information Security Officer should have the following skills:

- In-depth knowledge of Information Security
- In-depth knowledge of the Government Agency
- Previous experience in writing policies and procedures
- Technical writing skills

Additional short-term support can also be obtained from other departments or external parties on a strictly need basis.

4. 5. 3. Self Development of Information Security Policies and Procedures

Depending on the factors described above, the management of < Organization Agency Name > may decide to establish their policies and procedures following a self-development approach. It can do so by assigning an information security expert that is available internally or can obtain help from an external party.

The policies should be developed based on various standards including but not limited to the following:

- US- Federal Information Processing Standards FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems
- US-National Institute of Standards & Technology NIST PUB 80053--Recommended Security Controls for Federal IS
- Germany- Federal Office for Information Security (BSI)Baseline Protection Manual
- ISO/IEC 27001
- Saudi Laws
  - E--Transaction Law
  - E- Crimes Law

The management of < Organization Agency Name > is required to ensure a full compliance with the Information Security requirements mandated. Hence, coverage is required for all of the 29 baseline policy areas covered in the Policies document provided with this Development Framework. However, the management has the opportunity to further enhance and /or add other areas to the coverage if the necessitated by any unique operations of the agency in any policy area.

1) Self-Development by Own Employees:

The first option for policy development should be in-house development by own employees. The Information Security experts who are assigned this responsibility must have the following skills and competencies:

- Information Security certification
- In-depth knowledge of Information Security
- In-depth knowledge of the Government Agency
- Previous experience in writing policies and procedures
- Technical writing skills
- Information Security policies and procedure writing skills

If a majority of the above requirements are not fulfilled by an existing internal resource, the management must consider hiring additional resources.

2) Development with the Help of External Contractors:

Non-availability of in-house skills will be the primary reason for engaging an external contractor.

In case an external contractor is engaged to develop policies and procedures, management must ensure credentials and local resources of this external party. In addition, the ultimate review and approval authority of the policies, standards and procedures developed by this party should rest with the head of information security and the top management of the <Organization Agency Name>.

The mechanisms described above are applicable to each area where development of policies and procedures are concerned

4. 6. Process for Information Security Common Policies

Based on the Self Assessment and the Risk Assessment described earlier, the Project Team will be able to identify policies that need to be developed.

Once the Policy Areas are clearly identified, the Project Team will be responsible for creating a policy structure and fill in information accordingly. The following policy structure can be used as a basis for creating information security common policies:

- **Policy Title:** Name of the Policy Area
- **Policy Purpose:** Briefly illustrate the purpose of the Policy.
- **Policy Applicability:** Define various internal and external entities as well as the people to which a particular Policy statement will apply.
- **Executive Owner:** Identify the person who has the ultimate authority and responsibility for any changes and updates in the policy. Any changes or updates in the policy has to be approved by the executive owner
- **Custodian:** The person who is responsible for maintaining, communicating, and updating the policy based on directions from Executive Owner.
- **Enforcement:** Defines the consequences of any violation of the policy.
- **Policy Sub Area:** Defines sub areas of a policy area for e.g. Logical Access Management – Access Control.
- **Policy Statement:** This section describes the control statements part of the specific policy
- **Policy Effective Date:** This section defines the date from which the policy is applicable and is to be followed

Example:

Policy Title: *Corporate Information Security Policy*

Purpose: *The purpose of this policy is to communicate the management commitment and key goals for establishing risk based information security controls in the <Organization Agency Name>.*

Policy Applicability: *This policy applies to all temporary or permanent <Organization Agency Name> employees, vendors, business partners, and contractor personnel and functional units regardless of geographic location.*

Executive Owner: *IS Officer*

Custodian: *Head of IT*

Enforcement: *Any employee or third party (vendors, business partners, and contractor personnel etc) found to have violated this policy may be subjected to disciplinary actions as per the organization's policies and Saudi Arabia's laws and regulations including but not limited to Labour Laws, Anti e-Crimes Law and e-Transaction Law...*

Information Security Policy Statements

Corporate Security Key Objectives

"Government Agency" *information systems shall be used only for authorized business purpose and limited personal* *usage as per organization's information system acceptable usage policy.*

The Project Team will be required to follow the Documentation Control process described in Appendix III while creating policies.

4. 7. Process for System Specific Standards Policies

Based on the Self Assessment and Risk Assessment, the Information Assets will be identified and classified. Each asset will be assigned a risk rating.

Based on the Policy areas identified in the common policies, the Project Team will be responsible for creating standards structure and fill in information accordingly. The following System Specific standards structure can be used as an example for creating information security system specific standards:

- **Policy Area:** This section describes the Policy area to which the standard belongs.
- **Standard Area:** This refers to the category that the Standard falls under.
- **Detailed Standard Statements:** This section describes the control statements of the specific standard.
- **Applicability:** This section identifies the CIA rating of the agency that will implement this standard.
- **IT Specific Systems:** This section identifies the IT systems to which the standard applies.
- **Standard Reference No:** This refers to the reference number of the Standard statements.

Example:

Policy Area - Information Security Awareness

Standard Area - Information Security Awareness Sessions

Detailed standard statements

1. Awareness programs must focus on end user security responsibilities.
2. The programs must be conducted periodically at least once every 6 months.
3. Its effectiveness must be measured and suitably corrected and improved over time.
4. All new hires must undergo Security Awareness training as part of the induction process.
5. Awareness programs must use methods such as Email, Posters, Video or Classroom
training.

Applicability: Agencies with Risk Rating of - High, Medium, Normal

The Project Team will be required to follow the Documentation Control process described in Appendix III while creating policies.

4. 8. Review & Approve Information Security Policies

Upon the completion of the creation of Information Security common policies and system specific standards, the documents shall be submitted to the Steering Committee for review and approval. Inputs will be taken from all stakeholders to verifying the acceptability of policies created. The Steering Committee will either accept or reject the Policies created. Rejected policies will be subject to change as per the Steering Committee comments.

4. 9. Process for Information Security Procedures

Upon receiving the approval of the Information Security Policies and Standards, the Project Team will be responsible for creating the procedures for all relevant policy areas and standards. The creation of procedures is also subject to existing procedures covered under Information Technology or Human Resources Policies and Procedure.

The following procedure structure can be used as an example for creating information security procedures:

- **Objective:** This section states the information security related objective of the procedure.
- **Policy Reference:** This section identifies the relevant policy for a given procedure.
- **Procedure:** This section lists down and describes the systematic activities to be followed under the procedure. These activities should always be described in terms of specific actions by specific parties. Some of these activities will be value-added, review and approval type activities while other admin type activities will also need to be added to complete the process flow.
- **Related Form:** This section specifies the names of the related forms, if any, that exist for the procedure.

Example:

Logical Access Management

The objective of the logical access management procedures is to manage user access to "Government Agency"s' information systems.

User Group Access Profile Creation Procedure

Objective

This procedure illustrates key activates for creation of standardized User Group Access Profile on information systems. User Group profiles are associated with a set of agreed and predefined system privileges that are considered appropriate for a specific group of information system users.

Policy Reference: *Logical Access Management Policy*

Procedure: *When a system is initially being setup, the IT Manager together with information system owner is responsible for defining and implementing group user profiles before system is put into production. For the system that is already in production, the relevant development/ configuration staff together with information system owner undertakes this responsibility.*

The relevant IT person (as stated above) coordinates with the information system owner to identify the following:

- *The potential group of users who shall be using this system.*
- *The type of access those users shall need to perform their assigned tasks.*

4. 10. Review & Approve Information Security Procedures

Upon the completion of the creation of Information Security procedures, the documents shall be submitted to the Steering Committee for review and approval. Inputs will be taken from all stakeholders to verifying the acceptability and feasibility of procedures created. The Steering Committee will either accept or reject the procedures created. Rejected procedures will be subject to change as per the Steering Committee comments.

4. 11. Project Management

4. 11. 1. Objective

This process has the following objectives:

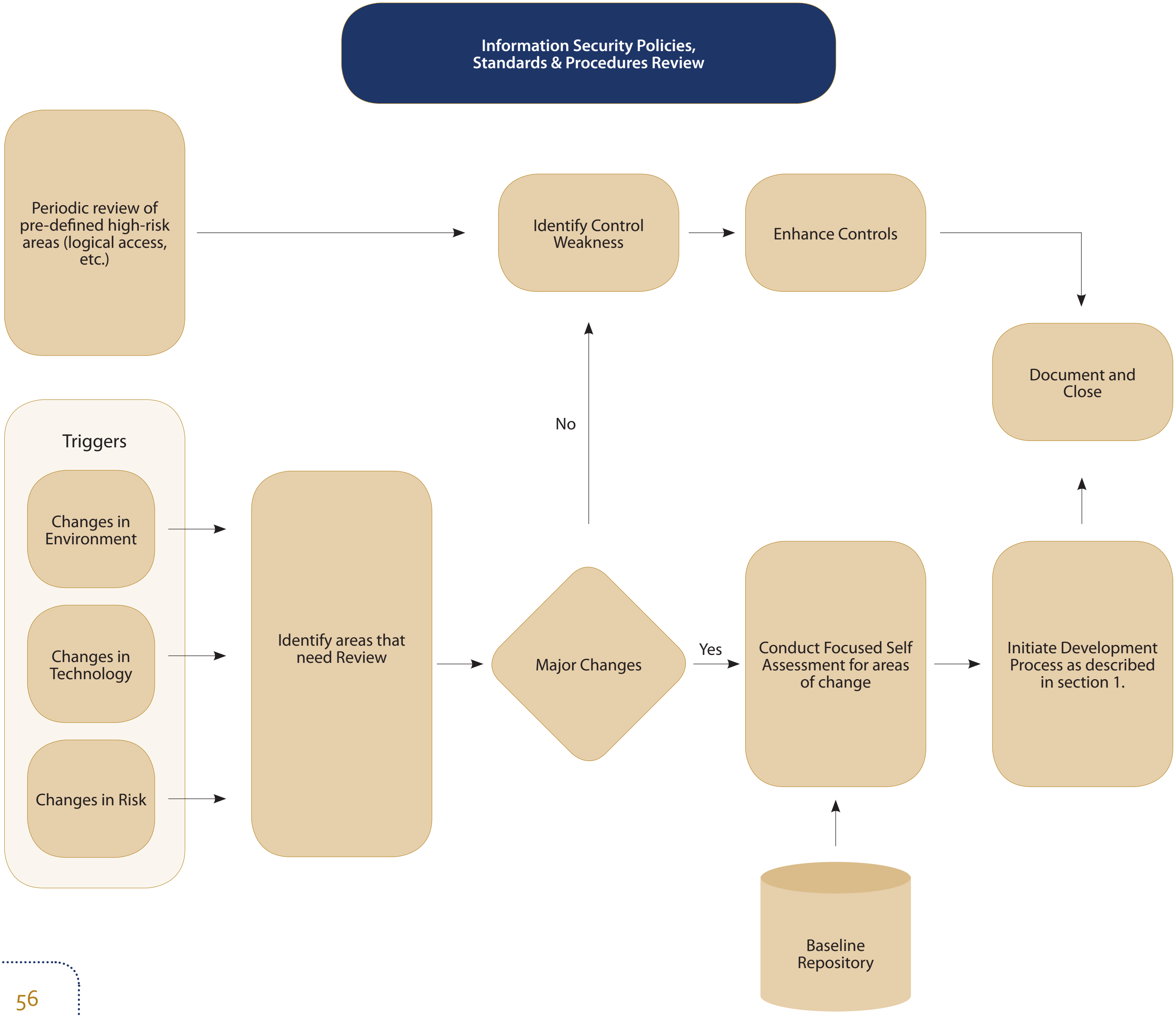
- Manage and oversee the information security policies and procedures development.
- Report the status of the information security policies and procedures development to the steering committee.

4. 11. 2. Manage the Project

Throughout all the information security policies and procedures development phases, the Project team shall continuously maintain strong and effective project management and each Government Agency management shall apply quality assurance procedures to ensure that the information security requirements are met and avoid any project overruns and delays.

The project manager shall monitor the development of the information security policies and procedures and provide status reports using the project status report template in Appendix II Section 2.5 to the steering committee on ongoing basis.

4. 12. Annual Review of Information Security Policies & Procedures


Information Security Policies,
Standards & Procedures Review
Periodic review of pre-defined high-risk areas (logical access, etc.)
Identify Control Weakness
Enhance Controls
Document and Close
No
Triggers
Changes in Environment
Changes in Technology
Changes in Risk
Identify areas that need Review
Major Changes
Yes
Conduct Focused Self Assessment for areas of change
Initiate Development Process as described in section 1.
Baseline Repository

4. 12. 1. Periodic Review

< Organization Agency Name > will be required to conduct a periodic review on predefined High-risk areas of policies, standards and procedures. Segregation of duties must be maintained while conducting reviews i.e. the team members that were involved during the development process must not review the policies and procedures.

Based on < Organization Agency Name > Information Assets risk rating, the Review Team will select High-risk areas and conduct reviews of the effective of policies, standards and procedures accordingly. The identified weakness resulting from the review will require controls to be modified or enhanced.

4. 12. 2. Identify areas that need review

The need for review of Policies and Procedures arises from that fact that there are constant changes in the business environment, technology and risks. Over time, the changes that occur cause the policies and procedures to become ineffective and inefficient thus causing an increase in risk areas. The steering committee is responsible for setting up an annual review process of information security policies and procedures.

The changes that occur can be minor, major or significant. Based on the classification of change the review process can be detailed or brief. The Steering Committee should create a Review Team that will be required to conduct the following:

- Identify and classify changes in Environment
  - Size
  - Branches
  - Services
  - Staff size
  - Physical location
  - Government rules & regulations
- Identify and classify changes in Technology
  - IT Applications
  - IT Systems
  - Networking

4. 12. 2. 1. Process for Major/Significant Changes

In case Major changes in environment are identified, the Steering Committee will instruct the Information Security Department to conduct a Focused Self Assessment cover the area of change.

1. Focused Self Assessments

The Focused Self Assessment should be conducted as per the guidelines stated in section 1.2, as the title suggest this Self Assessment will be limited to the identified areas of Major changes. The Self Assessment would identify gaps between the policies, standards, procedures and the baseline.

2. Initiate Development Process

Upon identification of gaps, the Steering Committee will either recommend a set of projects or a single project. Projects will be dependent on the size of changes identified by the Review Team. The Steering Committee will assign a Project Manager who will then be responsible for following the development process explained in section 1.

4. 12. 2. 2. Process for Minor Changes

Upon identification of Minor changes, the Steering Committee will delegate the Review Team to identify weakness in controls implemented through the current policies and procedures.

1. Identify Control Weakness

The Review Team will be required to assess the current effectiveness of controls in places; this means the Review Team will conduct sample tests on policies, standards and procedures. They will first understand the policy and standards and its associated procedures. They will then take a previously reported case of policy violation and identify the areas where risk mitigation failed. A report will be produced that will be produced for the Steering Committee's review and approval.

2. Enhance Controls

The identified areas of risk mitigation failures would require enhancement of existing controls. This would entail creating additional procedures statements or adding extra steps in performing various tasks related to risk mitigation.

4. 12. 2. 3. Document and Close

All finding from the review must be documented and presented to the Steering Committee for final review and approval.

Chapter 3

Information Security Policies and Procedures Implementation Guide

1. Introduction

1. 1. Purpose

This document presents guidelines for implementing information security policies and procedures for the <Organization Agency Name>. The document also presents related forms and templates to support this implementation.

Implementation and delivery of information security policies and procedures is one of the key responsibilities of government agencies. The focus is on sound policy implementation and seamless delivery of information security policies - on time, within budget and to an acceptable level of quality.

The information security policies and procedures development framework will be issued to Top Executive of each Governmental Agencies with a defined timeline, thereafter it will become the responsibility of the Top Executive to ensure that an adequate implementation program is followed to ensure successful implementation. It is important to note that this guide is intended to help the agency in implementing the approved policies and procedures resulting from the development process that should be completed prior to commencing any implementation activities.

Implementation of information security policies and procedures will facilitate the adoption of a full information security management system. This implementation program is designed to support the <Organization Agency Name> in rolling out the security policies and procedures in line with the management priorities.

The focus of this implementation guide is on overarching principles for effective implementation, drawing on the experience of agencies to date, as well as leading program/project management and information security practices.

1. 2. Program Ownership

The <Organization Agency Name>›s Top Executive (Governor/Deputy Governor/Director etc.) is the owner of the Information Security Program. He shall have vested authority and accountability for implementing the Information Security policies and procedures in line with guidelines provided for the purpose.

2. Information Security Department Placement

The Top Executive will establish an Information Security Function as per the Department Placement Options document provided separately. The structure shall provide relationship of information security department with other relevant major positions in the organization. This relationship will be defined in the context of the following aspects:

- Reporting Relationship covering all Information Security compliance matters
- Administrative Relationship covering Admin and Budgeting matters for Information Security Department

The establishment of the Information Security Deparment is the prerequiste of setting up the Implementation Program. The Information Security Director will be assigned the role of Program Manager for the purpose of this Implementation Program while further roles and responsibilites are defined in section 5.1.

3. Implementation Program Mandate

Upon receiving the Information Security framework the completeness of all documents received must be checked as per Appendix 8.1.

The Program Owner will be required to issue a mandate within the agency to all stakeholders instructing them to carry out the implementation of the approved Information Security Policies & Procedures. This mandate would be based on the required timeline set by Saudi Government

4. Implementation Program Setup

Following the issuance of the mandate, the Program Owner shall set up the basic structures for the Information Security Implementation Program. The following key aspects shall be considered:

4. 1. Top-Down approach

A top down approach is envisaged for implementation of information security policies and procedures. This will ensure that the work program can be implemented through clear objective setting, based on <Organization Agency Name> business plan objective, from senior management, through middle management, to staff members of <Organization Agency Name>. The <Organization Agency Name> will set accountability at different levels for implementing the program.

