e-Governance Security Assurance Framework - An Overview

Standardization Testing and Quality Certification Directorate (STQC)
DIT, MICT ,Government of India

Mitali Chatterjee, Senior Director
STQC Directorate, Kolkata & Chairperson of Expert Committee on Information Security

15th Jan 2010

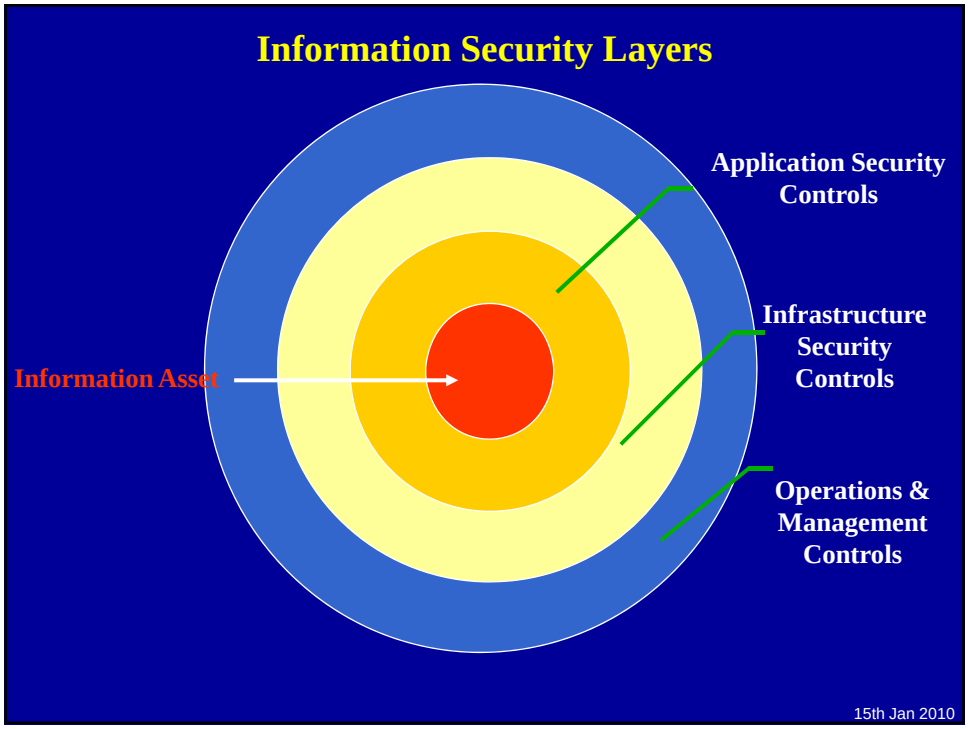
e-Governance Security Standards and Guidelines An Overview

Why Need for Information Security?

With the aim to provide "trusted" services by safeguarding the "information assets" in terms of confidentiality, integrity and availability. The "Value" of information held and processed by e-Governance services needs to be protected at all the following layers

- Application
- Infrastructure
- Operations and Management

15th Jan 2010



eSAFE Approach

eSAFE(e-Governance Security Assurance Framework) is based on:

- ISO 27001: the international standard for an Information Security Management System (ISMS)
- In line with Information Security Program for Federal Information Systems in USA - Federal Information Security Management Act (FISMA 2002)

15th Jan 2010

Basis of the approach

Need for compliance under IT Act

Under Section 43A of IT Act it is required to comply "reasonable security practices and procedures" and Government in consultation with professional bodies such as DSCI is in the process of prescribing ISO 27001 as reference standard

Adopting FISMA approach helps in:

- Categorizing e-Governance information systems based on the objectives of providing appropriate levels of information security according to a range of **risk levels**
- Identifying minimum information security requirements controls for information systems in each such category

15th Jan 2010

Risk And Risk Assessment

Risks are functions of the **likelihood** of a given **threat-source's** exploiting potential **vulnerabilities**, and the resulting **impacts** of that adverse event on the system or the organization.

Mathematically Risk = (Probability of a adverse event occurring)*(Impact of event occurring)

Risk Assessment: A report that shows an organization's vulnerabilities and the estimated cost of recovery in the event of damage. It also summarizes defensive measures and associated costs based on the amount of risk the organization is willing to accept (the risk tolerance).

A "Risk Analysis" is the process of arriving at a risk assessment, also called a "threat and risk assessment.

