Information Security Management Implementation Guide for Government Organizations

Version 1.1
August, 2007

STQC Directorate,
Department of Information Technology
Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi 110003

1.0 Introduction

Information Security Management for Government organizations provides a broad overview of information security program concepts to assist senior officers in understanding how to oversee and support the development and implementation of information security programs. Senior officers are responsible for:

- Establishing the organization's information security program;
- Setting program goals and priorities that support the mission of the organization; and
- Making resources are available to support the program.

Senior management commitment to security is more important now than ever before. Studies have shown that it is the single most critical element that impacts the success of an information security program. This requires focus on effective information security governance and support, which needs integration of security into the strategic and daily operations of an organization.

The *key Questions* for implementation of the information security management in government are:

- Why to implement information security management?
- What factors lead to success of Information Security Programme?
- What are the steps of developing effective information security program?
- What are the information security laws, regulations etc, required to develop an effective information security program?
- Which organizations can provide help in implementing and evaluating the effectiveness of information security program?

This guide provides the answers to above questions.

2.0 Why to implement information security management?

Government departments now rely extensively on computerized information systems and electronic data to carry out their missions. Increased computer connectivity has revolutionized the way governments are working in many countries across the world. With India's 'Big-leap' towards e-Governance, launched by DIT through the National e-Governance Plan, India is poised to join this league.

Effective working of any government department depends on the realization that 'information' is the most critical asset and needs to be protected. Protecting the confidentiality, integrity and availability of this information has become the key to smooth functioning of these government departments, enhancing transparency in their operations and ensuring legal compliance. The requirement for protecting the information has increased in recent times because the reliance of government departments on information systems and services, thus making them more

vulnerable to security threats. Interconnection of public and private networks and sharing of information resources has also added to the complexity of creating a seamless information infrastructure.

It has therefore become necessary for all government departments to understand the information security requirements in the context of their departmental objectives and incorporate appropriate security controls.

Information Security requirements can be identified from three main sources :

1. The first source is derived from assessing risks to government departments. Through risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.
2. The second source is the legal, statutory, regulatory and contractual requirements (if any) that a government department and its service providers have to satisfy.
3. The third source is the particular set of principles, objectives and requirements for information processing that a government department has developed to support its operations.

