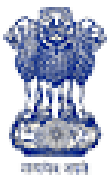
Document No: eSAFE-GD100

Version: 1.0

January, 2010

E Security Assurance Framework:

Guidelines for Security Categorization of Information System
eSAFE-GD100



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

Guidelines for Security Categorization of Information Systems

GD 100

Department of IT
Government of India
Ministry of Communications & IT
Electronics Niketan, 6 CGO Complex
New Delhi – 110003

Introduction

National Information Security Assurance Framework for eGovernance has identified the need to develop various standards and guidelines to ensure information security in various eGovernance information systems. This document will provide guidelines for categorizing the information systems used for eGovernance to enable selection of appropriate levels of security measures. The guidelines will give an idea about the types of information and information systems to be included in each category.

This guideline is one of the documents identified in the eGovernance Security Assurance Framework (eSAFE). The list of the documents is given below.

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 of Security Controls
GD 220	Guidelines for Assessment of Effectiveness of Security Controls
GD 300	Guidelines for Information Security Risk Assessment and Management

Contents

Figures

Tables

1 Scope

1.1 Objective

To provide a guideline to classify information systems based on potential impacts to the organization in case of security breaches.

1.2 Description

The guideline can be applied for all information systems to be used for eGovernance by all government departments and the third party service providers.

2 Target Audience

Managers and concerned employees of Govt. departments and the third party service providers of Information System Security.

3 Type of Document

It is a Guidelines document recommended for enforcement in systems for eGovernance.

4 Definitions and Acronyms

AVAILABILITY: Ensuring timely and reliable access to and use of information.

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

INFORMATION: An instance of an information type.

INFORMATION RESOURCES: Information and related resources, such as personnel, equipment, funds, and information technology.

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.

INFORMATION SYSTEM: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

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: (i) requires the use of such equipment; or (ii) 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 TYPE: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

INTEGRITY: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

5 Categorization of Information Systems

This guideline establishes security categories for information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill 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.

Security Attributes

It is well known that information security is nothing but preservation of the following three attributes of security. All security impacts are basically breach of one or more of these security attributes.

Confidentiality(C)

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…”

A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity (I)

INTEGRITY
“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”

A loss of *integrity* is the unauthorized modification or destruction of information.

Availability (A)

“Ensuring timely and reliable access to and use of information…”

A loss of *availability* is the disruption of access to or use of information or an information system.

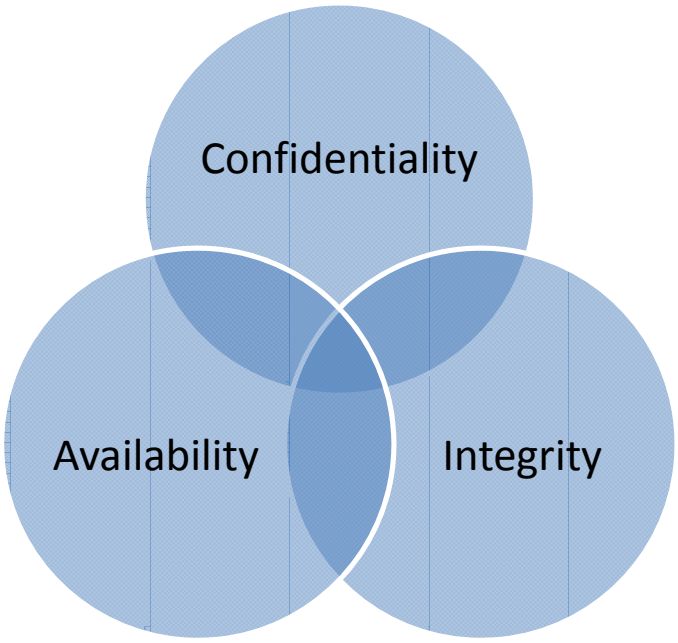


Figure 1: Information Security Attributes

Potential Impact

All information systems can be categorized as LOW IMPACT, MEDIUM IMPACT and HIGH IMPACT depending on the assessed impacts.