4. 2. Identify Stakeholders

All parties that are likely to be affected by the implementation must be identified. This may be carried out in a workshop setting with the representatives of management and key functions. A stakeholder may be defined as "anyone who is impacted by the implementation of information security policies and procedures". Each stakeholder has an essential contribution to make and appropriate expectations of each stakeholder need to be met.

The <Organization Agency Name> will identify Information Asset Owners (IAO) for each of the information systems that the organization operates. These will be key senior members of staff from within the <Organization Agency Name> which owns the system. They will typically be the data owners for those information systems operated within their business area. They will be responsible for their systems' day-to-day protection and for providing information assurance on the information assets they own. Each IAO will also ensure that the organization›s requirements for information incident identification, reporting, management and response apply to the information assets they own. This includes the mechanisms to identify and minimize the severity of an incident and the points at which assistance or escalation may be required.

4. 3. Establish Steering Committee

Program Owner will constitute a Steering Committee with fair representation from the top management as well as stakeholders. The Steering Committee will be the authority in resolving issues related to the implementation and take decision on changes required. The Steering Committee will prioritize the implementation in line with the CITC guidelines taking into consideration factors such as the risks involved, resource availability, etc.

4. 4. Appoint Overall Program Manager

The Steering Committee shall appoint a Program Manager with the appropriate experience, and capabilities for managing the implementation program efficiently and effectively. The Program Manager will be responsible for all phases of the implementation of policies and procedures and will report to the Steering Committee. In case of any conflicts he may seek advice of the Steering Committee. The Program Manager should be familiar with the organization, its culture, systems and information security in general. He should have a strong knowledge of the resources that they have to work with and great ability to work with others and attain good cooperation from the people with whom they are working.

5. Program Implementation

Successful implementation of Information Security Policies and Procedures requires the support of Top Executive and all stakeholders. An Implementation Program will enable the organization to achieve the required objectives set forth by Saudi Government on Information Security.

The various phases of the Implementation Program are as stated below:

5. 1. Establish Roles & Responsibilities

After issuing a mandate the Top Executive would be required to assign roles and responsibilities for the implementation program, it is essential that roles and responsibilities be assigned before the Implementation Program is initiated. This will help the Implementation Program as each Phase requires accountability and ownership.

5. 1. 1. Program Owner

Generally, this role is assigned to the Top Executive of the Agency.

The Program Owner must initiate the Implementation Program and will be accountable for the complete Implementation Program. He will also be responsible for ensuring that the Implementation Program is followed in a correct manner. He has the following responsibilities:

- Champion the Program
- Provide budget approvals for the Program
- Accept responsibility for problems escalated by Program Manager
- Define goals and objectives for the Program.
- Set targets on Key Performances Indicators (KPI).
- Decide who the members are of the Steering Committee.

The Program Owner must have good Communication skills, Organizational skills, Facilitation skills, Leadership skills, good problem solving skills. He should have knowledge of the <Organization Agency Name>. He must have a reputation to exert pressure within an Agency to overcome resistance to the Program.

5. 1. 2. Steering Committee

The primary function of the Steering Committee is to provide oversight to the program management activities conducted by the program manager. This will include but not limited to review the requirements assessment and gap analysis reports, approve initiatives, projects, as well as the ongoing monitoring and review of the overall program and the individual projects. The Steering Committee must ensure all stakeholders are informed about the status and progress of the Implementation Program. The responsibilities include:

- Analyze the output of the Requirements Assessment and gaps identified.
- Validate and prioritize Initiatives identified.
- Review reports issued by the Program Manager
- Review reports against targeted KPI
- Review Change Applications that are submitted to Steering Committee
- Review applications for Change and advise the Owner to approve/reject the application
- Approve the Significant and Major Planned Changes resulting from the implementation of policies and procedures
- Participates in Post Implementation Review (PIR) as needed
- Review PIR reports as needed

5. 1. 2. 1. Membership

The Steering Committee has permanent members and ad hoc membership based on the Steering Committee meeting agenda. It is not necessary to have the same designated members in each Agency, where possible the members should be of the same designation or their equivalent.

Permanent Members:

- Program Owner (chair)
- Program Manager
- IT Director
- Information Security Director
- Service Desk
- Telecommunication Services
- Computing Services
- Security Services

Ad hoc membership can include:

- Accounts
- Operations
- Service providers as deemed necessary by the Program Owner or the Program Manager
- Vendors as deemed necessary by the Program Owner or the Program Manager
- Others as deemed necessary by the Program Owner or the Program Manager

Members of the Steering Committee should possess communication skills, organization skills, facilitation skills, leadership skills, presentation skills, negotiating skills. They should also have extensive technical knowledge and financial skills.

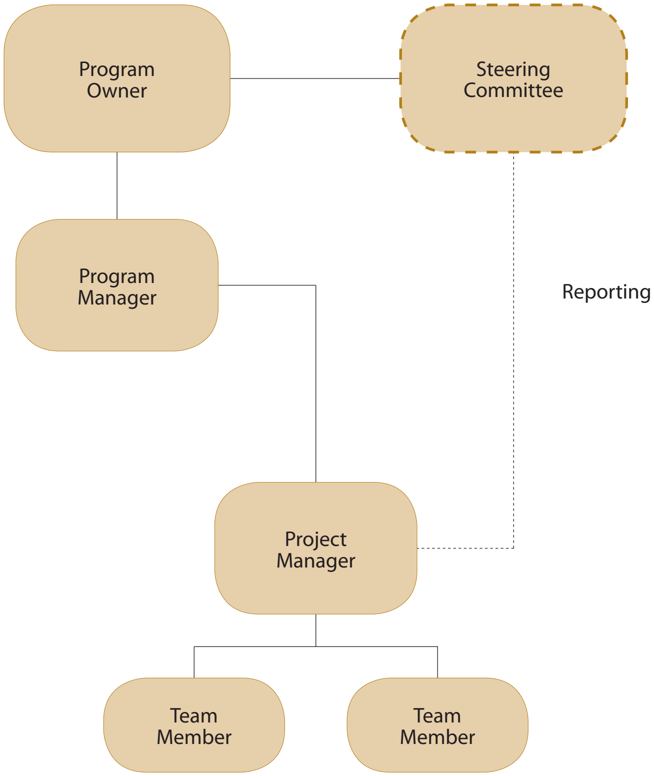
5. 1. 3. Program Manager

The Program Manager will be responsible of making sure the implementation program is followed and adhered to. He must take identified Initiatives and convert them into projects, depending on the size of the initiative could be considered multiple projects or single project with various initiatives defined as phases. The other responsibilities of a Program Manager include:

- Maintain the goals and objectives set forth by Project Owner
- Conduct requirements assessment and produce reports for Steering Committee's review.
- Assess likely impact of the Implementation Program on the Live environment
- Assess the Implementation Program resources required
- Assess and create an estimated budget(within the initial approved budget) required for the Implementation Program
- Create Initiatives based on gaps identified from requirements assessment report.
- Prioritize identified Initiatives
- Assign Project Manager
- Prepare Management Reports of the Program Implementation
- Analyze reports and determine any trends or apparent problems that occur including resistance to change
- Conduct Post Implementation Reviews
- Ensure adherence to the Program
- Ensure that resources have the required skill sets
- Monitor and maintain the Implementation Program for continuous improvement
- Initiates and facilitates Top Executive meetings for Major change reviews and endorsement

The key skill required for this role include , Communication skills, Organizational skills, Facilitation skills, Leadership skills, Knowledge of the Agency, Influential, Project management skills, Presentational skills, Negotiating skills, domain expert in all Information Security areas, Strong staff management skills, some Financial skills.

The following illustration represents the roles and responsibilities



5. 2. Requirements Assessment (GAP Assessment)

The Program Manager must collect and analyze all current Information Security Policies and Procedure against the approved Information Security Policies and Procedures. Any constraints for implementing the policies and procedures will be highlighted, and the constraints and exceptions, if any, shall be communicated to all Stake Holders.

The key source information and the basis for this assessment shall be the Assessment Report from the Development Stage of this project (Refer ISPDG Development Framework for more details). The gaps or the missing policy areas identified at that stage will now determine what needs to be done to fill those gaps.

5. 2. 1. Understand Policy requirements and their impact

Program Manager must understand the Policies and Procedures documents and evaluate how these policies will effect <Organization Agency Name>. Based on the Assessment report prepared as part of the development framework, he must identify the gaps in the policies and procedures currently being followed, whether documented or not. He must identify the missing areas that would require implementation effort, for the following:

- Policies
- Procedures
- Infrastructure
- Organization Structure
- Resources

The Program Manager must report his findings to the Steering Committee and obtain their sign-off.

5. 2. 2. Assess risk of non-compliance

The missing areas identified in the analysis phase indicate non-compliance with the mandated policies. This non-compliance is an indication of security risks faced by the organization. A what-if scenario should be presented to highlight the importance of non-compliance. The Program Manager must also assess if compensating control is in place that covers the risk.

5. 2. 3. Assessment Approval

The Steering Committee will review and approve the findings report of missing areas and risk associated with non-complaince of the policies and procedures framework. The Steering Committee members may disagree with the findings provided they give justification that contradict the findings. In this case, the chair of the Steering Committee shall make necessary decisions on the acceptance of the assessment made by the Program Manager.

5. 3. Alternate Implementation Approaches

One of the major considerations during the development of this Implementation Guide is the realization that many of the government agencies may not currently have a well-established information security department and also may not have well-documented and implemented information security policies and procedures.

This would result in a major development and implementation effort to achieve compliance with the Government Mandate. It is advisable that an implementation approach be followed in line with the leading practices of the project management with the aim to apply structured management to all the efforts required to achieve this common target compliance with the mandate. The primary benefits would include end-to-end management control and visibility over the complete effort and likely optimization of resources.

This program / project approach is based on the defining multiple initiatives that result in one or more well-defined projects that are then managed by a project manager and governed in line with leading project management practices. These initiatives and projects typically combine similar or related set of activities/efforts/investments that are required to fill the security gaps identified during the assessment.

It should be noted that the project management approach described above is to be selected depending on the size and complexity of the effort required and the magnitude of the investments needed to be made by the agency.

For some agencies, an alternate approach may also be possible where significant investments or efforts are not needed and the relatively simple activities are expected to result in compliance with the Government Mandate. In such cases, the detailed project management approach may be considered as optional and the Agency management will create a set of corrective actions and assign the relevant individual tasks and activities to their staff in line with the overall compliance effort.

The subsequent sections of this implementation guide describe a structured project management approach based on one or more defined projects as part of an overall program.

5. 4. Initiatives

The Program Manager would identify and document the needed actions to cover the missing areas identified in the analysis phase. These needed actions shall be defined as specific initiatives to mitigate the associated risk of non-compliance. Initial resource requirements and other pre-requisites shall be defined for each initiative before the Program Manager will present them to the Steering Committee.

- The Steering Committee must get commitment from all members to allocate resources for each initiative.
- The Steering Committee must allocate and approve an estimated budget for each Initiative which should not exceed the initial budget set forth by Top Executive.
- The Program Manager will prioritize the initiatives and assign timelines before they are put forward to the Project Manager for execution.

The Program Owner shall approve the initiatives set forth by the Program Manager

5. 5. Projects

Once the Initiatives are clearly defined and documented, it will be the responsibility of the Program Manager to assign one Project Manager to each initiative (or group of initiative) as a single or multiple projects. The Project Manager will take each initiative and follow the Project Management cycle as stated in section 5. He must follow the priority of the initiatives as given to him by the Program Manager. The Project Manager will seek the guidance of the Program Manager for all initiatives, he will collaborate with the Program Manager in various phases of each project i.e. planning, scheduling, executing, monitoring, controlling and closing.

5. 6. Major Program Risks

The risks involved in the implementation of each policy and procedure must be identified, documented and mitigating plans must be defined. It is important to consider the degree to which, and in what ways, limits to information security can have a significant impact on implementation.

What will be the consequence of gaps in information when the initiative is rolled out?

Overly ambitious timeframes are among the most common risks in implementation. Time pressures can leave too little time to address factors for success, such as different options for program delivery, consultation with implementers and stakeholders, or resource requirements and constraints. This can result in substantial variances between funding estimates for an initiative and the resources that actually have to be employed to deliver the initiative successfully.

If the assumptions made about an initiative are clearly identified, along with their sensitivity to change, then the agency and those implementing the initiative can be better informed of the possible risks and their consequences. An awareness of uncertainties increases the chance of successful implementation, including for safety-net initiatives, demand-driven programs or wholly new initiatives, where there may be raised expectations.

Swift and significant action may be needed if important implementation risks begin to materialize. If consideration of emerging risks suggests the initiative is too large or ambitious for the agreed timelines and resource, this should be brought to the Governors attention. Appropriate responses to emerging problems will be more manageable and predictable where robust implementation contingency plans have already been developed as part of the risk management strategy.

Management must consider various tools and techniques to overcome resistance to change while executing the implementation program. They must employ change management when implementing policies and procedures within the Agency.

5. 7. Critical success factors

The critical success factors for the Implementation Program must be identified, documented and monitored. The critical success factors include

5. 7. 1. Management support

Top management support is required for any organizational change including policy and procedure implementation. The management support can be evidenced through representation of top management in Steering Committee, approval of project charter and communication to the stake holders.

5. 7. 2. Awareness and training

The human side of computer security is easily exploited and constantly overlooked. No matter how powerful the technical security underpinning of the system is, or how strong the regulations, or policies, there is still the possibility that they will be broken simply because someone subverts them. Raising the employee awareness through awareness and training programs is a critical success factor. The level of employee awareness must be measured through defined metrics such as surveys, questionnaires, number of awareness campaign conducted, and number of people attended/covered by campaigns etc.

For successful policy implementation proper awareness among the stake holders is essential. The Program Manager shall use the sample awareness plan as mandated by the Saudi Government. The awareness plan will cover the following:

- Awareness objectives
- Intended audience
- Key awareness needs of the Audience
- Techniques to be adopted for rolling out the awareness plan.
- Awareness initiatives against awareness needs
- Schedule for the awareness plan.

The Awareness Plan document is available separately as part of the set of documents received with the Framework.

5. 7. 3. Change Management

Without proper change management the implementation may face resistance from many areas. The Program Manager will develop a change management process for the Implementation Program and Projects. The process will identify key resistance areas corresponding to implementation initiatives. The plan shall cover tools and techniques to eliminate or minimize negative effects of the implementation of information security policies, procedures, and standards. The change management process is described in detail in section 7.1 of this document.

5. 7. 4. Budget

Budget is an important aspect of successful Implementation Program. Resource requirements, cost, funds and timelines must be appropriately estimated, budgeted, approved by the Steering Committee.

5. 7. 5. Enforcement and adaptation

Successful implementation happens only when appropriate policies are created, effectively implemented, accepted by all stake holders, regularly monitored for any violation or deviation with appropriate process in place to deal with violations and deviations. User awareness surveys and number of violations reported in a defined period can be considered as measure of enforcement. During the course of the policies' life cycle all these metrics shall be monitored for improvement

6. Project Management

Upon appointment of the Project Manager the initiatives identified will be converted to projects based on the priority approved by the Steering Committee.

- Planning
- Executing
- Monitor & Controlling
- Review & Closing

6. 1. Planning

Upon receiving the initiatives and assigned project, the Project Manager will need to build a plan for executing each project.

6. 1. 1. Resource Estimation

The Project Manager shall estimate the resource requirement for implementing the policy and procedures. The resources include human resources as well as technical and infrastructure resources. Based on these estimations, a budget analysis must be conducted by the Project Manager to show the approved budget fits the activities required to execute the project. Any changes required in the approved budget must be obtained from the Implementation Program Owner.

6. 1. 2. Develop Schedule

Based on the resource availability the implementation schedule shall be developed for each Initiative. The schedule must be approved by the Steering Committee and communicated to all stake holders. A project schedule in the form of a Gantt chart should be created, preferably in a project tracking tool. Describe how contingency buffers will be tapped and revised when actual performance falls behind estimates. Describe how and when schedules will be modified and how agreement and commitment to the revised schedules will be achieved.

6. 1. 2. 1. Define Milestones

A milestone is "a major event in the project" and represents the completion of a set of activities. It will be the responsibility of the Project Manager to create Milestones that reflect appropriately significant and assessable deliverables at each stage. Where the project involves a range of concurrent or parallel activities, an example is mentioned below:

Milestone	Description	Delivery Date
Project team Constitution	Create an Project team	dd/mm/yy

6. 1. 2. 2. Define Activities

An activity is “a set of tasks which are required to be undertaken to complete the milestone.» the Project Manager in collaboration with Program Manager would identify all activities required achieve the milestone of the project. An example is mentioned below:

Activities	Description	Sequence
List available employees	Provide a list of employees that are currently not engaged in other projects	
Evaluate employees	Evaluate employees based on experience and required goals and objectives as per Project Charter.	After list of employees has been provided

6. 1. 2. 3. Define Tasks

A task is simply “an item of work to be completed within the activity”. The Project Manager will then define the tasks required for each activity. The Project Manager would need to define tasks that can be quantifiable in terms of effort required by resources. An example is mentioned below:

Activity	Task	Sequence
List available employees	Contact Department Head and get a list of available employees.	First
List available employees	Compile list received from various departments into one document	Second

6. 1. 2. 4. Estimate Effort

The Project Manager will for each task listed will have to quantify the likely “effort” required to complete the task, care must be taken while quantifying effort. Defining to short a time will put pressure on the resource assigned and will result in poor quality of work. Assigning too much time will lead to reducing time in task that requires more effort and will eventually lead to delay in meeting the Project end deadline. An example is mentioned below:

Task	Effort
Contact Department Head and get a list of available employees	No. Days
Compile list received from various departments into one document	No. Days

6. 1. 2. 5. Estimate Required Resources

The Project Manager for each task identified will list the resources allocated to complete the task, the Project Manager must understand and associate key skills required to complete each task. This can be done in collaboration with the Department Head or the Program Manager. An example is listed below:

Task	Resource
Contact Department Head and get a list of available employees	Name
Compile list received from various departments into one document	Name

6. 1. 3. Budget control

The Project Manager must specify the control mechanisms used to measure the cost of work completed, compare actual to budgeted cost, and implement corrective actions when actual cost deviates excessively from budgeted cost. He must specify the intervals or points at which cost reporting is needed and the methods and tools that will be used to manage the budget. The Project Manager is responsible for tracking actual hours and for reporting actual and estimated project hours by milestone to the Steering Committee.