Refer document "Guidelines for Information Security Risk Assessment and Management eSAFEGD300"

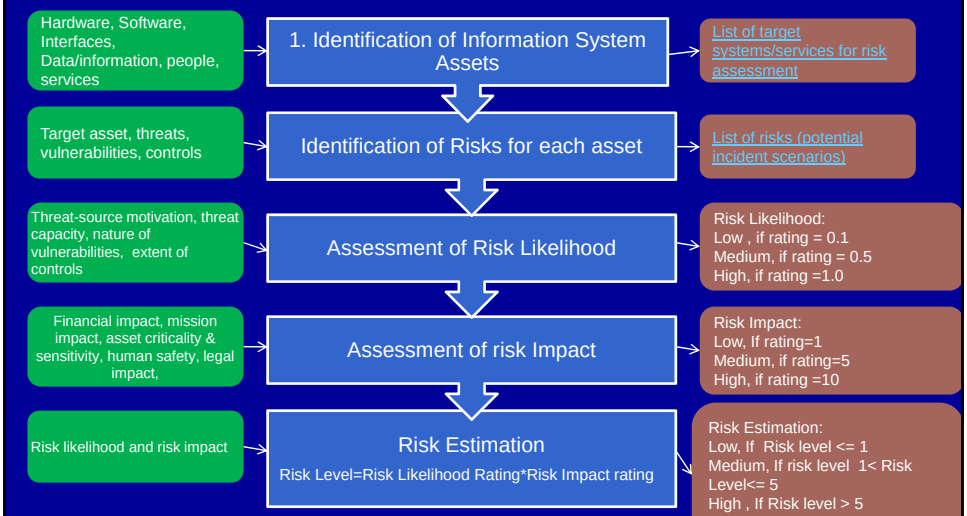
15th Jan 2010

Risk Levels

Risk Level	Risk Description
High	Risk needs to be mitigated as soon as possible. Risk treatment plan with identified additional controls and control improvements and time frame for implementation needs to be prepared.
Medium	Risk needs to be mitigated within a reasonable period of time. Risk treatment plan with identified additional controls and control improvements and time frame for implementation needs to be prepared.
Low	Risk is acceptable and no other control or control improvements are required.

15th Jan 2010

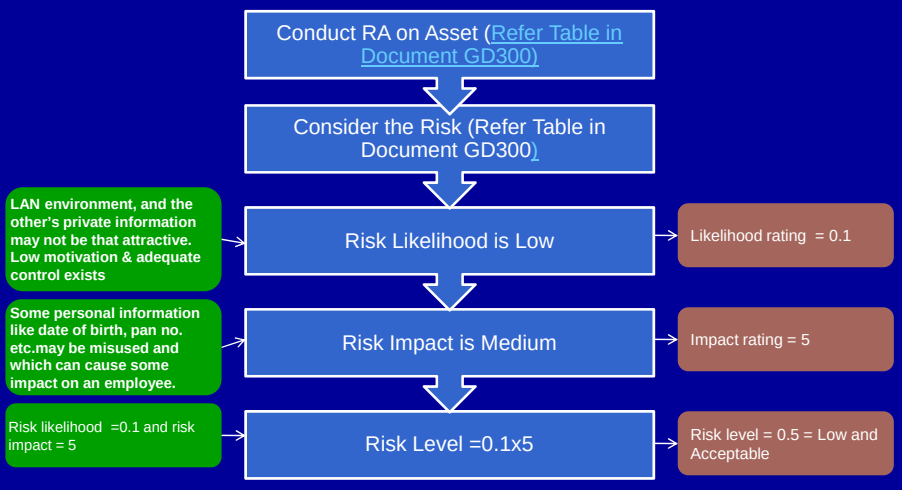
Risk Level Assessment Steps



Refer document "eSAFEGD300"(6.0 Risk Assessment)