LOW IMPACT

The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on **organization** [1]and **individuals**[2].

MEDIUM IMPACT

The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organization and individuals.

HIGH IMPACT

The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organization and individuals.

[1] Organization is the Government department, who owns the information system.
[2] Individuals are the personnel using or associated with the information system.

6 Method of Security Categorization for Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values can be determined by assessing the organization and individual impacts corresponding to breaches of the security attributes (Confidentiality, Integrity and Availability). The overall impact on an information system is a function of different impacts which are described below.

6.1 Impact on Organization (Tangible)

Impacts on organization caused due to direct financial losses in case of compromise or weaknesses of the system. These impacts can be measured quantitatively.

6.1.1 Cost of damaged assets

Financial impact caused due to loss or damage of assets like hardware, software and other infrastructure.

6.1.2 Cost of recovery

Financial impact caused due to the efforts required to repair of hardware, rebuilding of software, recreation of information and restoration of services. It includes the cost to identify, remediate, recover and resume operations for each system.

6.1.3 Loss of revenue

Financial impact caused due to outages of the revenue generating systems/services.

6.2 Impact on Organization (Intangible)

Impacts on organization caused due to indirect financial or other losses in case of compromise or weaknesses of the system. These impacts cannot be measured quantitatively but can be assessed qualitatively as ‘high’, ‘medium’, ‘low’ etc.

6.2.1 Loss/deterioration of functionality

Impacts caused due to loss, degradation or interruptions in services provided by the system. Impacts caused due to failure of missions and objectives.

6.2.2 Loss of image/reputation

Impacts caused due to loss of user confidence, loss of goodwill/negative effects on reputation, weakening of negotiating capability, loss of competitive advantage, loss of trust, loss of technical reputation etc.

6.2.3 Statutory/Legal/Contractual noncompliance

Impacts caused due to inability to fulfill legal , statutory and contractual obligations, breach of contract with third parties, cost of judicial proceedings and penalties,

6.3 Impact on Individuals

Impacts faced by the third parties using the system due to weaknesses or compromise of the system.

6.3.1 Financial loss

Impacts caused due to direct financial losses incurred by the third parties or individuals transacting or using the system.

6.3.2 Intangible loss

Impacts caused due to intangible losses such as breach of privacy, harassment etc faced by the third parties or individuals using the system.

6.3.3 Injury or Death

Impacts caused due to injury or death of the third parties in case of compromise or weaknesses of the system.

The relationship between the contributing impacts on the overall information system is shown in the following diagram (Figure 2).