6. 1. 4. Quality Standards, processes and Metrics

The implementation of the policy and procedure shall follow the Agency›s quality standards E.g. Documentation standard. However appropriate process and metrics must be developed for monitoring the effectiveness and improvement during implementation and monitoring phases. Define the control mechanisms used to measure the progress of the implementation completed at milestones. Specify the methods and tools used to compare actual v/s scheduled implementation and use corrective action when actual deviates from planned.

6. 1. 5. Roles & Responsibilities

The project is more likely to succeed if there is strong executive-level support for the delivery processes for the policy. Without strong and visible top-down support, any underlying changes will be ineffective.

6. 1. 5. 1. Steering Committee (Acting as Project Steering Committee)

The Steering Committee will be regularly informed of the project status and the issues arising from the execution of the project will be addressed by them. The Steering Committee will be able to approve change made in the Project Schedule, but will ensure conformity to the mandated timeline. Further details of the roles and responsibilities are discussed in section 3.2.3, Steering Committee can have members from inside the agency or more broadly involve stakeholders, specialist consultants or representatives from another agency.

6. 1. 5. 2. Project Manager

For each Initiative to be effective a senior responsible officer is required, the Project Manager is accountable for the successful execution of the Project. This is the person to whom the Steering Committee or relevant executive turn for progress reports. The Project Manager shall play a pivotal role in ascertaining the right people have been engaged, and are working on the right things at the right time.

6. 1. 5. 3. Project Team

The Project Manager is also required to set up the most appropriate team to execute the Project. This includes the adequacy of skills of the project team. A key requirement for the Project Manager is to assign roles and responsibilities to the team members, and it is responsibility of the Program Manager to ensure these assignments are done correctly. Project Manager should draw the project team from across the stakeholders, considering the right skills to oversee the implementation of the initiative. If the right skills are not available care must be taken while assigning tasks.

6. 1. 6. Mapping of Roles and Responsibilities

The risk in deferring or not considering the formalization of cross organizational arrangements is that a lack of agreement and confusion about roles may emerge later in implementation. The key is to set up arrangements early, and to formalize them promptly. When engaging other Departments, a Memorandum of Understanding (MOU) or an agreement outlining the objective, roles, responsibilities and reporting requirements of those involved shall be considered. The Program Owner should map each section of the policy to the roles listed in the attached template. The map will be used to ensure that executives in the agency understand their responsibilities under the policy.

This template is a useful tool in establishing and communicating responsibilities and actions required at all levels. It should be distributed to relevant individuals and used as a discussion document in implementation planning.

6. 1. 7. Project Charter

The Project Manager will consolidate the preliminary information received by the Program Manager in a document called project charter. This document will have a statement of the scope, objectives and participants in the project. It shall provide a preliminary delineation of roles and responsibilities, outlines the project objectives, identifies the main stakeholders, and defines the authority of the Project Manager. It may also serve as a reference for various other projects that may result from the Initiatives.

The projector charter shall cover the following areas in general.

- Implementation Overview
  - Initiative/s Description
  - Goals and Objectives
  - Scope Statement
  - Critical Success Factors
  - Assumptions
  - Constraints
- Project Authority and Milestones
  - Funding Authority
  - Implementation Oversight Authority
  - Major implementation Milestones
- Project Organization
  - Project Structure
  - Roles and Responsibilities
  - Project Facilities and Resources
  - Points of Contact
  - Glossary
  - Revision History
  - Appendices

6. 1. 8. Communication

Communication about a policy or program initiative needs commitment and support from all those involved with implementation. This involves being 'outward-looking', that is, a view not only from the agency perspective but also from the perspective of stakeholders, and in particular on how the target audience will react and the best means of communication.

The objective of communication should be clear (and in line with the initial policy objective). This is assisted by the development of a communication strategy which also provides a means of assessing success or otherwise.

Communication is a central component of any change process. The greater the impact or change, the greater the need for clear communication of the reasons and rationale behind it, the benefits expected, the plans for its implementation and its proposed effects. Without effective communication, stakeholders may miss out on vital information and may not understand why change is needed, or the benefits to them of the change.

The objective of communication is to:

- keep awareness and commitment high
- maintain consistent messages
- ensure that expectations do not drift out of line with what will be delivered

Media management is often an important aspect of a communication strategy. The strategy may need to consider both proactive and reactive aspects of media management.

When developing the strategy it is important to allow senior management to be engaged in the process, to discuss their expectations and to provide any feedback. This also facilitates identifying how the success criteria for the initiative can be reflected in key messages of the communication strategy.

Changes to communication means and priorities may be required during implementation, in order to cater for the evolving requirements of stakeholders, particularly as their knowledge increases and demand for information grows. Monitoring of stakeholder reactions to the various means of communication assists in assessing the need for such changes and in managing expectations throughout implementation.

6. 1. 9. Procurement Plan

If new technology is required for the project, the purchase requirements must be identified and procurement plan must be prepared as per the Agency policy for procurement.

6. 1. 10. Project Approval

The project plan must be subject to Steering Committee approval and communicated to all stake holders.

6. 2. Execution

6. 2. 1. Kickoff Meeting

Project Manager shall convene a kickoff meeting with all the stakeholders explaining the Project Plan. Minutes of Meetings must be prepared, distributed and filed.

6. 2. 2. Execute the project plan

The project shall be executed in accordance with the overall approved project charter and project plan. Team Members execute the tasks assigned under each phase of the project plan. It is the responsibility of the Project Manager and the Department Head to ensure that resources assigned are executing the tasks within the given time frame.

The Execution Process ensures that planned activities are carried out in an effective and efficient way while ensuring that measurements against plans, specifications, and the original scope continue to be collected, analyzed and acted on throughout the project lifecycle. Without a defined execution process each team would execute plans using their own best practices, experience, and methods, thereby resulting in control, tracking and corrective action activities to be missed.

6. 2. 3. Execution improvement

Improvement is analyzed based on the metrics defined. Periodically data will be collected by the Project Manager, and analyzed. This information will be part of the periodic reports provided to Steering Committee. The critical success factors provide a health check of the implementation. Project Manager is responsible for performance measurement which includes finding variances between planned and actual work, cost and schedule.

Project Manager is responsible for providing Project Status Report to all key stakeholders to provide visibility. All Project Key stakeholders are responsible for the review of the metrics and variances. All Project Key stakeholders are responsible for taking necessary action of the variances thus determined so as to complete the project within time and budget.

6. 2. 4. Status reports

The purpose of the Status Report is to develop a standard format for the formal exchange of information on the progress of the project. The Status Report should be tailored to the project, but should be the same form for the full team. Status Reports should be prepared by the project team detailing activities, accomplishments, milestones, identified issues, and problems. Status Reports should follow a standard template so all reports are in the same format.

The Status Report Template (Appendix 8.2.8) should be used to report key information including:

- Current status
- Performance
- Significant accomplishments for the period
- Scheduled activities
- Issues

Along with the Status Report form, the following may be attached:

- Updated Gantt charts
- Recovery plans for activities not on schedule
- Corrective action plans for expected problems
- Resolution to assigned action items

6. 2. 5. Procurement and implementation

During the Execution Phase the Agency may require purchasing products or services needed to implement the policies and procedures e.g. Access control system etc... In these cases, the Procurement Plan shall be put into action. An Agency may have a defined set of guidelines and policies that provide the infrastructure for project purchasing which should be integrated within the Procurement Plan.

These guidelines will outline the policy for solicitation, source selection, and contract administration. Although the solicitation and contracting responsibilities themselves may not always be managed by the Project Manager, it is still important that the Project Manager have a fundamental understanding of the contracting and procurement policies.

6. 3. Monitoring and control

Effective implementation monitoring and review enables agencies to ensure that adequate resources continue to be available to deal with the scope, risk and sensitivity of the Project. It also, enables stakeholders to assess the project progress, identify and address problems and review its ongoing relevance and priority. Monitoring and review is more effective when it is performed by personnel with skills and knowledge specific to the project being undertaken and who have adequate administrative resources to process routine monitoring data.

Monitoring and reporting requirements should reflect the importance of the initiative and its non-complaince risks and have regard to the administrative burden that data collection and reporting places upon the project team and other agency resources. Reporting is most effective when it delivers the right level of detail for accountabilities at each agency level.

6. 3. 1. Performance measurement (KPI)

Early identification of appropriate data sources assists in establishing timely and effective monitoring activities. The timely reporting of key issues and trends may have a higher priority than the precise accuracy of underlying data, particularly for higher risk initiatives.

Where a project has multiple initiatives it is important that any concerns or lessons from each stage are assessed, escalated as necessary, and resolved. Issues arising should be appropriately addressed before the project progresses to the next stage.

Evaluating a project can assist in determining the extent to which the tasks performed contribute in achieving the initiatives defined. Key lessons learnt may make a significant contribution to the delivery of future initiatives. Evaluations should aim to identify lessons that may help in the future to:

- Improve project execution and decision-making
- Help resource allocation
- Enhance accountability in terms of assessing what outcomes were achieved
- Promote organizational learning and good practice.

6. 3. 2. Scope verification

Scope Verification shall focuses on insuring that the policies and procedures are implemented correctly and meet the organizational objectives.

Scope verification is achieved through formal reviews of the implementation. Once the implementation is complete, the Steering Committee after reviewing the status shall sign of the implementation complete report.

6. 3. 3. Recommend changes and corrections

The changes or deviations if any from the approved plan shall undergo the change management process. The Project Manager shall recommend the request to the Steering Committee after analyzing the risk involved and mitigating controls. The Steering Committee will take informed decision on whether to approve or reject the change.

7. Risk monitoring

Risk identification, monitoring and resolution are key tools to successful completion of the implementation. The risk management process begun as part of Project Planning and is kept current until Project Closeout. The key elements to this process are:

- Creating a central repository for risk information and associated documentation of risk items and resolution strategies
- Summarizing information on a risk form
- Including a risk summary in the regular status meetings
- Providing a consistent and ongoing evaluation of risk items and development of risk strategies:
  - Identify the risk
  - Evaluate the risk
  - Define a resolution

7. 3. 1. Report performance

The Project Manager shall collect and consolidate data on project status. These reports shall be forwarded to the Steering Committee. The Steering Committee shall review the reports during the weekly performance review meetings.

7. 3. 2. Progress review meetings

The Steering Committee shall hold periodic progress review meetings to review the implementation status. Project Manager's reports will be discussed. Steering Committee shall take decisions on change requests. Major review areas shall include

- Schedule variance
- Budgets variance
- Resource changes
- New risks / unforeseen circumstances
- Plan changes

Minutes of meetings of all progress review meetings shall be documented and filed.

7. 1. Closing

The policies and procedure implementation project shall be formally closed after a formal review of the implementation by the Steering Committee. Once successful implementation is evidenced, the Steering Committee shall report to the management the status to gain the formal acceptance. The Steering Committee shall then sign off the project completion and release the resources allotted. The formal closing process shall include :

- Review implementation
- Gain Formal acceptance
- Final reporting
- Index and Archive records
- Update lessons learned
- Sign Off
- Release resources

Chapter 4
Implementations Challenges

1. Overview

This section provides an overview of the Change Management Plan to be used by <Organization Agency Name>. The document details roles and responsibilities that are assigned in the change management process which are:

- Change Process Owner
- Change Manager
- Change Initiator
- Change Analyst
- Steering Committee

The document also details the phases of change management process:

- Initiate Change
- Assess Change
- Categorize Change
- Test Change
- Approve Change
- Plan & Schedule Change
- Implement Change
- Review implementation

Change management plan provides tools and techniques required to manage individuals, teams and departments when bringing about change in their environment and measuring its effectiveness.

2. Roles & Responsibilities

It is essential that roles and responsibilities be assigned before the change management process is initiated. This will help the change management process as each process requires accountability and ownership. Through these roles, the relevant management and staff will have a clear understanding of their responsibilities and functions within each phase of Change Management.

<Organization Agency Name> are required to define roles and responsibilities that support the change management process. The responsibilities defined would govern the objective of change brought about by the Information Security policy and procedures.

2. 1. Change Process Owner

Change process owner for changing Information Security policies and procedure must be assigned outside the Information Security Department as not to create a conflict of interest. Accordingly, the Top Executive must be assigned ownership of the change process.

The change process owner would be accountable for the complete process and would be responsible for ensuring that the Change Management process is being followed correctly. Other responsibilities include

- Maintain the goals and objectives within the process,
- Design and recommend metrics and reports for management.
- Provide a fully functional Change Management process resulting in employee satisfaction
- Ensure that resources have the required skill sets
- Maintain continuous process improvement on a regular basis.

The key skills required for this role include having Influence over all organization, Communication skills, Organizational skills, Facilitation skills, Leadership skills, Knowledge of the <Organization Agency Name>, Project management skills, Negotiating skills, General Technical knowledge, Strong staff management skills, Financial skills.

2. 2. Change Manager

Change Manager for changing Information Security policies and procedure must be assigned from within the Information Security Department as he would have better understanding of the Information Security environment. According to industry standard practices, this can be an additional role of Information Security Manager/ Chief Information Security Officer depending on the <Organization Agency Name> structure. As defined in the earlier sections, this person will also be the Program Manager of the Information Security Implementation Program.

Change Manager is responsible for approving or rejecting applications for change after Information Security Steering Committee review, other responsibilities include:

- Assess likely impact of Change to the live environment
- Assess the implementation resources required for the Change
- Assess the ongoing costs of the Change as appropriate
- Assesses the impact of not doing the Change
- Approve acceptable changes endorsed by the Steering Committee or Top Executive for Significant and Major change
- Validate prioritization of Change
- Validate Change category
- Validate completeness of Change
- Conduct Post Implementation Reviews,
- Review Management Reports – KPIs (See if targets have been met, issue corrective measure for non achievable targets).
- Analyze Change records to determine any trends or apparent problems that occur including resistance to change
- Identify and document changes that by-pass the Change Management process and provides information to the Change Process Owner to address compliance requirements
- Assist the Change Process Owner in identifying and prioritizing process improvements
- Ensure adherence to the process
- Initiates and facilitates Top Executive meetings for Major change reviews and endorsement
- Routes Significant and Major Changes to Steering Committee or Top Executive review
- Communicates with all necessary parties to coordinate Change build, test and implementation
- Update the Change log with all progress
- Review outstanding change awaiting consideration or awaiting action

The key skills required for this role include , Communication skills, Organizational skills, Facilitation skills, Leadership skills, Knowledge of the <Organization Agency Name>, Influential, Project management skills, Presentational skills, Negotiating skills, domain expert in all Information Security areas, Strong staff management skills, some Financial skills.

2. 3. Change Initiator

Change Initiator for changing Information Security policies and procedure can be assigned within the Information Security Department as he would have better understanding of the Information Security environment. According to industry standard practices this can be an additional role of the relevant Information Security Staff/ IT Staff depending on the <Organization Agency Name> structure.

Change Initiators primary responsibility will be to receive Change notices from the Project Manager(s) and record them in a Change application, here the Change Initiator would be required to complete all mandatory information for the Change.

The key skills required are:

- Communication skills
- Knowledge of the <Organization Agency Name>
- Information Security knowledge

2. 4. Change Analyst

Change Analyst for changing Information Security policies and procedure must be assigned from within the Information Security Department as he would have better understanding of the Information Security environment.

Change Analyst will receive the Change Application along with the Information Security policies & procedures to be implemented. His primary responsibility is to assess the current state of policies and procedures and check them against the newly generated policies and procedures thereby creating a GAP analysis between the two states. Change Analyst would also be required to conduct a SWOT (Strength, Weakness, Opportunity, Threats) analysis for newly generated policies and procedures i.e. what are the strengths of having this policy and procedure implemented, what are weaknesses that this policy and procedure implementation is covering, what opportunities will be available to the <Organization Agency Name> by implementing this policy and procedure and what are the threats it might encounter by implementing this policy. A sample of a GAP analysis and SWOT analysis can be found in the appendix.