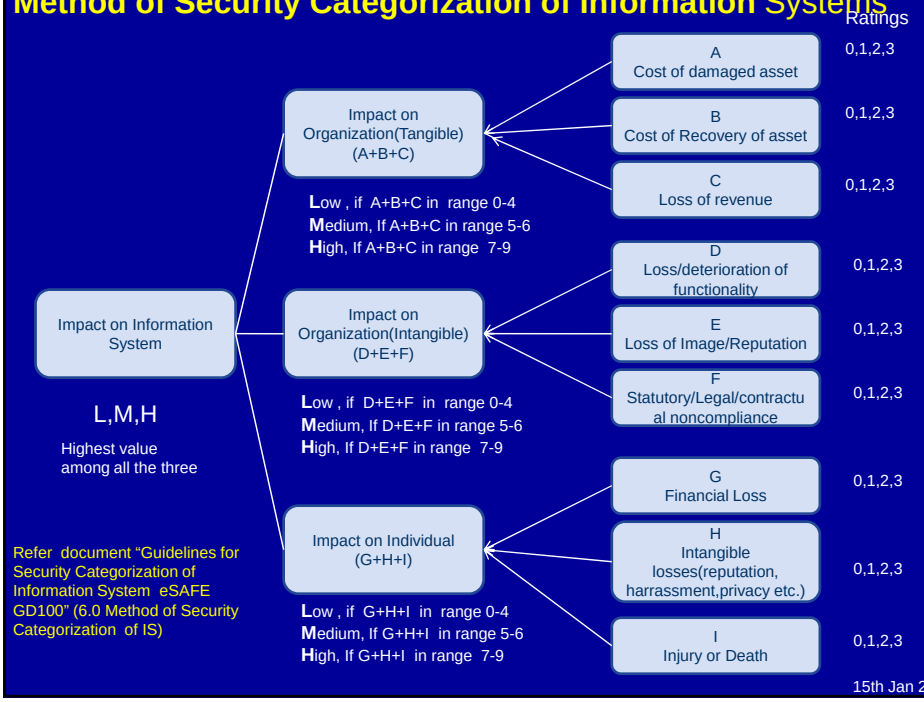
15th Jan 2010

Example: Risk Level Assessment



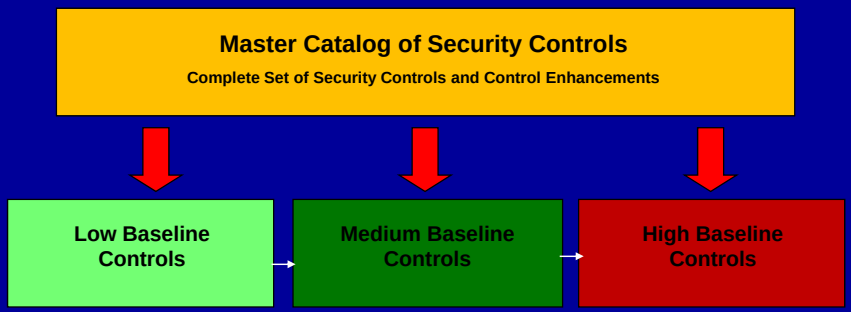
15th Jan 2010

Method of Security Categorization of Information Systems



15th Jan 2010

Security Control Baselines



Low Baseline

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Medium Baseline

Builds on Low Baseline with ***additional controls, and control enhancements selected from the master catalog***

High Baseline

Builds on Medium Baseline with ***additional controls, and control enhancements selected from the master catalog***

15th Jan 2010

Example of a control

O.BC-8: INFORMATION SYTEM BACKUP & RECOVERY

Control: Back-up of information (user-level and system- level information) and software contained in the information system shall be taken at defined frequency and protected at storage location.

Explanation: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the recovery time objectives (RTO) and recovery point objectives (RPO). While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media

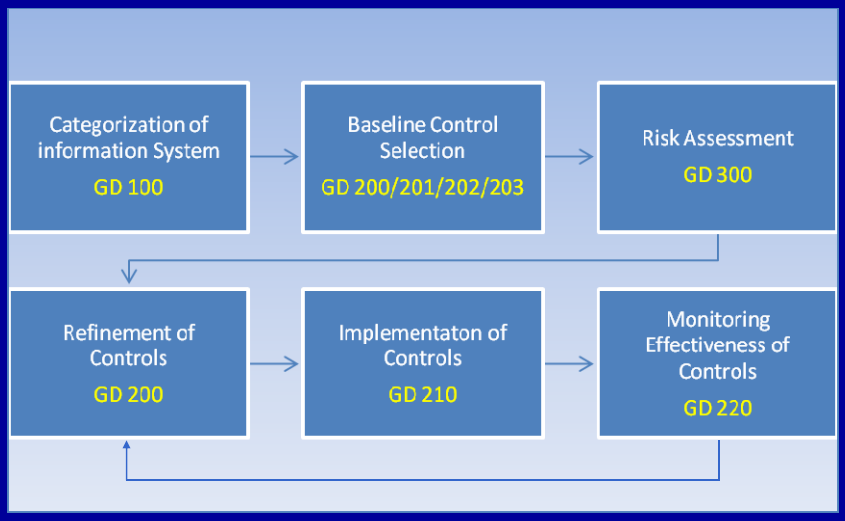
Control Improvements:

