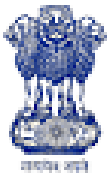
Document No: eSAFE-ISF01

Version: 1.0

January, 2010

E Governance Security Standards Framework:

An Approach Paper



Government of India
Department of Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

eGovernance Security Standards Framework

An Approach Paper

STQC IT Services

Contents

Figures

1 Introduction

STQC has been entrusted with the responsibility of developing the Information Security Standards and Guidelines for eGovernance in India. This paper presents an approach to identify the necessary standards and guidelines based on an Information Security Assurance Framework.

2 Information Security Assurance Framework

2.1 Information Security

eGovernance involves Information Technology enabled initiatives that are used for improving the interaction between Government and citizens or Government and business as well as the internal Government operations. To provide "trusted" services, eGovernance needs to focus on Effectiveness, Efficiency, Flexibility & Transparency.

If the citizen or end user is to derive maximum benefit from the provision of e-Services through e-Governance, the e-Service must possess the following attributes.

- The users must know the information about the available e-services;
- The users must be aware of the benefits of these services;
- The user should be able to locate the e-services easily;
- The e-services must be accessible to all members of the intended target groups;
- The information from the e-services should be comprehensive, correct, readily available, and easy to understand with respect to language and structure;
- The provision of e-services should be confidential, and in no way violate the privacy of either party;
- The design of eGovernance applications should comply with the existing legal data protection requirements and relevant legal and statutory laws & acts.

From the attributes it becomes evident that the "value" of information held and processed by the eGovernance service needs to be protected at all levels (i.e. Application, Infrastructure, and Operation & Management). Information security is intended to safeguard the information assets and is determined in terms of confidentiality, integrity and availability.

Confidentiality: Protecting sensitive information from unauthorized disclosure or intelligible interception

Integrity: Safeguarding the accuracy and completeness of information and software; protecting data from unauthorized, unanticipated or unintentional modification

Availability: Ensuring that information and vital IT services are available when required

To safeguard the "value" of information, effective security measures (that can limit the risks and vulnerability) need to be implemented harmoniously. These security measures provide layers of

protection to the Application, IT Infrastructure, Control & Management in a eGovernance computing environment.

In fact security of any information system is essentially an amalgamated output of Application Security, Infrastructure Security, and Secure Operation & Management. Enforcement of security at all levels is essential to achieve a fairly secure environment. As the probability of simultaneous failures of security at all layers is less this approach has been found to be the most effective in to-day's context. This layered approach is alternatively known as 'Defense in depth'.