Other responsibilities of a Change Analyst include:

- Initial assessment of the Change Application and return incomplete Change Application to Change Initiator
- Participate in the Post Implementation Review as necessary
- Participates in the Steering Committee meetings as needed

The key skills required for this role include:

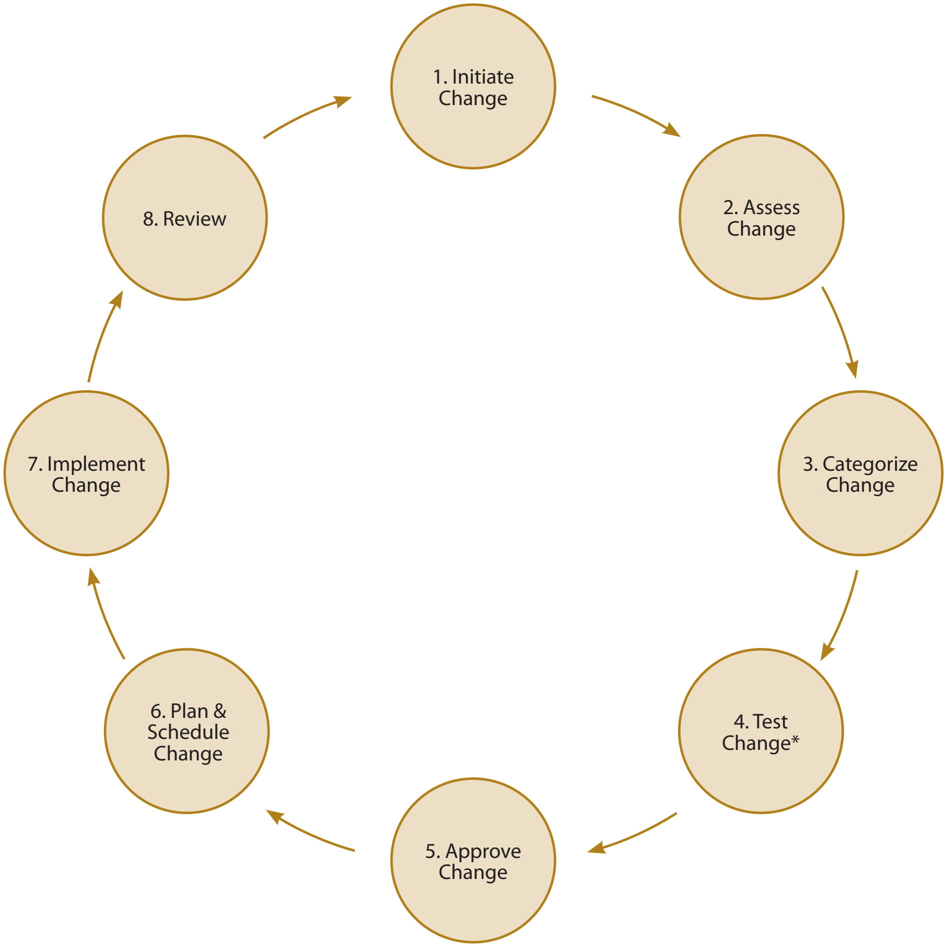
- Communication skills
- Organizational skills
- Knowledge of <Organization Agency Name>
- Strong Analytical Skills
- Data Collection Experience/Skills
- Strong Information Security Technological Skills specific to environment, back-end systems

2. 5. CAB: Change Advisory Board (Information Security Committee acting as CAB)

The Steering Committee will act as a Change Advisory Board for newly generated policies and procedures. The primary function of Steering Committee is to review the changes proposed and make sure they are in line with the Information Security policies and procedures Framework. Steering Committee responsibilities include

- Review Change Applications that are submitted to Steering Committee
- Evaluate modified Significant and Major Changes for schedule impact
- Participates in the scheduling of Significant and Major Changes
- Validate the prioritization and Change Category
- Reviews applications for Change and advise the Change Manager to approve/reject the application
- Considers all Changes on the agenda and advise the Change Manager about which Change should be approved
- Participates in Post Implementation review as needed
- Review Post Implementation Reviews as needed

3. Change Management Process



** Note: In certain scenarios testing is required to verify the changes being implemented do not adversely affect <Organization Agency Name> systems, applications and their day to day operations.*

The primary objective of change management is to record, evaluate, authorize, prioritize, plan, test, implement, document and review change of Information Security policy standards and procedures in a controlled manner. Secondary objective of change management is to ensure transition occurs in a smooth fashion this generally means dealing with issues relating to resistance to change.

<Organization Agency Name> are required to follow below mentioned change management process in order to change their existing policies and procedures.

3. 1. Initiate Change

Once the Change Initiator receive a formal notice the changes required, he will submit a Change Application to begin the Change Management process. The Change Application is then forwarded on to the Change Analyzer for assessment of change. The following are the steps that are followed in this phase:

- Change Initiator submits Change Application
- Change Initiator records basic details (name of Department, affected users)
- Forward to Change Analyzer

3. 2. Assess Change

Change Analyzer will assess the change required in collaboration with the Change Manager which includes:

- Financial
- Technical
- Business impact.

The availability of resources and scheduling is also considered in the assessment. After the assessment, the Change Manager will be advised as to whether to approve the RFC. If the RFC is approved, it will proceed for planning, implementation and testing. If the RFC is not approved, the Initiator is responded to with an explanation.

The change is accepted based on the completeness of Change Application information. Rejected Change Applications are returned to the Initiator with an explanation for the rejection. The following are the steps that are followed in this phase.

- Review Change Application for completeness of information
- Accept or Reject Change Application based on completeness of mandatory information
- Anticipate resistance to change and apply tools and techniques to combat resistance to change (Please refer to appendix II for tools and techniques for resistance to change)

3. 3. Categorize Change

The Change Analyzer assesses the change in collaboration with the Change Manager to determine the category of change whether it is minor, significant or major.

This can be determined by asking questions such as:

- which policy will be changed i.e. determine if a policy already exists
- which users will be affected by this policy i.e. manager or staff
- which procedure will be change i.e. determine if a procedure already exists
- which users will be affected by this procedure i.e. Manage or staff
- what technological changes will be required to be implemented in the current IT setup

whether new hardware equipment and / or software will be implemented to the production environment as a pre-requisite to support the new policies and procedures

3. 4. Test Change

Testing of change would be required in certain scenarios where applications and systems are involved. The Change Analyzer would use a test environment with the help of Information Technology Department to deploy changes needed to implement certain policies and procedures.

The testing of the change should provide the Change Analyzer the following outputs:

- Potential problems
- Hardware limitations
- Software limitations
- User feedback

3. 5. Change Approval

Steering Committee is responsible for considering the risk to the <Organization Agency Name> of any Change. Through the normal workflow, the Change Manager will assign a Change Category of minor, significant or major in collaboration with Change Analyzer. The Change Category determines the management level that is included in the assessment of the Change. After the assessment, the Steering Committee will be advised as whether to approve the Change.

The change is either approved for continued processing or is rejected and explained to the initiator.

- The Change Manager assesses the resources and impact on the IT infrastructure referencing the policies and schedules the Change categorized as Minor based upon the Service Level Agreements and inform the Steering Committee of the actions taken.
- The Change Manager circulates the Change Application to the Steering Committee members for assessment prior to the formal Steering Committee meeting.
- The Change Manager forwards the Change Application to Top Executive for business and financial assessment. The Change Manager will also inform the Steering Committee.
- Top Executive endorses or rejects the Change Application categorized as Significant or Major. If the Change Application is endorsed, Change Application goes to the Information Security Steering Committee.
- Steering Committee members assess the resources and impact on the IT infrastructure referring to the Configuration database and Service Level agreements as necessary.
- The Steering Committee advises the Change Manager of the acceptance of the Change to the environment as well as priority and schedule.
- If the Change Application is rejected, the Change Application is closed and logged with the reasons for the rejection. The Initiator has the right to appeal.

3. 6. Plan & Schedule Change

Approved Changes are turned over to Project Manager for planning and implementation.

Change Manager will assist in the coordination, communication, and the scheduling of the authorized change. He also validates that the back-out procedures or the remediation plans are prepared and documented in advance.

Once the Project Manager has completed his planning and scheduling including creating work schedules for the Change, he must get an endorsement from the Change Manager or the Steering Committee before actual execution of the plan. Once endorsed the Project Manager will distribute the Project Plan to all stakeholders and would communicate the start of the Change implementation.

3. 7. Implement Change

Each resource will be assigned a specific task and it is the responsibility of the Project Manager to ensure all tasks are being performed as per the plan, any deviations must be reported to the Steering Committee.

Steering Committee monitors the progress of the Change Application through this process and provides the oversight to the entire implementation process. Project Manager consults with Change Manager during the implementation process for any deviations from the approved Change Application.

Following implementation, the Change Manager will determine if the required results were produced. The Change Manager will authorize if the back-out plan is to go into effect and is implemented.

3. 8. Review

The Change Manager reviews Change Application according to the Post Implementation Review Policy.

- After a pre-defined period, the Change Manager conducts a Post Implementation Review (PIR) per the PIR Policy. The results are documented in the Change Application and are provided to the Steering Committee for review.
- The results will be used as input for the improvement activities for the Change Management process.
- If the results of the PIR are not satisfactory, the Steering Committee members re-examine the original Change Application and decide what actions to take. This may involve requesting a new Change Application after closing the original RFC.
- If the results are satisfactory the Change Application status is moved to Close.

4. Resistance to change - Tools and Techniques used to manage

In any large program implementation, resistance to change can pose a real threat to the success of the change being brought in. In most cases, it is the key to overcome and/or manage this resistance to achieve the goals.

ADKAR is a goal-oriented change management model that allows change management teams to focus their activities on specific results for an Agency, The goals or outcomes defined by ADKAR are sequential and cumulative. The Change Manager must obtain each element in sequence in order for a change to be implemented and sustained. This model can be used to identify gaps in the Change Management process and provide effective coaching for employees of an Agency. The ADKAR model can be used to:

- diagnose employee resistance to change
- help employees transition through the change process
- create a successful action plan for personal and professional advancement during change
- develop a change management plan for your employees

The ADKAR model has the ability to identify why changes are not working and help take necessary steps to make the change successful.

4. 1. Awareness

The objective of awareness is to make all level of staff aware why the upcoming change is needed. Employees of an Agency should understand the change implemented is to improve the level of security for information assets, which will eventually lead to overall success.

4. 2. Desire

It is imperative that management encourage the desire of their employees to support and actively participate in the forthcoming change, regardless of the immediate appeal or flash of the new procedures or processes.

4. 3. Knowledge

Management must provide the training and education to its staff of the methods of changing to the new policies, procedures and Information Security function. High levels of awareness and desire will often be useless without the necessary knowledge of how to change to accomplish the goals desired.

4. 4. Ability

Along with the knowledge of how to affect successful change, everyone involved needs to be given the specific training and information to achieve success in implementing the details of the defined changes. Workshops, online training are a critical component of delivering the education the employees needs to make the changes successfully.

4. 5. Reinforcement

To successfully implement change senior management should use repetition and reinforcement, if an employee repeats a task for a long period i.e. a month religiously, he will create a habit. Reinforcing the new "habits" of employees typically improve the success of the changes made, these reinforcement can done through promotion, appraisal and various motivational techniques.

Concentrating on awareness, desire, and knowledge, is the foundation that provides the base for the acceptance of change and the ability to successfully implement the new policies and procedures. With the use of the base foundation and a follow up with strong reinforcement, the natural human reluctance to accept change can be eliminated. This will create a strong team effort to make the coming developments proceed smoothly and very successful. Implementing ADKAR properly often translates into change management devoid of trauma, stress, and regression.

Chpter 5

Information Security Policies and Procedures Awareness Plan

1. Introduction

An Information Security Awareness program enhances the effectiveness of security controls that have already been implemented. Employees aware of their security responsibilities provide a powerful deterrent against threats both known and unknown.

This document presents the process and methodology that <Organization Agency Name> must follow in implementing and maintaining a Security Awareness program. Further it outlines the roles and responsibilities, program elements and sample schedule of the program.

2. Overview

The Security Awareness Program is an important element of a successful Security Program Implementation process.

This Awareness plan developed by the Security Awareness Program Owner at <Organization Agency Name> must follow a Project Management Approach so as to yield best results. The five phases of this program are:

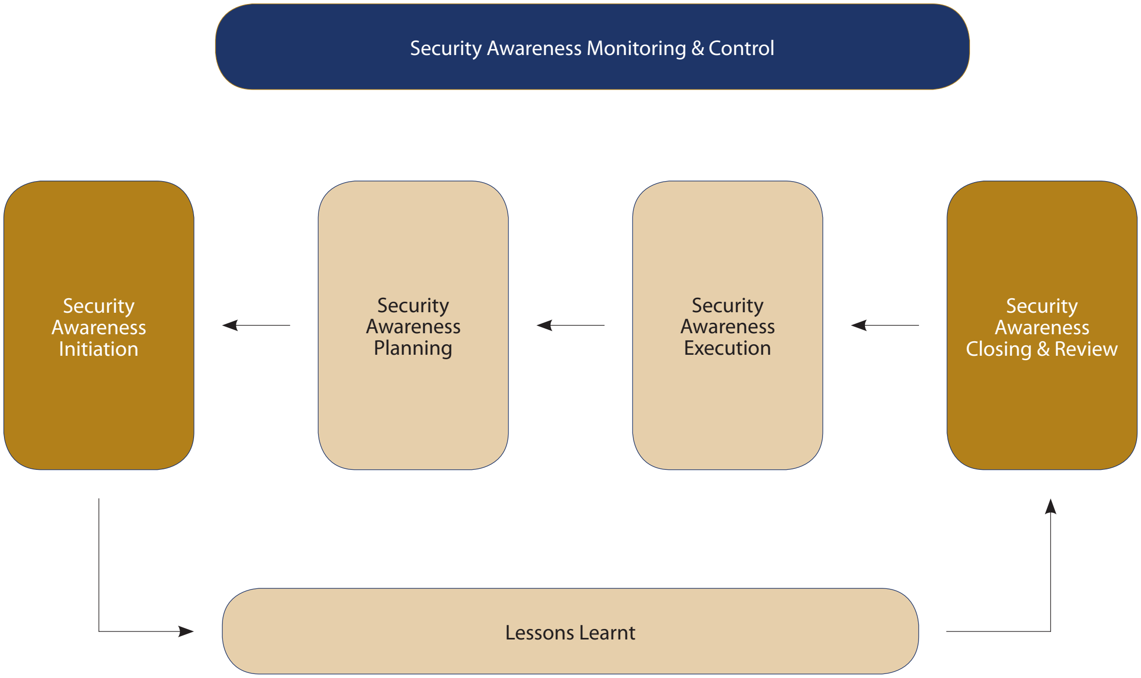
- Security Awareness Initiation
- Security Awareness plan
- Security Awareness Execution
- Security Awareness Monitoring and Control
- Security Awareness Closing and Review

This approach allows <Organization Agency Name> to develop training programs that is most suitable to its requirements, deliver a quality product against an agreed timeline and monitor effectiveness of the Security Awareness program.

3. Security Awareness Program Methodology

This section illustrates the overall process and sub-processes for deploying the Security Awareness program. In order to deploy the program in a time bound manner, a project management approach is followed.

As Security awareness is a continuous process, it is intended that the program is operated for a 12 month period, results are reviewed on an ongoing basis and adjustments/enhancements are identified in the objectives and scope of awareness plan for the next period.


Security Awareness Monitoring & Control
Security Awareness Initiation
Security Awareness Planning
Security Awareness Execution
Security Awareness Closing & Review
Lessons Learnt

3. 1. Security Awareness Initiation

This represents the start of the Program. The key purpose of this phase is identifying the scope, objectives and constraints related to the program, defining Security Awareness roles and responsibilities. Project Management is a critical successes factor in this phase.

3. 1. 1. Allocating Roles and Responsibilities

The roles and responsibilities must be clearly defined and allocated. Please refer to Appendix 1 for further details.

3. 1. 2. Identifying a Project Manager

The Project Manager manages the Project through its life cycle. He determines the scope, budget, project management plan and monitors the progress of the security awareness. He understands the constraints that may hamper the smooth running of the program and initiates approval processes.

3. 1. 3. Identifying <Organization Agency Name> Security Awareness Requirements

Security Awareness requirements will depend upon identifying needs, estimating effort and prioritizing training plans:

3. 1. 3. 1. Identifying needs

Identify the results of previously conducted programs or perform a current state assessment against a security baseline. A focused training program must then be developed to address this knowledge shortfall.

E.g. Security knowledge in a particular security domain (Access Control) was found to be less that the expected baseline value. Or

The results of the last Internal/External Audit showed significant findings in high risk policy areas.

Identify the most important policies in terms of impact of lack of awareness. The topics will include but not be limited to the following areas:

Table 4

Security Management	Information Classification	Risk Management	Physical (and Environmental) Security
Personnel Security	Security Awareness Training	Security Incident Response	Security Monitoring
Network Security	PC/Workstation Security	Support and Operational Security Related	Encryption and Information Confidentiality
Media Security	Identification and Authentication Mechanisms	Systems Life Cycle Security	Business Continuity Planning

3. 1. 3. 2. Prioritizing awareness areas

<Organization Agency Name> must priorities areas for training. Two levels of Training are Basic and Focused.

Basic Training covers all staff, Third Party Contractors, HR/Administration

Focused Training on the other hand covers Information Security Personnel and IT Operations Personnel. This will include Vendor training and/or other specialist training.

Refer to Table 2 for training focus areas.

It is important that Focused Training for IS Personnel are conducted before implementing Basic awareness or focused training for IT Staff.

3. 1. 4. Defining the Objectives of the program

Security Awareness objectives are high level goals set out by <Organization Agency Name> and drive the program. The program should initially concentrate on specific security messages in a sequence that enables <Organization Agency Name>'s staff to progressively educate, absorb and apply the security policies towards daily business activities.

The defined objectives must be measurable at the end of the program.

E.g. 70% of staff understood the central message of the Password policy campaign

3. 1. 5. Defining the scope of the program

The scope of the program will focus upon what target audience must be reached and the tools employed

Who is the target audience?

3. 1. 5. 1. Identifying the target audience is important as awareness programs need to be tailored to specific requirements.

The following table describes the target audience with respective awareness focus areas, that <Organization Agency Name> needs to reach through its Security Awareness.

Table 5

Target Audience	Security Awareness Focus Area
Senior Management	Security Management Responsibilities; Endorsing and Supporting Security Initiatives; Reviewing program progress and effectiveness
Information Security Management and Staff	IS Framework, Policies, Procedures and Standards, IS Audit, Business Continuity, Disaster Recovery
General Public	<Organization Agency Name> Security Policies; Acceptable Use; Incident Reporting;
IT Operations Management and Staff	Security Responsibilities; Business Continuity Plan Testing; Disaster Recovery Procedure
Third Party Contractors/Consultants	Security Responsibilities
Administration Department Management and Staff	Physical Security Policies and Procedures; Business Continuity Procedures
HR Department Management and Staff	Security Responsibilities; Employment Entry/Exit Procedures; Disciplinary Process

3. 1. 5. 2. What program tools will be used?

