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

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)

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

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"
**Risk Levels**

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>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.</td>
</tr>
<tr>
<td>Medium</td>
<td>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.</td>
</tr>
<tr>
<td>Low</td>
<td>Risk is acceptable and no other control or control improvements are required.</td>
</tr>
</tbody>
</table>

**Risk Level Assessment Steps**

1. Identification of Information System Assets
2. Identification of Risks for each asset
3. Assessment of Risk Likelihood
4. Assessment of Risk Impact
5. Risk Estimation

Refer document "eSAFE/GO300" (6.0 Risk Assessment)
Example: Risk Level Assessment

Conduct RA on Asset (Refer Table in Document GD300)

Consider the Risk (Refer Table in Document GD300)

Risk Likelihood is Low

Likelihood rating = 0.1

Risk Impact is Medium

Impact rating = 5

Risk Level = 0.1 x 5

Risk level = 0.5 = Low and Acceptable

LAN environment, and the other’s private information may not be that attractive, low motivation & adequate control exists

Some personal information like date of birth, pan no. etc. may be misused and which can cause some impact on an employee.

Risk likelihood = 0.1 and risk impact = 5

Method of Security Categorization of Information Systems

Impact on Organization(Tangible) (A+B+C)

Low, if A+B+C in range 0-4
Medium, if A+B+C in range 5-6
High, if A+B+C in range 7-9

Impact on Organization(Intangible) (D+E+F)

Low, if D+E+F in range 0-4
Medium, if D+E+F in range 5-6
High, if D+E+F in range 7-9

Impact on Individual (G+H+I)

Low, if G+H+I in range 0-4
Medium, if G+H+I in range 5-6
High, if G+H+I in range 7-9

L, M, H
Highest value among the three

Refer document “Guidelines for Security Categorization of Information System eSAFE GD100” (6.0 Method of Security Categorization of IS)
Example of a control

O.BC-8: INFORMATION SYSTEM 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 backup 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

<table>
<thead>
<tr>
<th>O.BC-8: INFORMATION SYSTEM BACKUP &amp; RECOVERY</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ID</td>
<td>[a], [b]</td>
<td>[a], [b], [c], [d]</td>
<td>[x]</td>
</tr>
</tbody>
</table>
Documents under e-Governance Security Assurance Framework (eSAFE)

Title of Document | Scope of Document | Target Audience
--- | --- | ---

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 | 2. Third party service provider supporting such activities.

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 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-GD202 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 Controls | Under preparation |  
eSAFE-GD220 Guidelines for Assessment of effectiveness of security controls | Under preparation |
List of documents under e-Governance Security Framework

<table>
<thead>
<tr>
<th>Document Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISF 01</td>
<td>Information Security Assessment Framework</td>
</tr>
<tr>
<td>GD 100</td>
<td>Guidelines for Information System Categorization</td>
</tr>
<tr>
<td>GD 200</td>
<td>Catalog of Security Controls</td>
</tr>
<tr>
<td>GD 201</td>
<td>Baseline Security Control for LOW IMPACT INFORMATION SYSTEMS</td>
</tr>
<tr>
<td>GD 202</td>
<td>Baseline Security Control for MEDIUM IMPACT INFORMATION SYSTEMS</td>
</tr>
<tr>
<td>GD 203</td>
<td>Baseline Security Control for HIGH IMPACT INFORMATION SYSTEMS</td>
</tr>
<tr>
<td>GD 210</td>
<td>Guidelines for Implementation of Security Controls</td>
</tr>
<tr>
<td>GD 220</td>
<td>Guidelines for Assessment of Effectiveness of Security Controls</td>
</tr>
<tr>
<td>GD 300</td>
<td>Guidelines for Information Security Risk Assessment and Management</td>
</tr>
</tbody>
</table>

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, New Delhi
  - Mr. R. Ramesh, TD, OTC, NIC Chennai
  - Prof. Chandan Mazumder, Jadavpur University, Kolkata

15th Jan 2010
Thank you