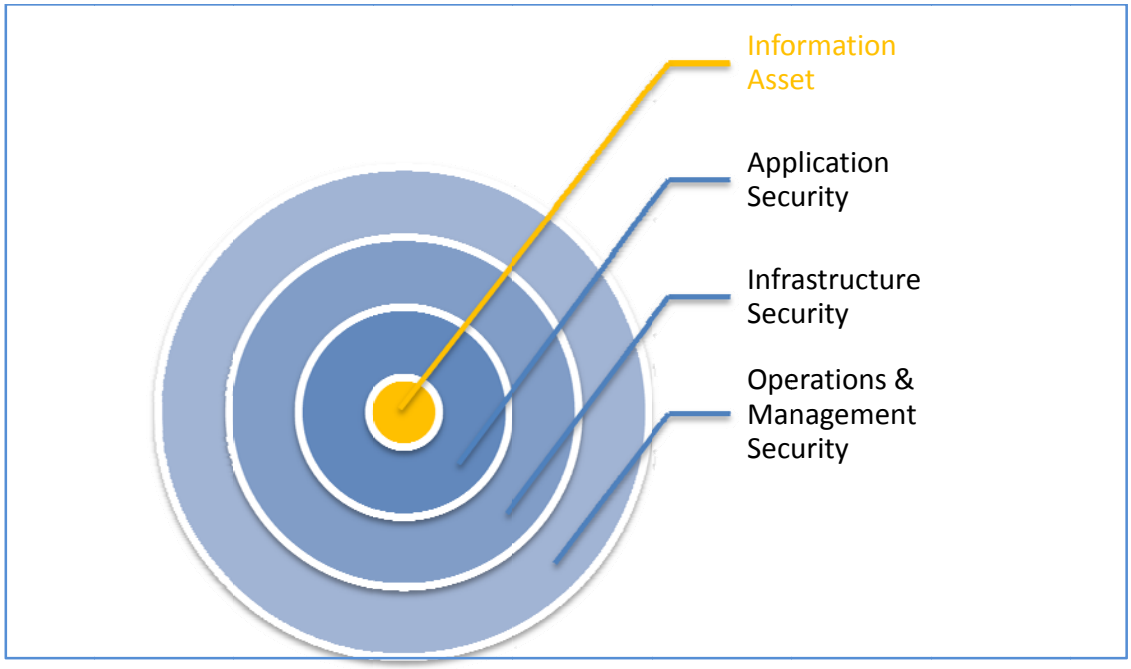


Figure 1: Security Layers

In considering the security measures at different levels that should be put in place, a risk analysis must be performed. The risk analysis must consider the intent, motivation and capability of sources of threat, the feasibility and potential frequency of methods of attack, the nature of vulnerabilities that may be exploited, the value of assets to be protected, the consequences of a successful attack and the cost of any counter measures.

2.2 Assurance Framework

It is well established that information security can be assured through selection of suitable security controls and management of risks. The key activities in assuring information security are

a) Categorization of information system
b) Selection of baseline security controls
c) Risk assessment
d) Refinement of the security controls based on risk assessment

e) Implementation of the security controls
f) Monitoring and analysis of the effectiveness of the security controls

The detail Information Security Assurance Framework will be described in ISF 01.

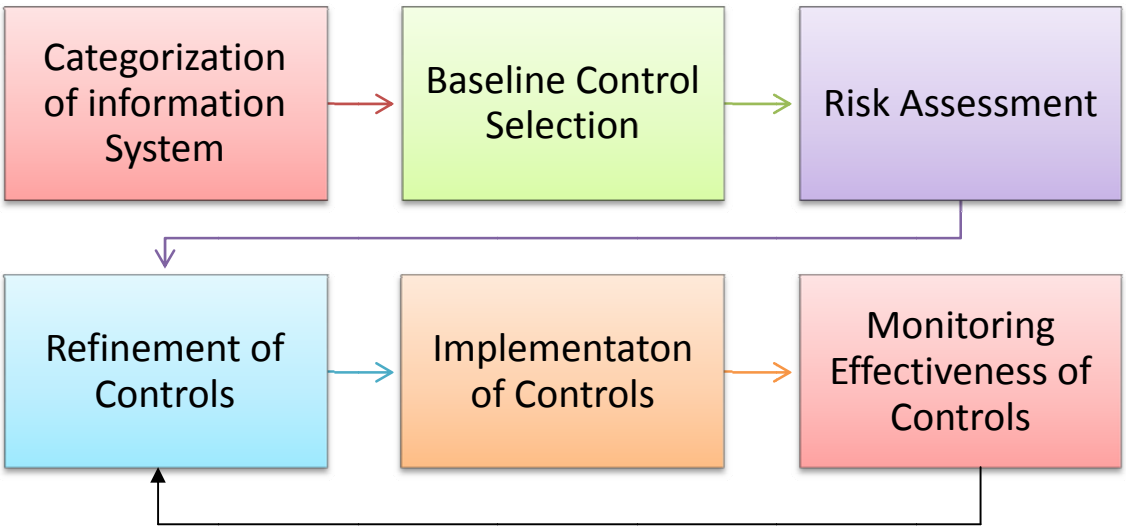


Figure 2: Information Security Assurance Framework

3 Categorization of Information System

The security categorization are done based on the potential impact on an organization, should certain events occur which jeopardizes the information system needed by the organization to accomplish its assigned mission, protect its assets, fulfil its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categorization should also consider the vulnerability and threat information corresponding to the information system. All information systems can be categorized as LOW IMPACT, MEDIUM IMPACT and HIGH IMPACT depending on the assessed impacts. A detail guideline document (GD 100) will be developed for this purpose.

4 Selection of Baseline Security Controls

Baseline Security Controls are the minimum information security requirements (Application Security, Infrastructure Security and Operations and Management Security) for information and information systems in each security category (LOW IMPACT, MEDIUM IMPACT and HIGH IMPACT). A guideline document (GD 200) will be developed which will list all possible security controls and act as a master catalog of all security controls.. Baseline security controls are subset of controls taken from the master

catalog. There will be three baseline documents LOW BASELINE (GD 201), MEDIUM BASELINE(GD 202), HIGH BASELINE (GD 203).