A number of tools exist that can be incorporated into the Security Awareness program as illustrated in Table 3. In the long term, a variety of tools must be employed for any particular policy domain so as to maintain end user interest and improve learning.

The following tables provide a description and relative cost of various tools and their suggested frequency of use.

Table 3

Component	Description
Organization wide Awareness Tools	The following organization wide awareness tools should be designed and developed. **Governor's Message:** This document would elaborate on <Organization Agency Name>'s expectations from its employees with respect to information security **Employee Handbook:** This document would provide the basic information security guidelines to all the employees of <Organization Agency Name> **E-Learning Module:** Depending upon the Information Security requirements of <Organization Agency Name> an e-Learning module may be developed. This e-Learning module would provide detailed information on several topics related to information security like Backup, Email, Incident Management, Internet Usage, Virus Protection, Data Confidentiality etc. **Frequently Asked Questions:** The Frequently Asked Questions will serve as a quick reference for security related queries of the employees. These FAQs must be hosted in an Intranet location for general viewing.
Internal Publications	<Organization Agency Name> can spread awareness messages via a variety of Internal Publications related to topics of greatest concern to it. The internal publications that can be designed for this purpose are as follows: **Posters and Screensavers:** Posters and Screensavers attract attention of employees to basic information security matters. Posters should be frequently changed to retain impact. In addition, posters should be professional in presentation and consistent with other posters throughout the organization **Brochures and Pamphlets:** <Organization Agency Name> should develop brochures and pamphlets with concise, eye-catching messages related to information security **Security Newsletter:** Dedicated "Information Security Newsletters" can be designed and developed in order to impart knowledge of different information security issues. E.g. The latest published Patches, Critical Virus/Malware alerts, new security controls implemented at <Organization Agency Name>.

Component	Description
Intranet Portal	An intranet webpage is a good mechanism that introduces the staff/contactor to the Information Security related policies, procedures, standards, FAQs and surveys. Additionally all of the internal publication listed above would also be available on the intranet portal.
Security Awareness Assessment Tools	<Organization Agency Name> must design and develop the templates of assessment tools so as to regularly gauge the level of security awareness amongst the employees. Templates for following assessment tools must be developed as a part of this phase: Surveys: The surveys would contain the questions pertaining to information security and <Organization Agency Name>'s information security policies and procedures in specific areas. Quizzes and Puzzles: The quizzes and puzzles would be related to the areas of information security and would help <Organization Agency Name> to measure the level of security awareness of the employees Baseline Templates: The templates would serve as a score card to measure the level of security awareness of the employees. These templates will be used prior to and after the program implementation so as to quantify the effectiveness of the Security Awareness program Intranet Portal can be effectively used for this purpose.
Presentations	<Organization Agency Name> will design and develop the relevant Security Awareness course content for the following target audience: Top Management: The presentation for top management would contain more generic and concise security messages **New Joiners:** This presentation will contain the basics of information security and <Organization Agency Name>'s information security practices **Trainers:** This presentation will impart training to the trainer so that he can educate all the employees of <Organization Agency Name> on an ongoing basis Intranet Portal can be effectively used for maintaining an online archive of such presentations for subsequent reference purposes.

Delivery Methods

Table 6

Tools and Techniques	Typical Cost Implication	Suggested Frequency	Examples
Pamphlets/ Brochures	Low	Half-yearly or Annual	Security awareness tri-fold brochures to be distributed to all current <Organization Agency Name> information resources users; Laminated card with security reminders
Video	Medium-High	Ad-hoc once in 3 or 5 yrs	Short one minute videos that permit tailoring to <Organization Agency Name>'s specific technology, organization, business issues, and objectives, and can be more closely related to existing security awareness program initiatives and strategy.
Screen Savers	Medium	Half yearly	Changing pattern of screen savers with computer security messages.
Posters	Low	Annually	Poster series with new posters available annually. Series of carefully designed posters to be brief and concise in their presentation of a variety of computer security concerns. Useful in lobby areas, cafeteria, bulletin boards, break rooms etc.
Newsletters/ Articles	Medium	Monthly	Newsletter published quarterly dedicated to information security. It can be customized with <Organization Agency Name>'s name and logo.
Intranet	Low	Updated weekly	An Intranet site provides an excellent platform for dissemination of <Organization Agency Name>'s information security policies.
E-mail, Voice-mail	Low	Every Quarter	Publicize simple messages via e-mail (or voice mail) to alert employees to information security related matters within selected areas, buildings or offices
Promotional Items	Medium	Ad-hoc	All items with security awareness program logo or message such as mouse pads, pens, plastic cups, plastic mugs, etc.
In-house Awareness Items	Low	Ad-hoc	Scratch pads/memo pads/Selected <Organization Agency Name> printed document like Salary Statement with security awareness logo.
Presentations/ Classroom sessions	Low	Twice monthly or Annually	Security awareness sessions can be scheduled once or twice monthly depending upon attendee numbers. New Joiner attendance is mandatory. Existing employees must attend once a year.

3. 2. Security Awareness Planning

During this phase the project team is created, budget and schedules are prepared and Baseline metric is developed.

3. 2. 1. Create a Security Awareness Implementation team

The team members chosen must have good Information security knowledge. They must also possess good inter personal and presentation skills.

Choosing the right resources for the implementation team will depend upon the chosen delivery mode. The following are skill sets and competencies that resources must possess.

Table 7

Skill Set / Competency	Description
Information Security Knowledge	Domain Expert in all Information Security areas
Proof Reading/ Quality Analysis	QA of all draft materials to analyze errors in language, quality
E-media skills (External Agencies if applicable)	Skills required to develop Documentation and layout; Flash media; Email content; Screensaver; Video
Print Media (External Agencies if applicable)	Skills required for preparing Brochures, Posters, Calendars etc.

3. 2. 1. 1. Develop a baseline

A baseline must be set that will provide a mechanism to test the effectiveness of the chosen delivery tool.

E.g. 70% of new joiners who attended the Security Awareness class sessions provided positive feedback.

3. 2. 1. 2. Develop a security awareness plan (in the form of a schedule)

A schedule must be developed with clearly defined milestones in terms of awareness training/messages to be rolled out for various segments of the audience (as identified above), frequency and timing of the messages, awareness content and the channel to be used. Each of these factors should be chosen carefully in view of the cost impact on the awareness budget of the organization.

A sample awareness plan is attached in Appendix 1

3. 2. 1. 3. Develop a security awareness Budget

The Project Manager must prepare a budget that is within the annual budget allocation for Security Awareness activities.

Table 6 is an illustrative example of budget (illustration only and not actual cost)

Table 6

Budget Item	Number of Units	Unit Cost	Total Cost
Information Security Awareness videos	99	SAR 999	SAR 99999
Information Security Awareness poster sets	99	SAR 999	SAR 99999
Quarterly Information Security Newsletter - 4 issues	99	SAR 999	SAR 99999
Information Security Web site materials initial design	99 FTE hours	SAR 99999	
Information Systems Security Association memberships for 99 central staff and 99 regional staff	99	SAR 999	SAR 99999
Free weekly security e-mail available through SANS		SAR 0	
Travel expense for central security staff to visit remote sites to assist in training	99	SAR 999	SAR 99999
Human resources effort (Internal)	9999 FTE hours		SAR 99999
Specialist Training			SAR 99999
Total estimated expenses:			SAR 99999

3. 2. 1. 4. Communicate Program kick off

Communicate the formal kick off to the project sponsor about the start of the program.

3. 3. Security Awareness Execution

In this phase all training materials are developed and disseminated as per the schedule. The following are the key activities:

- Prepare Training Material for the program
- Perform a review of the developed material and incorporate changes if any.
- Perform a final QA of the draft and incorporate changes if any.
- Determine final version for deployment.
- Adapt material into chosen delivery method
- Perform QA and approve final version.
- Deploy the delivery tool

3. 4. Security Awareness Monitoring and Control

Throughout the Security Awareness Planning and Execution phase the project is monitored and controlled. Any issues or hindrances that will affect the project timelines or objectives of the program must be identified and rectified. Any outstanding issues must be notified to the IS Steering Committee. The following are some key activities:

- Monitor the progress of the plan against the milestone list.
- Monitor obstacles and perform corrective actions.
- Facilitate conflict resolution and notify the IS steering committee/program sponsor if additional help is required.
- Provide a monthly status report of the program to all stakeholders.

3. 5. Security Awareness Closing and Review

During this phase the annual program is closed and the effectiveness is measured against the baseline determined during the Security Awareness Planning phase.

The key activities of this phase include measuring effectiveness and Updating lessons learnt.

3. 5. 1. Measure Effectiveness

Table 8

Survey Method	Choose Sampling size A sample size must cover at least 15-20% of staff size
	Identify risk topics for survey Choose high risk policy areas or those topics with low awareness
	Prepare the survey and obtain approval from Security Awareness Owner.
	Conduct Survey, Analyze the results and compare against baseline metric
	Communicate the results The Security Awareness Owner will distribute the survey results to select persons in strictest confidentiality
	Follow-up actions All results are collated and will form the cornerstone for the following years Security Awareness
Other Techniques	IS Audit Perform a desktop audit for instance to see whether passwords are written down and posted around computer terminals; See if confidential files are left unattended.
	Social Engineering Use social engineering techniques like masquerading and test whether helpdesk or front desk follows security guidelines while providing customer assistance.

3. 5. 2. Update lessons learnt

All lessons learnt during the program must be discussed within the project team and studied to help further improve the Security Awareness effectiveness.

Chapter 6
Information Security Department Placement Option

1. Introduction

This document presents Information Security Department placement options for the <Organization Agency Name>. It explains the various aspects of defining an Information Security function, the necessary roles and responsibilities required for an effective Information Security function according to Industry Standards.

2. Overview

This document will provide an overview of various options with regards to establishing an Information Security function within <Organization Agency Name>, the document details roles and responsibilities that are required within the Information Security function. Furthermore, this depicts the required processes to establish an Information Security Function, which includes:

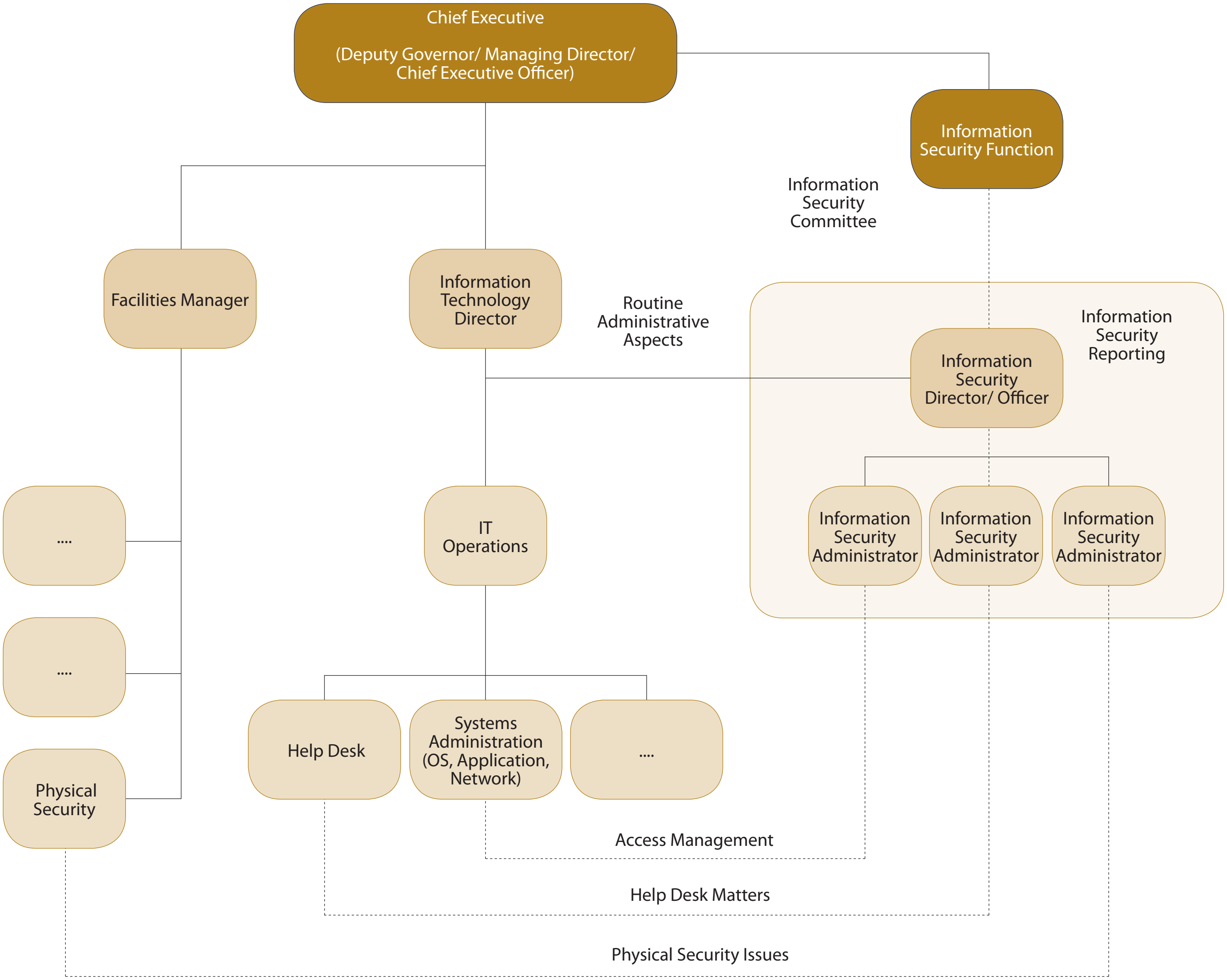
- Initiating
- Planning
- Executing
- Monitoring & Controlling

In today's complex Information system environments, Information security plays an important role to ensure critical data's integrity, confidentiality, and availability. The dramatic expansion in computer interconnectivity and the exponential increase in the use of the Internet are positively changing the way government agencies communicate and conduct business. However, with the advancement in technology, vulnerabilities are introduced leading to the risk of losing critical information. Knowing the risks, governmental agencies should be aware of the need for an Information Security Department that monitors and controls the risks and threats surrounding the information security. Just like other functions, the information security has key functions that need to be planned, developed, implemented, monitored and controlled.

3. Information Security Department Placement Options

Based on the size and complexity of an Agency, there are three options that are available for Information Security Department Placement. A detailed description, advantages and disadvantages are included for each of these options. A recommendation is also included for each option and this must be carefully read and understood by the agency.

3. 1. Option 1


Chief Executive
(Deputy Governor/ Managing Director/ Chief Executive Officer)
Information Security Function
Information Security Committee
Facilities Manager
Information Technology Director
Routine Administrative Aspects
Information Security Reporting
Information Security Director/ Officer
....
IT Operations
Information Security Administrator
Information Security Administrator
Information Security Administrator
....
Help Desk
Systems Administration (OS, Application, Network)
....
Physical Security
Access Management
Help Desk Matters
Physical Security Issues

The first option is designed and structured for a small size Agency with a low risk profile, care must be taken while following this structure as it might cause a conflict of interest. Clear segregation of duties must be defined taking into consideration the constraints of size and budget of an Agency.

In this option the Information Security Head has an information security reporting line established with the Information Security Committee; where as the administrative aspects of Information Security are managed under the supervision of Information Technology head. The colored dotted lines represent consultation requirements between various departments and Information Security function.