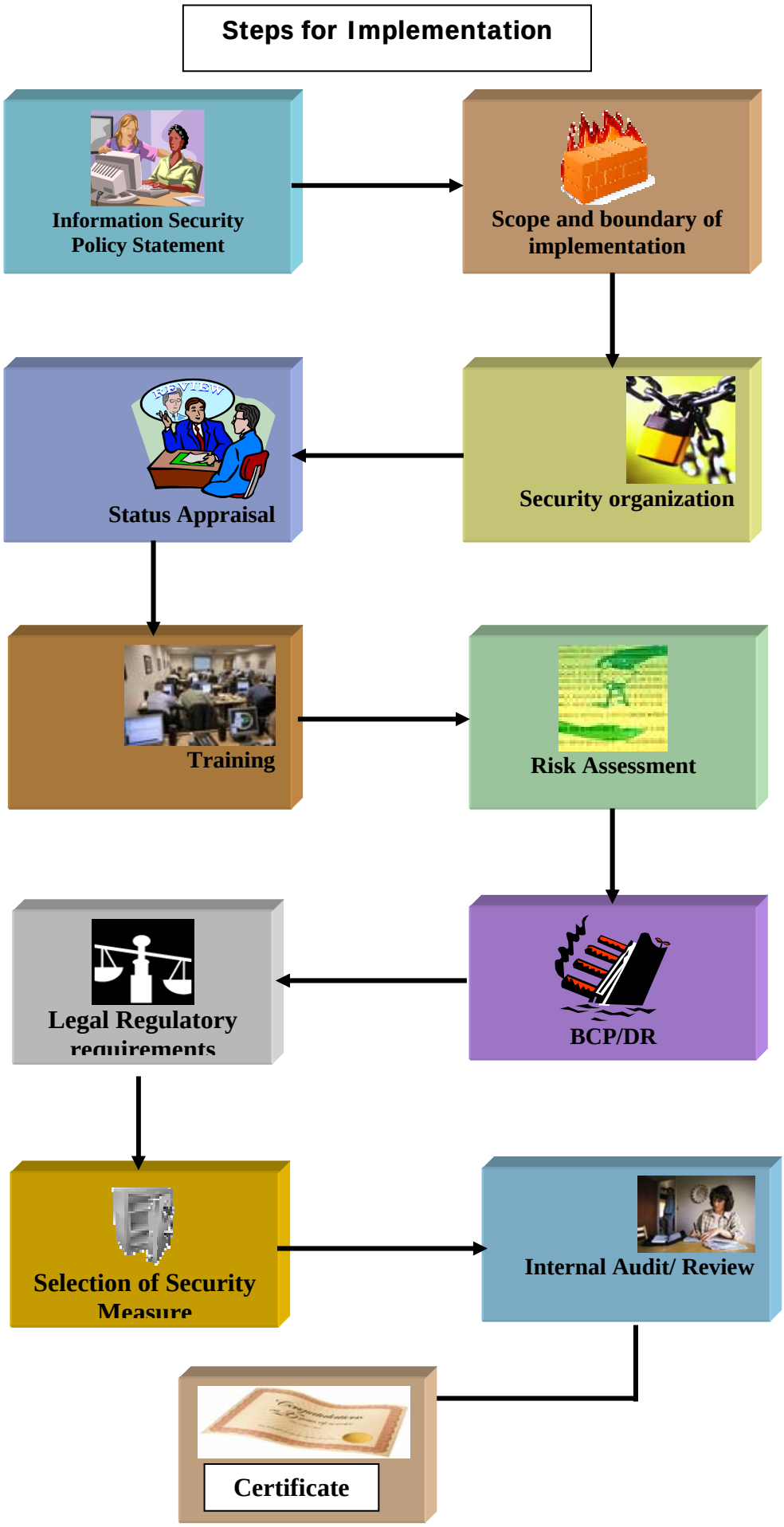
3.0 What factors lead to success of Information Security Programme ?

The following factors are often critical to the successful implementation of information security program in government departments :

a) Security policy, objectives and activities that reflect government objectives;
b) an approach to implementing security that is consistent with the culture;
c) Visible support and commitment from top management;
d) a good understanding of the security requirements, risk assessment and risk management;
e) Sensitizing to all concerned and seeking their support.
f) Distribution of guidance on information security policy and standards to all employees and stake holders;
g) Providing appropriate training and education;
h) a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

4.0 What are the steps of developing effective information security program?

For successful implementation of Information Security the programme must be developed and tailored to the specific organizational goals and objectives. However all effective security programmes have a common set of step by step approach based on various standards and guidelines. The following approach of Implementing Information Security programme is based on International Standard ISO/IEC 27001 (Information Technology – Security Techniques – Information Security Management Systems – Requirements) :


Steps for Implementation
Information Security Policy Statement
Scope and boundary of implementation
Security organization
Status Appraisal
Training
Risk Assessment
BCP/DR
Legal Regulatory requirements
Selection of Security Measure
Internal Audit/ Review
Certificate