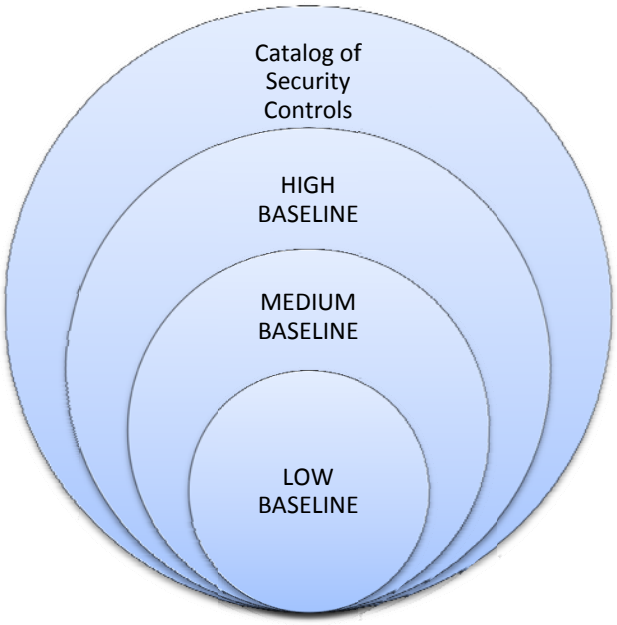


Figure 3: Security Controls

LOW BASELINE: Subset of basic level security controls taken from the master catalog of controls.

MEDIUM BASELINE: Builds on LOW BASELINE with additional controls taken from the master catalog of controls.

HIGH BASELINE: Builds on MEDIUM BASELINE with additional controls taken from the master catalog of controls.

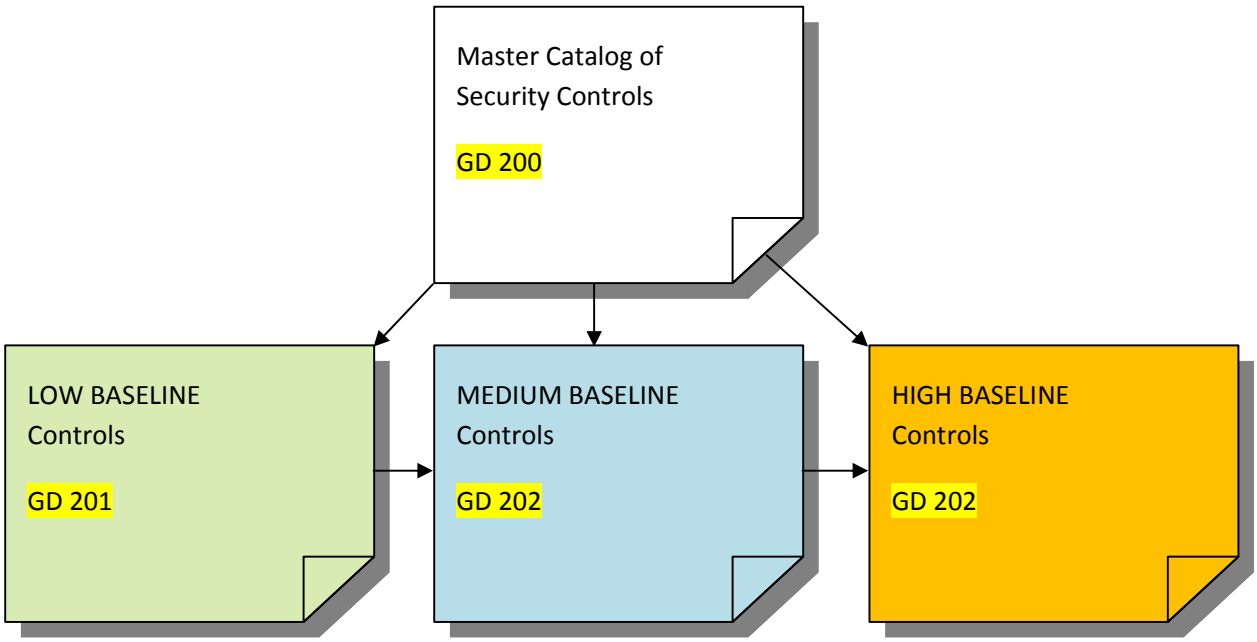


Figure 4: Baseline Security Controls

5 Risk Assessment

Over and above the baseline security controls depending on the operating environment and technology there can be some specific security requirements. These security requirements can be identified through a risk assessment process. Guideline document GD 300 will be developed to outline risk assessment and management methodologies.