The roles illustrated in Option 1 are explained further in section 4.1.1, the key advantages and disadvantages for above stated option are as follows:

3. 1. 1. Advantages vs. Disadvantages:

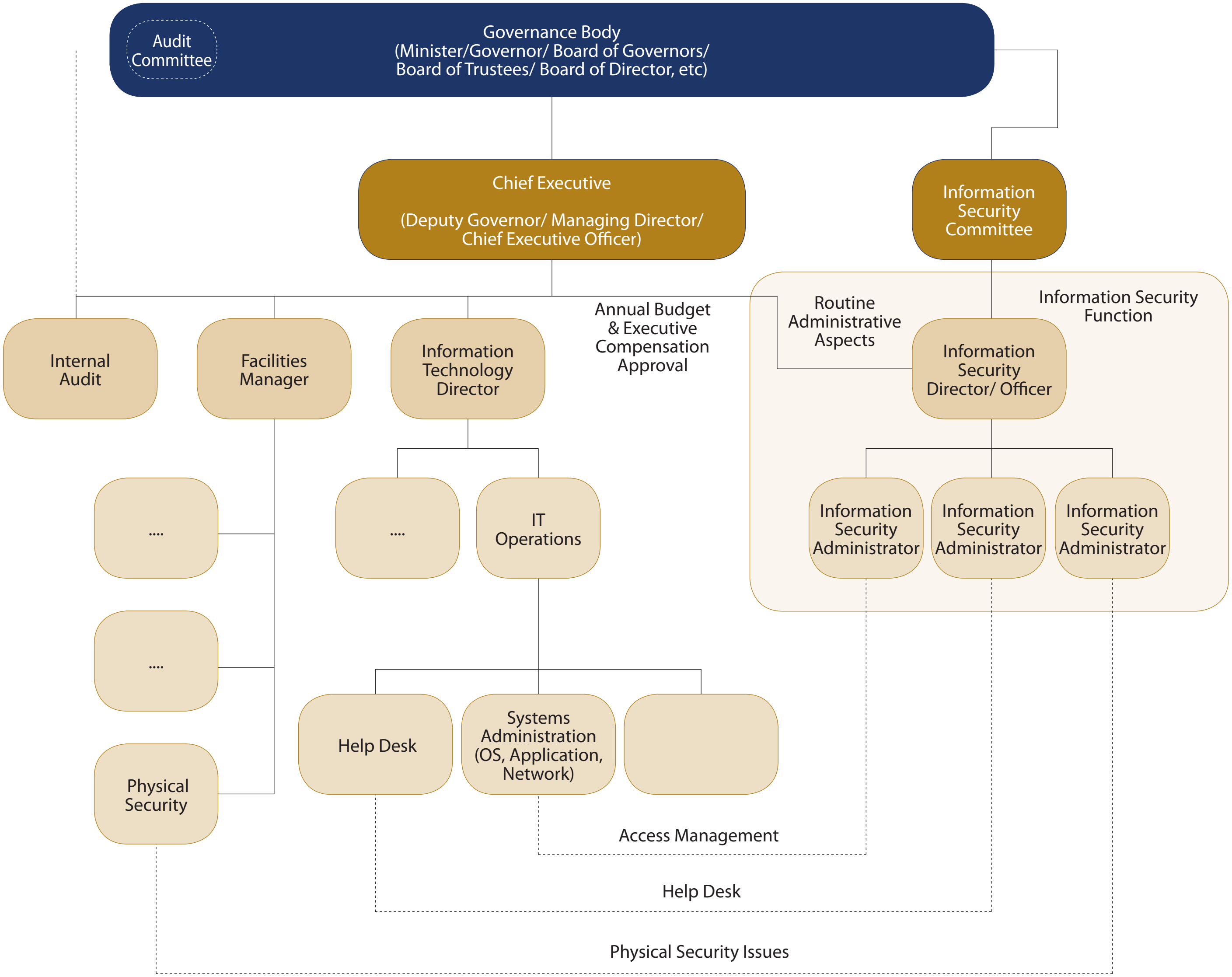
Advantages	Disadvantages
Reduced overall costs	Loss of independence
Less resistance to change	Inaccurate/Incomplete management reporting
	No segregation of duties
	Extra work load
	Less work efficiency
	Lack of expertise

The advantages describe option 1 to be cost effective solution as the roles can be shared between the Information Technology and Information Security function, also there is less resistance to change as the high level organization structure of the Agency does not change. However the disadvantages describe the information security function to have a loss of independence as it over shadowed by the Information Technology Department, the management reporting is inaccurate and incomplete as the routine administrative reporting is first made to the Information Technology Head and there after the Information Technology Head informs the Chief Executive. Information Technology Head can filter reporting that is in his interest, also he will not have decision making power for organizational changes that are required for successful enforcement of Information Security policies and procedures.

3. 1. 2. Conclusion:

Based on the advantages and disadvantages stated above Option 1 is suitable for smaller Agencies with a normal risk profile.

3. 2. Option 2



Audit Committee
Governance Body
(Minister/Governor/ Board of Governors/ Board of Trustees/ Board of Director, etc)
Chief Executive
(Deputy Governor/ Managing Director/ Chief Executive Officer)
Information Security Committee
Internal Audit
Facilities Manager
Information Technology Director
Annual Budget & Executive Compensation Approval
Routine Administrative Aspects
Information Security Function
Information Security Director/ Officer
....
....
IT Operations
Information Security Administrator
Information Security Administrator
Information Security Administrator
....
Help Desk
Systems Administration (OS, Application, Network)
Physical Security
Access Management
Help Desk
Physical Security Issues

The second option is designed and structured for a medium size Agency with a medium risk profile, clear segregation of duties must be defined while taking into consideration the constraints of size and budget of an Agency.

In this option the Information Security Head has a reporting line established with the Information Security Committee, where as administrative aspects of Information Security can be managed under the supervision of Chief Executive. The Chief Executive will be responsible for approving the annual budget and executive compensation. The colored dotted lines represent consultation requirements between various departments and Information Security function.

The roles illustrated in Option 2 are explained further in section 4.1.1, there are certain key advantages and disadvantages for above stated option:

3. 2. 1. Advantages Vs. Disadvantages

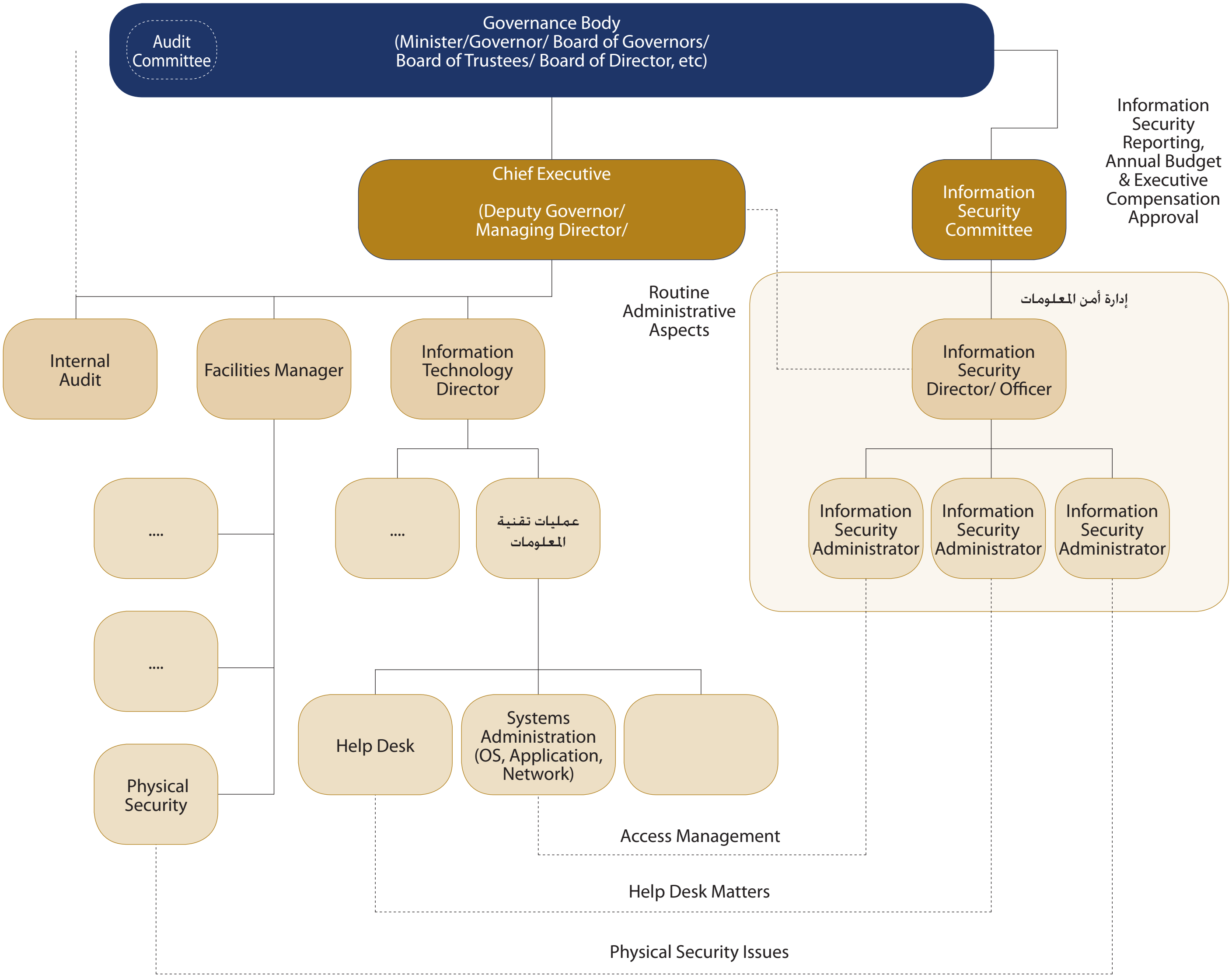
Advantages	Disadvantages
Efficient workload	Increase in cost
Segregation of duties	Inaccurate/Incomplete management reporting
Dedicated resources	Resistance to change
Management reporting	

The advantages describe option 2 to have the Information Security focused on the duties and responsibilities of Information Security, as there is clear segregation of duties and dedicated resources to perform the various task and functions of Information Security. The Management reporting is complete to the level of Chief Executive, here the Information Security Director will report directly to the Chief Executive. The Chief Executive has the decision making power to bring in effect organizational changes that are needed to enforce Information Security Policies and Procedures. The disadvantages of Option 2 include that of increase in cost due to the increase in staffing and facilities requirement. Although management reporting is complete to the level of Chief Executive, there can be instances where Chief Executive can filter report that is in his interest. This can give an inaccurate/incomplete picture to the Governance Body.

3. 2. 2. Conclusion:

According to the advantages and disadvantages stated above, Option 2 is suitable for medium size Agencies that have a medium risk profile.

3. 3. Option 3


Governance Body
(Minister/Governor/ Board of Governors/
Board of Trustees/ Board of Director, etc)
Audit Committee
Chief Executive
(Deputy Governor/
Managing Director/
Information Security Committee
Information Security Reporting, Annual Budget & Executive Compensation Approval
Routine Administrative Aspects
إدارة أمن المعلومات
Internal Audit
Facilities Manager
Information Technology Director
Information Security Director/ Officer
....
....
عمليات تقنية المعلومات
Information Security Administrator
Information Security Administrator
Information Security Administrator
....
Help Desk
Systems Administration (OS, Application, Network)
Physical Security
Access Management
Help Desk Matters
Physical Security Issues

The third option is designed and structured for a large size Agency with high and very high risk profiles; here top priority needs to be considered when choosing placement of an Information Security function, in which it must be placed in a manner where none of the Information Security key roles are compromised.

In this option the Information Security function routine administration is managed by the Chief Executive, however the Information Security Head reports directly to the Information Security Committee. The annual budget and executive compensation is approved by the Information Security Committee. The colored dotted lines represent consultation requirements between various departments and Information Security function.

The Information Security function works independent of the Chief Executive with set goals and objectives on Information Security, however the Information Security function is required to interact and collaborate on matters of Information Security with other concerned department before implementing new policies, standards and procedures.

The roles illustrated in Option 3 are explained further in section 4.1.1, the key advantages and disadvantages for above stated option are as follows:

3. 3. 1. Advantages vs. Disadvantages:

Advantages	Disadvantages
Efficient workload	Increase in cost
Segregation of duties	
Dedicated resources	
Complete management reporting	
Clear independence	

The advantages describe option 3 to have the Information Security focused on the duties and responsibilities of Information Security, as there is clear segregation of duties and dedicated resources to perform the various task and functions of Information Security. The Management reporting is complete to the Governance Body, here the Information Security Director will report directly to the Governance Body. The disadvantages of Option 2 include that of increase in cost due to the increase in staffing and facilities requirement.

3. 3. 2. Conclusion:

According to the advantages and disadvantages stated above, Option 3 is suitable for large size Agencies that have a high risk profile.

3. 4. Department placement based on Risk Profile

There are certain Agencies where the options stated above would not be applicable, for example large size Agency with normal risk profile, or a medium size Agency with a high risk profile. The below mentioned table details various combinations that can be applicable to different Agencies, the advantages and disadvantages stated above still apply for each option selection within the matrix.

	High Risk	Medium Risk	Normal Risk
Large Size Agencies	Option 3	Option 2	Option1
Medium Size Agencies	Option 2	Option 2	Option 1
Small Size Agencies	Option 2	Option 2	Option 1

4. Placement Option Approval

Budget constraints must also be considered when choosing an option, this entails getting approval from Top Management for the formation and creation of an Information Security Department. After choosing an Option, a formal proposal must be submitted to Top Management with an overall budget of establishing an Information Security Function.

Top Management must formally approve the proposal for Information Security Department Placement Option before initiating the Information Security Department Placement Process.

5. Information Security Department Placement Process

5. 1. Placement Initiation

This section discusses the Placement Initiation phase, as mandated by TOP Management <Organization Agency Name> will be required to have an Information Security function.

A GAP analysis needs to be conducted before establishing an Information Security function, the GAP analysis outcome will identify missing areas of an Information Security function (provided an Information Security function exists), here after it will be the responsibility of Top Management to create an Information Security function as stated in this guide.

Security is the responsibility of everyone within the company. All end users are responsible for understanding policies and procedures applicable to their particular job function and adhering to the security control expectations. Users must have knowledge of their responsibilities and be trained to a level that is adequate to reduce the risk of loss

Although exact titles and scope of responsibility of individuals may vary by Agency, the following roles support the implementation of security controls. An individual may be performing multiple roles when the processes are defined for an Agency, depending upon existing constraints and Agency structure. It is important to provide clear assignments and accountability to designated employees for various security functions to ensure that the tasks are being performed. Communication of the responsibilities for each function, through distribution of policies, job descriptions, training, and management direction provides the foundation for execution of security controls by the workforce.

5. 1. 1. Roles & Responsibilities

5. 1. 1. 1. Top Management

Top management has overall responsibility for protection of information assets. Agency operations are dependent upon information being available, accurate, and protected from individuals without a need to know. Financial losses can occur if the confidentiality, integrity, or availability of information is compromised. Members of the management team must be aware of the risks that they are accepting for an Agency, either through explicit decision making or the risks they are accepting by failing to make decisions or to understand the nature of the risks inherent in the existing operation of the information systems.

5. 1. 1. 2. Security Officer

The security officer directs, coordinates, plans and organizes information security activities throughout the Agency. The security officer works with many different individuals, such as executive management, business unit management, technical staff, and third parties such as auditors and external consultants. The security officer and his team are responsible for the design, implementation, management and review of the Agency security policies, standards, procedures, baselines, and guidelines.

5. 1. 1. 3. Information Systems Auditor

The information systems auditor determines whether systems are in compliance with adopted security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements. Auditors provide independent assurance to management on the appropriateness of the security objectives. The auditor examines information systems and determines whether they are designed, configured, implemented, operated, and managed in a way that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls that have been adopted and their effectiveness. Samples are extracted to test the existence and effectiveness of information security controls.

5. 1. 1. 4. Security Administrator

Security administrators manage user access request processes and ensure that privileges are provided to those individuals who have been authorized for access by management. These individuals have elevated privileges; they and create and delete accounts and access permissions. Security administrators also terminate access privileges when individuals leave their jobs or transfer among company divisions. Security administrators maintain records of approvals as part of the control environment and provide these records to information systems auditors to demonstrate compliance with policies.

5. 1. 1. 5. Physical Security

The individual(s) assigned to the physical security role establishes relationships with external law enforcement, such as the local police agencies, state police to assist in incident investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of CCTV surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, legal, and business areas to ensure that all practices are integrated.

5. 1. 1. 6. Help Desk Administrator

As the name implies, the help desk is there to handle questions from users that report system problems through a ticketing system. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk administrator contacts the computer emergency response team (CERT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control. These functions may alternatively be performed through self-service by the end-users, or by another area such as the security administration, systems administrators, etc., depending upon the organizational structure and separation of duties principles in use at the Agency.

5. 2. Placement Planning

Proper staffing is a success factor to the Information Security function. After defining the roles and responsibilities of the proposed placement options, the <Organization Agency Name> should consider the following:

- Develop a skills set matrix (refer to sample below) with the required skills needed.

Skills Set Matrix

Certifications									
Candidate	CISM	CISSP	CISA	CCSP	CPP	CEH	GIAC	ISO 27001	Other IS Qualifications/ Training
Name									
Name									
Name									
Name									
Name									
Name									

- Communicate the skill set needed and the timelines of when it’s needed with HR
- Initiate the recruitment process
    - Collect CVs
    - Short list and identify the prospective employees with the required characteristics
    - Arrange interviews with the selected candidates

5. 3. Placement Execution

In the Placement Execution phase, <Organization Agency Name> should start the decision making process pertaining the qualified candidates to fill the various positions based on the placement options mentioned earlier in this document.

- Candidates should be hired according to the <Organization Agency Name> hiring process.
- Upon the candidates' arrival to <Organization Agency Name>, an induction/orientation should be conducted to ensure a smooth start.

5. 4. Placement Monitoring & Controlling

To ensure the continuous success of the Information Security function, <Organization Agency Name> should consider the following:

- Undergo annual evaluations of employees
- Develop and maintain Job Descriptions
- Develop and maintain career development plans
- Conduct an annual skill set Gap Assessment
    - Develop a regularly updated training curriculum for each target group of employees taking the following into consideration:
    - Current and future business needs and strategy
    - Corporate values (ethical values, control and security culture, etc.)
    - Implementation of new IT infrastructure and software (i.e., packages, applications)
    - Current and future skills, competence profiles, and certification and/or credentialing needs as well as required re-accreditation
    - Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing

Chapter 7
Information Security Audit Manual

1. Introduction

This document presents information security Audit process for the <Organization Agency Name>. The audit process includes key activities for information security audit planning, execution and reporting.

2. Overview

Information security audit is performed to get an independent view about the status of informant security controls in an organization. The function is preferably performed by

1. An independent information security audit function reporting to Internal Audit Department of the organization.
2. Information Security Audit Function reporting to centralized information security governance function/committee in large Government organizations.

Information Security Audit function at Government Organization shall be responsible for the following key processes.

1. Information Security Audit Planning: This includes activities to perform risk based planning of types of information Security Audits to be conducted for the organization
2. Information Security Audit Execution: As part of this activity the specific planned information security audits are performed based on defined information security audit plan.
3. Information Security Audit Reporting. As part of this activity the results of information security audits are compiled and reported to relevant stakeholders

3. Information Security Audit Processes

This section further illustrates specific procedures for the identified information security audit processes. The information security audit planning procedure is presented in the beginning. Subsequently, procedures for information security audit execution and information security audit reporting are presented together due to their interdependencies during implementation of these processes.