I. The back-up information shall be tested at a specified frequency in accordance with agreed back-up policy to verify media reliability and information integrity
II. The backup information shall be selectively used in the restoration of information system functions as a part of contingency plan testing
III. The backup copies of the operating system and other critical information system software shall be stored in a separate facility or in a fire-proof container that is not collocated with the operational software
IV. The system backup information shall be protected from unauthorized modification

	Low	Medium	High	RA
O.BC-8: INFORMATION SYSTEM BACK UP AND RECOVERY	☑	☑, (i), (ii)	☑, (i), (ii), (iii)	(iv)

15th Jan 2010

Documents under e-Governance Security Assurance Framework (eSAFE)



15th Jan 2010

Title of Document	Scope of Document	Target Audience
ISF 01 e-Governance Security Standards Framework: An Approach Paper	presents an approach to identify the necessary standards and guidelines based on an Information Security Assurance Framework.	1. **Concerned managers and Employees for information security risk assessment management within an organization** 2. **Third party service provider supporting such activities.**
eSAFE-GD100 Guidelines for Security Categorization of Information System	Classify information systems based on potential impacts to the organization in case of security breaches. The guideline can be applied for all information systems to be used for e-Governance by all government departments and the third party service providers	
eSAFE-GD200 Catalog of Security Controls	Provide guidelines for selecting and specifying security controls for information systems for e-Governance of the state and central governments of India. The guidelines apply to all components of an information system that process, store, or transmit information	
eSAFE-GD201 **eSAFE-GD202** **eSAFE-GD203** Baseline Security Controls for Low Impact ,Medium Impact and High Impact Information Systems	provide guidelines for specifying security controls for low impact, Medium Impact and High Impact information systems for e-Governance of the state and central governments of India. The guidelines apply to all components of an information system that process, store or transmit information.	
eSAFE-GD300 Guidelines for Information Security Risk Assessment and Management	Provides guidelines for Information Security Risk Assessment and Management in an e-Governance project, supporting the e-Governance Security Standards Framework (eSAFE). This document can also be used to conduct risk assessment and risk management to comply the requirements of ISO/IEC 27001.	
eSAFE-GD210 Guidelines for Implementation of Security Control	Under preparation	
eSAFE-GD220 Guidelines for Assessment of effectiveness of security controls	Under preparation	

15th Jan 2010

List of documents under e-Governance Security Framework

ISF 01	Information Security Assessment Framework
GD 100	Guidelines for Information System Categorization
GD 200	Catalog of Security Controls
GD 201	Baseline Security Control for LOW IMPACT INFORMATION SYSTEMS
GD 202	Baseline Security Control for MEDIUM IMPACT INFORMATION SYSTEMS
GD 203	Baseline Security Control for HIGH IMPACT INFORMATION SYSTEMS
GD 210	Guidelines for Implementation of Security Controls
GD 220	Guidelines for Assessment of Effectiveness of Security Controls
GD 300	Guidelines for Information Security Risk Assessment and Management

- *Released for use by Stakeholders in e-Governance Applications*
- *Draft Documents under preparation by the Core group members from STQC*

15th Jan 2010

Expert Committee on Information Security

- Core Group Members from STQC :
- Ms. Mitali Chatterjee, Senior Director , Chairperson
- Mr. Arvind Kumar, Director
- Mr. N.E. Prasad, Director
- Mr. B.K. Mondal, Director
- Mr. Alok Sain, Director
- Mr. Subhendu Das, Director

- Review committee members:
- Mr. B.J. Srinath, Senior Director, CERT-In, New Delhi
- Dr. N. Sarat Chandra Babu, Director, C-DAC, Hyderabad
- Ms.Anjana Choudhary,Deputy Director General NIC,NewDelhi
- Mr. R. Ramesh, TD, OTC, NIC Chennai
- Prof. Chandan Mazumder, Jadavpur University, Kolkata

15th Jan 2010

Thank you

15th Jan 2010