6 Refinement of the Security Controls based on Risk Assessment

Based on the outcome of the risk assessment additional controls will be selected from the master catalog of controls.

7 Implementation of the Security Controls

After identification of the security controls it is necessary to implement the security controls in the respective information systems through managed processes. A guideline document GD 210 will be prepared which will outline implementation guidelines in details.

8 Monitoring and Analysis of the Effectiveness of the Security Controls

Monitoring and analysis of the effectiveness of the security controls can be conducted through periodic testing, evaluation, review of the implemented controls. A guideline document GD220 will be developed outlining the procedures of assessment of the effectiveness of the implemented security controls.

9 Information Security Standards and Guidelines

Document No.	Document Title
ISF 01	Information Security Assessment Framework
GD 100	Guidelines for Security Categorization of eGovernance Information Systems
GD 200	Catalog of Security Controls
GD 201	Baseline Security Controls for LOW IMPACT INFORMATION SYSTEMS
GD 202	Baseline Security Controls for MEDIUM IMPACT INFORMATION SYSTEMS
GD 203	Baseline Security Controls for HIGH IMPACT INFORMATION SYSTEMS
GD 210	Guidelines for Implementation Security Controls
GD 220	Guidelines for Assessment of Effectiveness of Security Controls
GD 300	Guidelines for Information Security Risk Assessment and Management

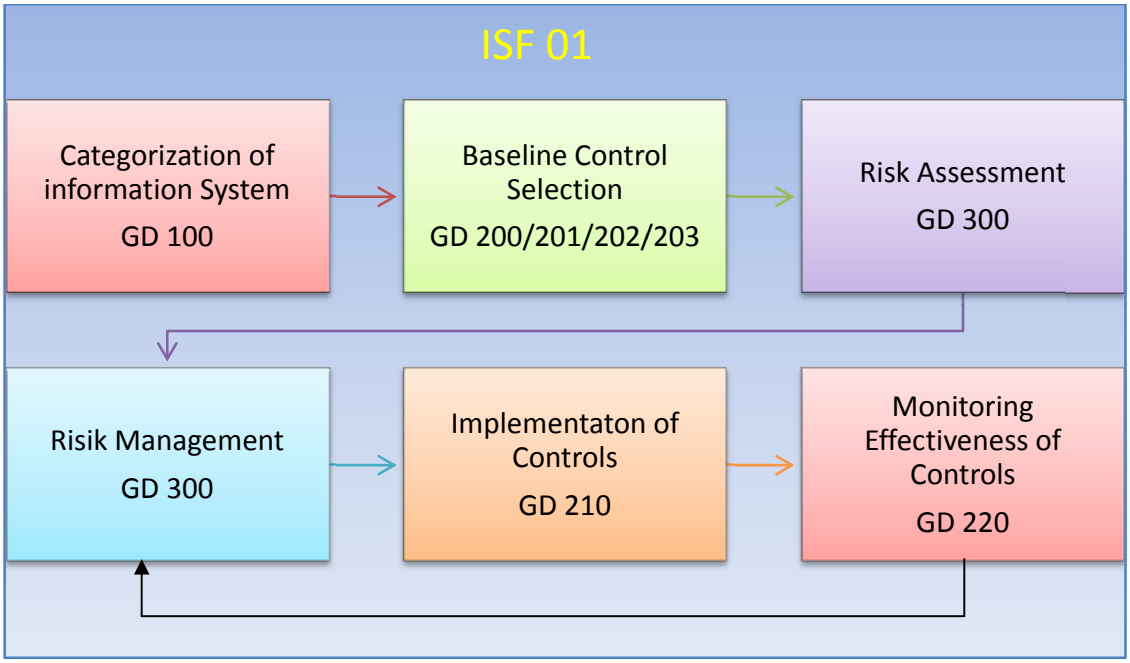


Figure 5: Information Security Standards and Guidelines Framework