3. 1. Information Security Audit Planning

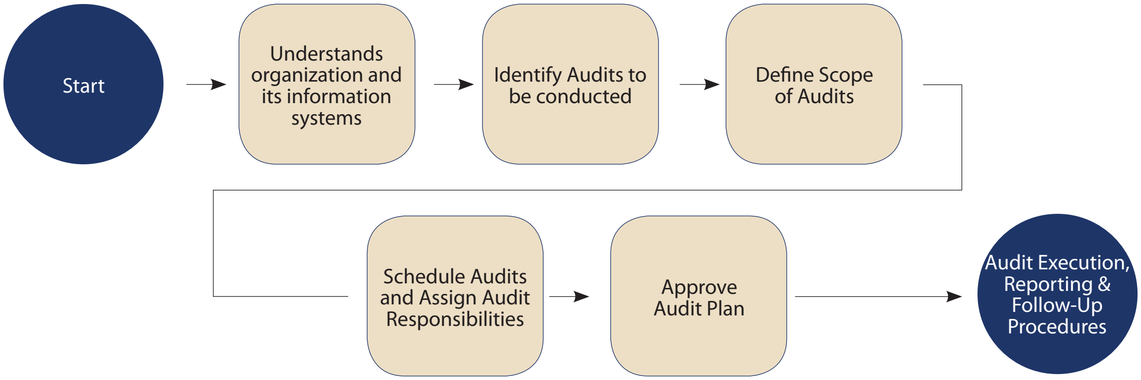
3. 1. 1. Objective

This procedure illustrates key activities to perform risk based planning of information Security Audit for the <Organization Agency Name>.

3. 1. 2. Policy Reference

Information Security Auditing Policy

3. 1. 3. Procedure


Start
Understands organization and its information systems
Identify Audits to be conducted
Define Scope of Audits
Schedule Audits and Assign Audit Responsibilities
Approve Audit Plan
Audit Execution, Reporting & Follow-Up Procedures

3. 1. 3. 1. Understand Organization and its information systems

1. The <Internal Audit Department Head> in coordination with the <Information Security Audit Manager> initiates information security audit planning process as part of annual Internal Audit Planning of the organization. The main responsibility for information security audit is assigned to the <Information Security Audit Manager>.
2. The <Information Security Audit Manager>

- Develops/updates his understanding of the various business and technical functions (especially IT and Information Security Functions) in the organization.
- The <Information Security Audit Manager> reviews the classified list of the organization's information system that was developed as part of information system identification and information system classification procedures.
- The <Information Security Audit Manager> assign security classification rating to the identified business and technology functions considering the security classification of the information system being used or managed by that business or technology function, input from <internal Audit Department Head> and other relevant factors.

3. 1. 3. 2. Identify Audits to be conducted

1. The <information Security Audit Manager> uses the security audit planning requirements form to list down the business functions and the information systems for which audit is to be conducted.
2. The <Information Security Audit Manager> identifies the frequency of audit for business/ Technology functions and Information Systems as follows.

- High Risk functions/information systems to be audited thoroughly every year
- Medium Risk functions/information systems to be audited thoroughly every two years, and on limited sample bases every year.
- Normal Risk functions/information systems to be audited on sample basis every year.

3. 1. 3. 3. Define Scope of Audits

1. The <Information Security Audit Manager> defines the scope of each audit.

- Scope of Business/Technology function audit is determined by identifying key areas of common information security policies and procedures that are relevant to the identified business/technology functions.
- Scope of Information Systems Audit is determined by reviewing relevant system specific security policy for the information systems. Where system specific policy is not available, the scope is determined by identifying review areas applicable to a similar system from the organization's system specific standard repository and international best practices.

2. The <Information Security Audit Manager> defines the type of audit to be conducted to address the scope of audit e.g.

- Information Security Process Audit.
- Technical Attack & Penetration,
- Vulnerability Assessment,
- Information Assets
- Security Configuration Review
- etc.

3. 1. 3. 4. Schedule Audit and Assign Audit Responsibilities

1. The <Information Security Audit Manager> defines specific schedule of each audit as follows.

- Identifies the estimated time to be taken by each audit.
- Identifies start and end date for each audit considering, identified audit frequency, audit durations, availability of auditee and other relevant factors.

2. The <Information Security Audit Manager> with input from the <Internal Audit Department Head> decides whether to conduct the security audit internally by his department resources', by external vendor, or by using an approach where his department resources work together with external audit resources to conduct information security audits.
3. Where applicable the <Information Security Audit Manager> with input from the <Internal Audit Department Head> determines internal audit department person responsible for conducting the audit.

3. 1. 3. 5. Approve Audit Plan

1. The <Information Security Audit Manager> sends the internal audit plan to < Internal audit Department Head> for review and approval
2. The <Internal Audit Department Head> review and approves the plan and send it to the organization's <Audit Committee> for review and approval.
3. Upon receiving the <Audit Committee> approval, the <Internal Audit Department Head>

- Communicates the security audit plan to relevant personnel within <Organization Agency Name>.
- Arranges required internal and vendor resources for the audit as per the organization's relevant processes.

3. 1. 4. Related Form

Security Audit Plan

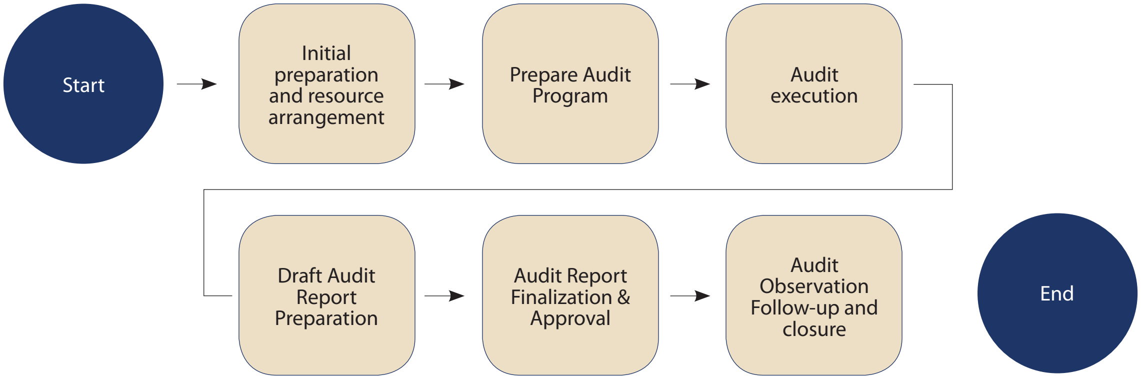
3. 2. Information Security Audit Execution, Reporting & Follow-up

3. 2. 1. Objective

This procedure illustrates key activities to execute the developed information security audit plan for the organization and report identified audit findings, risks, and recommendations to related stakeholders.

3. 2. 2. Policy Reference

Information Security Auditing Policy


Start

Initial preparation and resource arrangement

Prepare Audit Program

Audit execution

Draft Audit Report Preparation

Audit Report Finalization & Approval

Audit Observation Follow-up and closure

End

3. 2. 3. Procedure

3. 2. 3. 1. Initial Preparation and resources arrangement

1. The < information Security Audit Manager> arranges the human resources required to conduct scheduled audit.

- If the initiative is delivered internally, the <Internal Security Audit Manager> in coordination with the <Information Security Department Head> determines the internal resources that shall conduct the audit and informs them about their assigned audits.
- If the initiative is to be delivered externally, the <Internal Audit Department Head> ensures that the appropriate third party information security vendor is selected, and contract is signed with them to execute the audits as planned.

2. The <Internal Audit department head> informs relevant persons of the planned audit date and requests their cooperation. This information shall be communicated to

- The Head of the business function/technology function being audited.
- The owner of the information system being audited.
- Other relevant persons.

3. 2. 3. 2. Prepare Audit Program

1. Before the commencement of each audit a detailed audit program is developed for each audit using the audit program development form. The audit program shall document specific controls to be assessed as part of the audit.
2. Key considerations for developing the information security audit programs are:

- Refer to the relevant information system (or group of information systems) security policy.
- If the information system (or group of information systems) security policy and standard does not have a policy, refer to the relevant system specific security standard.
- For business/ technology functions audit identify the common polices and procedures applicable to that function that need to be audited.
- Refer to relevant best practices and guidelines.

3. The assigned audit team determines and documents appropriate audit techniques to validate the effectiveness of the controls specified in the audit program

3. 2. 3. 3. Audit Execution

1. The Information Security Audit Team conducts Information Security Assessment as per the developed Information Security Assessment program and defined Information Security Assessment techniques.
2. For procedural controls assessment

- Information security audit Team verbally discusses with the persons responsible for that information system the status of each control identified in the Information Security Assessment program.
- Based on the response received if it is determined that the control is not effective, the Information security audit team notes down the observations.
- If the audit team is informed that the controls are effective, the Information Security Audit Team requests supporting evidence to support that claim, or performs adequate Information Security Assessment technique to verify the correctness the claim. The information security audit team notes down any control weakness identified as part of the process.

3. Based on the information security audit scope, the information security audit team may use appropriate tools and techniques to perform information security audits e.g. configuration review, vulnerability assessment, Attack & Penetration Testing etc. In such cases

- Permission is taken from the relevant persons to run the security assessment tool.
- Appropriate security assessment methodologies are used to perform security assessment tests.
- Identified observation are noted and reviewed to remove any false observations from.

4. The information security audit team ensures to keep evidence of each observation identified in the information security assessment process.

3. 2. 3. 4. Draft Audit Report Preparation

1. The audit observations are properly documented in a draft audit report.
2. For each of the audit observations the following aspects are documented.

- Audit Finding: Describing the identified control weakness as audit observations.
- Risk: Describing the risk to the organization from the audit finding and its significance (High, Medium, and Low).
- Recommended Mitigation Actions: Describing the suggested action to be undertaken by the organization/information owner to address identified control weakness.

3. The draft audit report(s) is communicated to the auditee to obtain the confirmation of the audit findings, risk and recommendations.

3. 2. 3. 5. Audit Report Finalization & Approval

1. The auditor discusses the draft audit report with the auditee and provides adequate explanation of the identified audit observation, risks and recommendation. The auditee may agree or disagree with the auditor. In case of disagreement, the auditee is required to provide adequate supporting evidence of control effectiveness.
2. The auditee provides documented feedback to the auditor about their plan to address the identified observation, target date for resolving the identified observation and assigned responsible person for taking those actions.
3. Upon agreeing the observations and required correction actions with auditee, the audit report(s) is finalized and communicated to the < Internal Audit Department Head> for review and approval of the report.
4. After that the report is communicated to the <Audit Committee> for review and approval.

3. 2. 3. 6. Audit Observations Follow Up & Closure

1. Each Information system owner/relevant department head is responsible for addressing the identified information security audit observation related to his function/system in timely and effective manner.
2. Every month (or earlier as required) the relevant Information system owner/relevant department head informs < Internal Audit Department Head> about the status of his actions to address the related observation identified in the audit.
3. Based on the input received from auditee, the internal audit department prepares a monthly report about the status of Implementation of the audit recommendations and sends it to the <Audit Committee>.
4. The <Audit Committee> reviews the report received and takes necessary actions to ensure satisfactory resolution of all information security audit observations.

3. 2. 4. Related Form

1. Audit Program Development
2. Audit Reporting

4. Supporting Forms

4. 1. Information Security Audit Plan Template

Audit Plan Template for Business/Technology Functions Audit

#	Business/ Technology Function to be audited	Risk Rating (H/M/L)	Information Security Audit To be conducted	Summarized Scope of Audit	Frequency / Schedule	Person Responsible for Managing Audit	Skills Required	Comments
1								
2								
3								
N								

Audit Plan Template for Information System Audit.

#	Information System / Group of Information Systems to be audited	Risk Rating (H/M/L)	Information Security Audit To be conducted	Summarized Scope of Audit	Frequency / Schedule	Person Responsible for Managing Audit	Skills Required	Comments
1								
2								
3								
N								

4. 2. Information Security Audit Program Template

The template shall be filled for each information system or Group of information system to be audited

Information System/ Function Name: <Document Information System/ Function to be audited.>

Information System/ Function Name: <Document Information System/ Function reference number (where applicable).>

Control #	Control	Assessment Steps/ Audit Technique	Required Documentation/ Evidence	Findings	Received Evidence Reference Number	Auditee Details
<Audit Area>						
<Audit Sub Area>						

4. 3. Information Security Audit Report Template

Section 1: Executive Summary:

<Document overall Summary of key audit observations, risks and recommendations with focus on high risk observations >

Section 2: Audit Scope

< Document overall scope of Audit>

Section 3: Audit Approach

< Document overall approach of Audit>

Section 4: Audit Findings, Risks and Recommendations

< Document the specific findings captured as part of the audit, related risk and recommendations. This section is also used to capture auditees plan to address the identified observations>.

Ref #	Key findings and recommendations
1	<Audit Area> Finding 1: Risk Impact: Risk Rating (High/ Medium/ Low) Recommendation(s): Management Response: Agreed □ Not Agreed □ Management Action Plan: <Action Plan to address identified observations> Implementation Date: <Date> Responsibility: <Name, Title>

Chapter 8
Appendices

1. Appendix I : Guide on using Repository of Information Security Policies and Procedures

1. 1. Introduction

This section describes the overall structure of the simple MS-Access based tool that has been developed to represent repositories of information security policies and system specific security standards. This section aims at identifying the purpose and a high level structure of the sample repositories that Government Agencies will use in generating their information security policies and procedures.

1. 2. Purpose

The purpose of these sample repositories is to represent fair collection of information security policies and procedures for Government Agencies. These sample repositories will be used by Government Agencies during the Information Security Policies and procedures Development Process.

1. 3. Sample Repositories Structure

The Framework sample repositories contain the following three different sheets:

- The first one is a simple MS-Access based tool that contains a sample of Common Information Security Policies
- The second one is a document that contains the Information Security Procedures
- The third one is a simple MS-Access based tool that contains a sample of System Specific Security policy

1. 3. 1. Sample Common Information Security Policies Simple MS-Access Based Tool

The common information security policy simple MS-Access based tool contains the following elements:

- **Purpose:** Briefly illustrates the purpose of the Policy.
- **Policy Applicability:** Defines various internal and external entities as well as the people to which a particular Policy statement applies.
- **Executive Owner:** Identifies the person who has the ultimate authority and responsibility for any changes and updates in the policy. Any changes or updates in the policy have to be approved by the executive owner.
- **Custodian:** The person who is responsible for maintaining, communicating, and updating the policy based on directions from Executive Owner.
- **Enforcement:** Defines the consequences of any violation of this policy.
- **Information Security Policy Statements:** This element describes the control statements part of the specific policy.
- **Related Procedures:** This element identifies the relevant procedures for a given policy, if applicable.
- **Policy Effective Date**: This element defines the date from which the policy is applicable and is to be followed.

1. 3. 2. Sample Procedures Document

The procedures document contains the following elements:

- **Policy Reference:** This element identifies the relevant policy for a given procedure.
- **Objective:** This element clearly states the objective of the procedure.
- **Information Security Procedure Activities:** This element lists down and describes the procedure activities.
- **Applicable Form:** The element specifies the name of related form for a given procedure if any exists.

1. 3. 3. Sample System Specific Security Policies Simple MS-Access Based Tool

The system specific security standards simple MS-Access based tool contains the following elements:

- **Policy Area:** This element defines the main category of security controls in the policy.
- **Policy Sub Area:** This element defines the sub category of security controls in the policy.
- **Effective date:** This element defines represents the date from which compliance with standard becomes mandatory

1. 4. Developing the Information Security Policies and procedures

1. 4. 1. Developing Common Information Security Policies

The following are the key steps a Government Agency's project team members will follow in using the common information security policies development simple MS-Access based tool to generate its common information security policies:

1. Option 1: Generate all Common Information Security Policies in a Single Document

- Replace all the <Organization Agency Name> fields in the Common Information Security Simple MS-Access Based Tool by the Government Agency name so that the generated common information security policies are customized to show the organization name.
- Replace all the sample variables for <Custodian and Executive Owner> in the Common Information Security Simple MS-Access Based Tool with information related to the Government Agency Organization Structure.
- Define each policy effective date using the empty fields in the Common Information Security Simple MS Access Based Tool.
  - Utilize the provided common information security policies template in Appendix II Sub Section 2.2.1 to populate the entire content of the simple MS-Access based tool.

2. Option 2: Generate a Separate Document for each Common Information Security Policy

- Select the policy area from the Common Information Security Simple MS Access Based Tool and accordingly the relevant controls to this policy area are generated.
- Replace all the <Organization Agency Name>

fields for the selected policy area in the Common Information Security Simple MS-Access Based Tool by the Government Agency name so that the generated common information security policy area is customized to show the organization name.

- Replace all the sample variables for <Custodian and Executive Owner> for the selected policy area in the Common Information Security Simple MS Access Based Tool with information related to the Government Agency Organization Structure.
- Define the effective date for the selected policy area using the empty fields in the Common Information Security Simple MS-Access Based Tool.
- Utilize the provided single common information security policies template in Appendix II Sub Section 2.2.2 to populate the generated controls and additional fields.
- Repeat the above steps for each policy area that a Government Agency wants to generate.

3. Option 3: Generate Common Information Security Policy Based on Audience

- Select the audience type/category from the Common Information Security Simple MS Access Based Tool and accordingly the relevant controls to this audience are generated.
- Replace all the <Organization Agency Name> fields in the Common Information Security Simple MS-Access Based Tool by the Government Agency name so that the generated common information security policies of the selected audience type/category are customized to show the organization name.
- Replace all the sample variables for <Custodian and Executive Owner> in the Common Information Security Simple MS-Access Based Tool with information related to the Government Agency Organization Structure.
- Define the effective date for the selected audience type/category generated policies using the empty fields in the Common Information Security Simple MS-Access Based Tool.
- Utilize the provided common information security policies template in Appendix II Section 2.2.3 to populate the generated controls and additional fields.
- Repeat the above steps for each audience type/category.