Steps for Implementation		
S No	**Step**	**Description**
1.	**Information Security Policy Statement**	**Top management's commitment** to protect Information from loss of Confidentiality, Integrity and Availability in all its forms (Paper and other electronic form) in all stages of its life cycle e.g. origination, transmission, copying, storage and destruction
2.	**Scope and Boundary of Implementa-tion**	Based on the **criticality of the operations** (IT or Non IT dependent) and location, the scope and boundary for implementing the ISMS need to be worked out.
3.	**Security Organization**	Define **Management Structure and implementation Team**, representing various functions (HR, Admin, Legal etc) in the Organization besides IT with their clear roles and responsibilities.
4.	**Status Appraisal**	Organize **independent appraisal** of Implementation of existing Security policies, processes, networks and systems to identify the gaps against a Standard such as ISO 27001.
5	**Trainings**	a) Organize **Training Programs for Top Management, Executives and Implementers from IT** and other user Departments to bring general awareness and understanding of the standard in the context of their own working environment. This ensures effective implementation of Information Security at various levels and Departments while bridging the gaps identified at status appraisal above. b) Organize specific Training programmes for Implementation Team to develop methodologies and conduct Risk Assessment, **Business Continuity Planning (BCP), Disaster Recovery Plans(DRP), Incident Management** etc.
6	**Risk Assessment**	Conduct Risk Assessment to identify the **Risk Levels** for various Assets and Processes. Develop **Risk Mitigation Plans** based on the security needs.
7.	**Legal & other statutory requirements**	Based on the roles and responsibility of the Organization identify the **applicable Legal, Statutory, Regulatory requirements.**
8.	**Selection of Security Measures and implementa-tion**	Identify Security Measures based on the threats and Risks identified in the risk Assessment and the obligation of the Organization to comply with various Government policies, Laws and Regulations etc. These security measures can be selected from International Standard such as ISO 27001 comprising of **Physical Security, Human Resource Security, Network and Systems etc.** They can be in the form of **Security Policies & Procedures** and implemented through People, Process and Technology.
9	**Business Continuity Planning/ Disaster Recovery**	A **Business Continuity Management process** needs to be implemented to counteract interruptions to business activities and to protect critical processes from major failures and ensure their timely resumption to an acceptable level through a combination of preventive and recovery controls. **Develop continuity and disaster recovery plans** for the same

Steps for Implementation		
S No	**Step**	**Description**
10	**Internal Audits and Reviews**	Organize **internal audits** for Periodic Monitoring and improvement. The audit findings, security incidents, RA finding etc. to be **reviewed by the top management** to provide resources in terms of upgradation or new technology etc. This enables an effective implementation of ISMS with the continuous improvement.
11	**Certification**	As a means to demonstrates effective implementation of ISMS, Organization may apply for **Third Party certification** and organize for Assessment.

5. What are the information security laws, regulations etc, required to develop an effective information security program?

The government organization is required to identify all applicable laws, regulations and other government directives as applicable to their specific domain of work. Besides this they are also required to implement following Acts and their associated regulations:

a) IT Act
b) Right to Information Act
c) Copyright Act
d) Evidence Act

6. Which organizations can provide help in implementing and evaluating the effectiveness of information security program?

STQC is the first Certification Body, with international accreditation (RvA, Netherlands) in India, outside U.K. & Netherlands to provide Information Security Management System (ISMS) Certification to BS 7799-2 Standard and later upgraded to ISO 27001 Standard.

One of the largest certification body granted certification in diverse sectors in India & abroad like software Development, BPOs, Telecom, Automobiles, Banks, Manufacturing, Data Centres, Pharmaceutical. Some of the companies are Reliance IDC, Hughes Software, Satyam Computers, BHEL, Ranbaxy, ICICI, EXL, Tata Steel, Mphasis, Msource, Maruti, Ashok Leylands etc.

The only training organization in India having Lead Assessor programme approved by IRCA, UK and trained more than 700 personnel from various industries and organizations. STQC also conducts certified training programme for security professionals like Certified Ethical Hacking Professional, Certified Information Security Professional etc. More than 5000 personnel have been trained on these courses across the country. Details of the STQC services can be obtained from website **www.stqc.nic.in**

For Information related to other organizations providing guidance for implementation of Information Security Program, CERT-In India has a panel of 61 Organisations, details are available at their website www.cert-in.org.in.

For further details contact :

e-mail: mitali@ertleast.org, arvind@mit.gov.in, rakesh@mit.gov.in