1.4. 2. Developing Information Security Procedures

The following are the key steps a Government Agency's project team members will follow in using the procedures document to generate and or customize its information security procedures:

1. Utilize the sample procedures document to customize the Government Agency procedures or utilizes the information security procedures template in Appendix II Section 2.3 to generate and customize relevant Government Agency procedures from the provided procedures document.
2. Replace all the <Organization Agency Name> fields by the Government Agency name so that the generated procedures document is customized to show the organization name.
3. Replace all the sample variables for <IT/Information Security/Other Departments Position> with the information related to the Government Agency organization structure.

1.4. 3. Developing System Specific Information Security Policies

The following are the key steps a Government Agency's project team will follow in using the systems specific security standards development simple MS-Access based tool to generate its systems specific security standards:

1. Select the information system component (e.g. Database Application, Systems Servers, Router, Server Rooms, etc) under the information technology infrastructure type (i.e. Application, IT System, Networking and Physical Infrastructure) in the repository and according the relevant controls are generated.
2. Select the CIA level (High, Medium, Normal) of the selected information system component to generate the corresponding controls of the selected CIA level.
3. Replace all the <Information System> fields in the System Specific Security Standards Simple MS-Access Based Tool by the relevant information system component name so that the generated system specific standard statements of this component are customized to show its name.
4. Replace all the <Organization Agency Name> fields in the System Specific Security Standards Simple MS-Access Based Tool by the Government Agency name so that the generated systems specific security standard statements of this component are customized to show the organization name.
5. Define the standard effective date using the empty fields in the System Specific Security Standards Simple MS-Access Based Tool.
6. Utilize the provided systems specific security standards template in Appendix II Section 2.4 to populate the generated controls and additional fields.
7. Repeat the above steps for each information system component that the Government Agency wants to generate the related system specific security standard.

1. 5. Updating the Information Security Policies and procedures

With respect to updating the information security policies and procedures of the Government Agencies, it is desirable to hold hearing from concerned departments and understand the current situation. Furthermore, when updating the Government Agency's information security policies and procedures, it is important to make the necessary updates to the current state of the IT environment to enable the Agency to sustain the Government mandated policies and procedures.

Any acquired/developed information system within the Government Agency shall follow the Information Systems Acquisition and Development Policy and Procedure and accordingly the content/structure of the sample repositories shall be updated.

In case of the Systems Specific Security Standards, it is important to make daily efforts to collect information on new attacks and use it to update the Government Agency's system specific security standards.

When the information security policies and procedures have been revised based on results of inspection and evaluations on information security in a Government Agency, the Government Agency shall update the content of its sample repositories accordingly.

2. Appendix II: Documentation Control

The purpose of the documentation management process is to control the quality of policies and procedures documents and to maintain policies procedure documents update to meet the Agencies requirements.

2. 1. Procedure Responsibilities

- The <Document Owner> is responsible for:
  - Identifying the document custodian, author and the quality assurance executive;
  - Assist the document custodian where needed;
  - Classify the document; and
  - Approve the document.
- The <Document Custodian> is responsible for:
  - Reviewing the documents and Identifying the documents that need to be developed or updated;
  - Releasing copies of the document for modification;
  - Determining corrective action if the document is not approved;
  - Publishing the document; and
  - Updating the document record.
- The <Document Author> is responsible for:
  - Selecting the appropriate template for the document; and
  - Creating and updating documents.
- The <Quality Assurance Executive> is responsible for:
  - Reviewing and endorsing the created and updated document.
- The <Document Registrar> is responsible for:
  - Updating the document register
- The <Document Librarian> is responsible for:
  - Ensuring that the documents are stored in the correct section of the library; and

2. 2. Procedure Activities

Plan creating new document or updating existing document

- For a new document creation, the <Document Owner> must nominate the personnel who will hold the responsibilities of the Document Custodian, Document Author and the Quality Assurance Executive.
- The <Document Custodian> -in coordination with the <Document Owner> , if needed- must identify the scope of change in existing document, or the main content to be covered in the new document.
- The <Document Custodian> -in coordination with the <Document Owner>, if needed- must review the 'Document Register' to determine whether an existing document already has all or part of the required content. Where other documents partially cover the topic, consultation with other custodians -and owners, if needed- must be performed to determine the referencing required between the documents.
- The <Document Custodian> must fill the required details of the existing document -if applicable- and the new/updated document in the 'Document Initiation/Change Request Form':
- The <Document Custodian> -or the <Document Registrar>- must update the following details for the new/updated document in the 'Document Register'
- IT document reference - in accordance with referencing rules in ISMS the Documentation Management methodology;
- Document title;
- Version no. - in accordance with versioning rules in ISMS the Documentation Management methodology;
- Document owner;
- Document custodian;
- Document author;
- Quality assurance executive; and
- Document status, where it should be set to "Work In Progress".

2. 2. 1. Release a document copy

- If there is an existing document, the <Document Custodian> -or the <Document Registrar>- must update the existing document status to be "Review in Progress".
- If the case is a document update, the <Document Custodian> -or the <Document Librarian>- must create a copy of the document that is renamed to reflect the next version number. The copy of the document must be released to the <Document Author>.
- If the document is to be created, refer to 'Select the appropriate template' procedure instruction.

2. 2. 2. Select the appropriate template

- The <Document Author> should refer to the corporate rules for standard document formatting.
- The <Document Author> should select the required template.
- If a template does not exist, the <Document Author> should request the <Document Custodian> -or the <Document Librarian>- to assist in finding a similar document.
- The <Document Author> must submit the created/ updated document to the <Quality Assurance Executive> mentioned in the form.

2. 2. 3. Create/ Update the document

- The <Document Author> must receive the 'Document Initiation/Change Request Form' in order to know the requirements for the document creation or update.

  - If the document is to be updated, the <Document Author> must receive the copy document and start applying the required updates.
  - If a new document is to be created, the <Document Author> should agree the main sections with the <Document Custodian> and accordingly compose the document in line with the requirements in the request form.
- The <Document Author> must submit the created/updated document to the <Quality Assurance Executive> mentioned in the form.

2. 2. 4. Review the document

- The <Quality Assurance Executive> must review the document to ensure that The Group quality requirements are addressed and whether the documentation creation/update is as per the request.
  - If the review has resulted in specific feedback, it must be incorporated by the <Document Author> and resubmitted to the <Quality Assurance Executive> for review.
  - If the review is passed successfully, the <Quality Assurance Executive> must endorse the document by signing the request form.
- The <Document Custodian> -or the <Document Owner>, if needed- must be informed of the changes suggested by the <Quality Assurance Executive>.
- The <Document Custodian> -or the <Document Registrar>- must update the status of the new/updated document record to be "Pending Approval".
- The <Quality Assurance Executive> must submit the reviewed document and the request form to the <Document Owner>.

2. 2. 5. Classify the document

The <Document Owner> must initiate the 'Information Asset Classification' procedure to assign the appropriate classification level.

2. 2. 6. Approve the document

The <Document Owner> must perform a review of the content to sign off the request form.

- If the <Document Owner> has not approved the document and has specific feedback, refer to 'Determine corrective action' procedural instruction.
- If the review is passed successfully, the <Document Owner> must sign off the form and submit the document to the <Document Custodian>. The <Document Custodian> -or the <Document Registrar> must update the document status in the 'Document Register' to be "Approved".

2. 2. 7. Determine corrective action

The <Document Custodian> must assess the reason for not approving the document and determine the process that must be re-performed to take corrective actions. If the document needs to be updated, refer to 'Create/Update the document' procedural instruction.

2. 2. 8. Update the document information

The <Document Custodian> must determine -with the <Document Owner>, if needed- the next revision date for the document.

The <Document Custodian> must update the document information listed before the table of contents as per the requirement of the ISMS Documentation Management methodology.

2. 2. 9. Publish the document

The <Document Custodian> must publish an Adobe Acrobat Reader (PDF) format of the document to the intended audience listed in the distribution list. The publishing should be made in accordance with the ISMS Documentation Management and the Information Asset Management methodologies.

The <Document Custodian> -in coordination with <Document Librarian>- must ensure that the new modifiable version of the document is stored in the "Current" section of the 'Document Library', and that the appropriate access controls are applied to the document.

If there is an older version of the document, the <Document Custodian> must ensure that <Document Librarian> has moved the earlier version to the "Archive" section of the 'Document Library'.

2. 2. 10. Update the document record

The <Document Custodian> -or the <Document Registrar>, if must ensure that the records of the new/updated document is completed.

If there was an older version of the document, the <Document Custodian> -or the <Document Registrar>, must change the status of the document to be "Discontinued" to ensure that it is not referred to by mistake.

2. 2. 11. Review the document

The process is triggered based on periodic document review schedule, or through other processes.

- When the <Document Registrar> generates a quarterly list of documents from the 'Document Register' that are due review, the respective <Document Custodian> must be notified. Or each 'Document Custodian' must review their records on a monthly basis to determine the documents due review.
- When the process is triggered by changes that imply document update, the <Document Custodian> must be notified of the possible impact of changes on his/her document.
  - The <Document Custodian> -in coordination with the <Document Owner>, if needed must review the change impact on the document and determine if any changes are required in the document.
- If there are changes to be made, refer to 'Plan creating new document/ update existing document' procedural instruction.

If there are no changes required, the <Document Custodian> must update the next revision date for the document version if needed. The <Document Custodian> shall review the document again when the next revision date comes.

Term	Definition
Access Control	The process of granting or denying specific requests:
	1) for obtaining and using information and related information processing services; and
	2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access Control Lists - (ACLs)	A register of:
	1) users (including groups, machines, processes) who have been given permission to use a particular system resource, and
	2) the types of access they have been permitted.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Antivirus Software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
Asset	A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.
Asset Custodian	An individual designated by the data owner to be responsible for making judgments and decisions on behalf of the organization with regard to the asset information category designation, its use and protection, and its sharing
Asset Owner	The individual responsible for making judgments and decisions on behalf of the organization with regard to the asset sensitivity designation, its use and protection, and its sharing
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Term	Definition
Attack & Penetration	Security testing in which evaluators mimic real-world attacks to attempt to identify methods for circumventing the security features of an application, system, or network.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures
Audit Trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. The process of establishing confidence of authenticity. Encompasses identity verification, message origin authentication, and message content authentication. A process that establishes the origin of information or determines an entity's identity.
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authorization	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Availability	Ensuring timely and reliable access to and use of information.
Information Security Awareness	Activities which seek to focus an individual's attention on an (information security) issue or set of issues.
Backup	A copy of files and programs made to facilitate recovery if necessary.
Baseline Security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.
Block Cipher	A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.

Term	Definition
Brute Force Password Attack	A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.
Buffer Overflow	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.
Buffer Overflow Attack	A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory.
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates. The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy.
Change Management	Planning, testing, and implementing all aspects of the transition from one organizational structure or business process to another.
Chief Information Officer (CIO)	Agency official responsible for:
	1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency;
	2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Classified Information	Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
Client (Application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Term	Definition
Compensating Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Control	Controls are safeguards or measures implemented to minimize security risks.
Cookie	A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.
Correlation rules	In Security Monitoring and Reporting terms, rules written in such a manner that whenever separate unique events occur together they are reported for further investigation.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cryptographic Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
	1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and
	2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. A parameter used in conjunction with a cryptographic algorithm that determines. The transformation of plaintext data into cipher text data,. the transformation of cipher text data into plaintext data, a digital signature computed from data, . the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.

Term	Definition
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. It is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties . The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 1401-]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret.
Cryptology	The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.
Data Encryption Algorithm (DEA)	The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA).
Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
Decryption	The process of transforming cipher text into plaintext. The process of changing cipher text into plaintext using a cryptographic algorithm and key. Conversion of cipher text to plaintext through the use of a cryptographic algorithm.
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Detective Controls	Detective controls, detect undesired outcomes, after their occurrence. They are less effective than Preventive controls.
Digital Signature Algorithm	Asymmetric algorithms used for digitally signing data.
Disaster Recovery Plan (DRP)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Term	Definition
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack.
Domain	A set of subjects, their information objects, and a common security policy.
Event	Any observable occurrence in a network or system.
Evidence	Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. NOTE - Evidence does not necessarily prove truth or existence of something but contributes to establish proof.
Exploit	A technique or code that uses a vulnerability to provide system access to the attacker.
Firewall	A gateway that limits access between networks in accordance with local security policy.
Hacker	An individual with an affinity for computers. White-hat hackers are intrigued by the intellectual challenge of tearing apart computer systems to improve computer security. Black-hat hackers purposely crash systems, steal passwords, etc., not necessarily for financial gain.
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
	1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output.
	2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output. An approved mathematical function that maps a string of arbitrary length (up to a pre-determined maximum size) to a fixed length string. It may be used to produce a checksum, called a hash value or message digest, for a potentially long string or message.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.
Host-Based IDS	IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Term	Definition
Network-Based IDS	IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.
Image	An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Handling	The mitigation of violations of security policies and recommended practices.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s).
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
	1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
	2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
	3) availability, which means ensuring timely and reliable access to and use of information.
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Term	Definition
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which—
	1) requires the use of such equipment; or
	2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Ingress Filtering	The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.
Initiatives	For the purpose of this framework, action plans that have been identified as a means to fill the gaps and minimize the risks identified during the risk assessment phase.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention Systems	Systems which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Term	Definition
IP Address	An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
IP Security (IPsec)	An Institute of Electrical and Electronic Engineers (IEEE) standard, Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol.
IT-Related Risk	The net mission/business impact considering
	1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability, and
	2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to: Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. Non-malicious errors and omissions. IT disruptions due to natural or man-made disasters. Failure to exercise due care and diligence in the implementation and operation of the IT.
IT Security Awareness	The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.
Key Pair	Two mathematically related keys having the properties that
	(1) one key can be used to encrypt a message that can only be decrypted using the other key, and
	(2) even knowing one key, it is computationally infeasible to discover the other key. A public key and its corresponding private key; a key pair is used with a public key algorithm.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.

Term	Definition
Logical Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Memorandum of Understanding/Agreement (MOU/A)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. It is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Term	Definition
Policy	A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Port Scanning	Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.
Project	A project is a temporary endeavor undertaken to create a unique product, service or result. Projects have a definite start and end date.
Project Management	The application of knowledge, skills, tools and techniques to achieve the project objectives
Project Milestones	Milestones are significant events within the project schedule.
Proxy Server	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Repository	A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory.
Residual Risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat.

Term	Definition
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Secure Communication Protocol	A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection
Security Event Log	A log containing security events (like Logon/Log off success or failure, correlation events) that are associated with a date stamp
Security Patch	Software code that replaces or updates other code. Frequently patches are used to correct security flaws.
Security Policy	The statement of required protection of the information objects. Security Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
Sensitivity	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
Sensitivity Levels	A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.
Spoofing	"IP spoofing" refers to sending a network packet that appears to come from a source other than its actual source. Involves—

Term	Definition
	1) the ability to receive a message by masquerading as the legitimate receiving destination, or
	2) masquerading as the sending machine and sending a message to a destination.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
SQL Injection	A type of attack implemented by injection of malicious code into the SQL command. Injection occurs when user-supplied data is sent to an interpreter as part of a SQL command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
SSID	Service Set ID - A unique ID used to distinguish between different Wireless LANs.
SSL	An encryption system developed by Netscape. SSL protects the privacy of data exchanged by the website and the individual user. It is used by websites whose names begin with https instead of http.
Standard	A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.
Stateful Inspection	A firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. A single cryptographic key that is used with a secret (symmetric) key algorithm.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
System Administrator	A person who manages the technical aspects of a system.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Term	Definition
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Triple DES	An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES.
Trojan Horse	A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.
Two Factor Authentication	Authentication processing using two factors, typically: 'something you have' and 'something you know'.
User	Individual or (system) process authorized to access an information system. An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.
User Initialization	A stage in the lifecycle of keying material; the process whereby a user initializes its cryptographic application (e.g., installing and initializing software and hardware).
User Registration	A stage in the lifecycle of keying material; a process whereby an entity becomes a member of a security domain.
Valid Data Element	A payload, an associated data string, or a nonce that satisfies the restrictions of the formatting function.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification	The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system.
Virtual Private Network (VPN)	A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network.

Term	Definition
Virus	A self-replicating program that runs and spreads by modifying other programs or files
Virus Hoax	An urgent warning message about a nonexistent virus.
VLAN	Virtual Local area networks that allows hosts on different physical segments to communicate as if they were connected to a single network switch. VLANs help improve security, network manageability and reduces unwanted network traffic
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.
Wireless Application Protocol (WAP)	A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
X.509 Certificate	The International Organization for Standardization/International Telecommunication Union Standardization Department (ISO/ITU-T) X.509 standard defined two types of certificates the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate.
XSS (Cross Site Scripting)	XSS refers to a vulnerability that occurs whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Sources: Publicly available information in published material from:

- KSU
- PMBOK (PMI)
- ISO 27001
- US Govt. agencies, etc.

CERT.sa

المركز الوطني الارشادي لامن المعلومات

Computer Emergency Response Team

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

ص.ب٧٥٦٠٦ الرياض ١١٥٨٨ المملكة العربية السعودية
هاتف ٤٦١٨٠٠٠ ١ ٩٦٦+ فاكس ٤٦١٨١٩٠ ١ ٩٦٦+

Saudi Arabia ١١٥٨٨ Riyadh ٧٥٦٠٦ P.O. Box
٤٦١٨١٩٠ ١ ٩٦٦+ :Fax ٤٦١٨٠٠٠ ١ ٩٦٦+ :.Tel
www.citc.gov.sa
info@citc.gov.sa