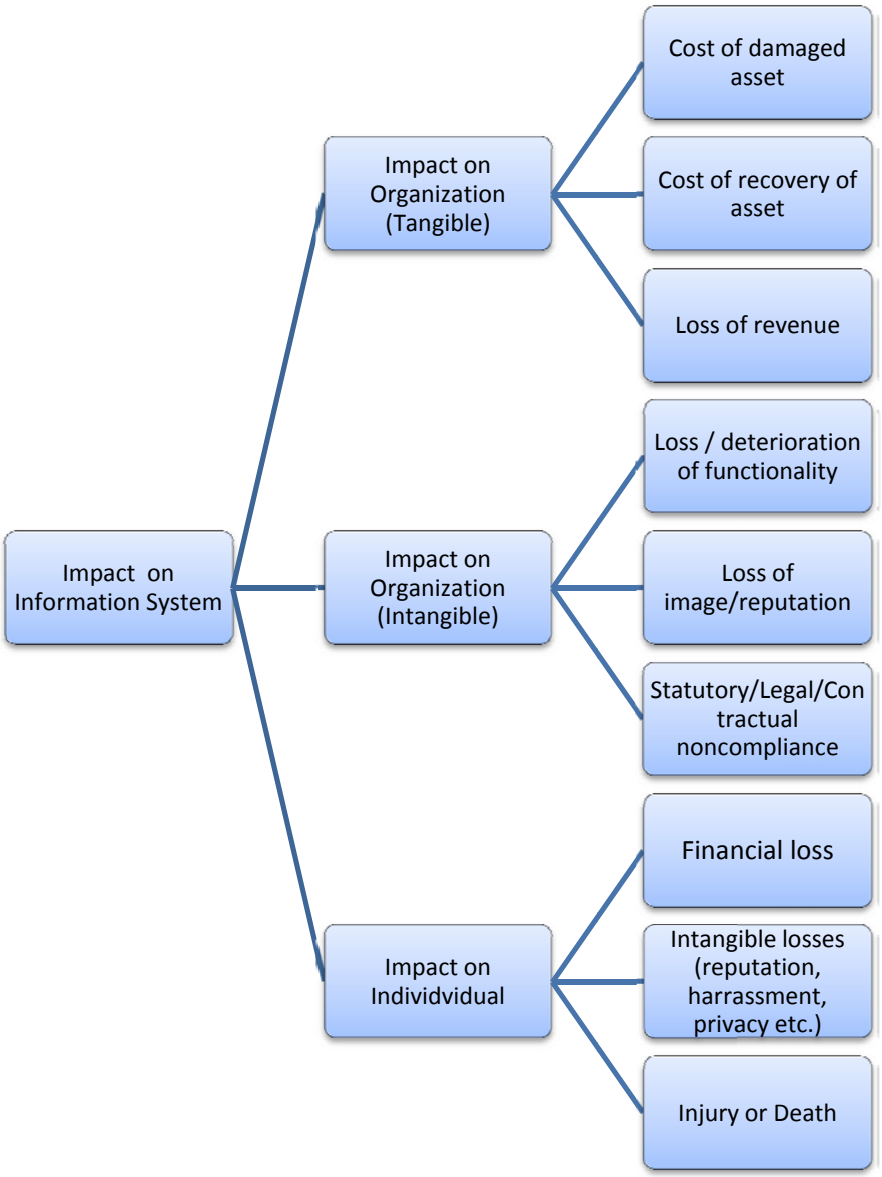


Figure 2: Impact Relationships

From the above impact relationship the impact analysis will be carried out by following bottom up approach.

Step 1: Evaluate "Impact on Organization (Tangible)" as a function of 'cost of damaged asset', 'cost of recovery' and 'loss of revenue'. As illustrated below.

Assign a value of 1, 2, or 3 to the 'cost of damaged asset' depending on the level of expected damage due to security breaches. For minor damage value is 1, for significant damage the value is 2, for catastrophic damage the value is 3. In case of no damage the value is 0

Assign a value of 1, 2, or 3 to the 'cost of recovery' depending on the level of expected recovery cost due to security breaches. For low cost the value is 1, for moderate cost the value is 2, for high cost the value is 3. In case of no cost involved for recovery the value is 0

Assign a value of 1, 2, or 3 to the 'loss of revenue' depending on the level of expected revenue loss due to security breaches. For minor loss the value is 1, for significant loss the value is 2, for catastrophic loss the value is 3. In case of no loss of revenue the value is 0.

Add the 3 values to find out the Impact on Organization (Tangible) from Table 1.

Step 2: Evaluate "Impact on Organization (Intangible)" as a function of 'loss/deterioration of functionality', 'loss of image/reputation', and 'statutory/legal/contractual liability'. As illustrated below.

Assign a value of 1, 2, or 3 to the 'loss/deterioration of functionality' depending on the level of expected loss/deterioration due to security breaches. For minor deterioration the value is 1, for significant deterioration the value is 2, for total loss the value is 3. In case of no loss/deterioration of functionality the value is 0

Assign a value of 1, 2, or 3 to the 'loss of image/reputation' depending on the level of expected loss due to security breaches. For minor loss the value is 1, for significant loss the value is 2, for severe or total loss of image/reputation the value is 3. In case of no loss of image/reputation the value is 0.

Assign a value of 1, 2, or 3 to the 'statutory/legal/contractual noncompliance' depending on the level of noncompliance due to security breaches. For minor noncompliance the value is 1, for significant noncompliance the value is 2, for total noncompliance the value is 3. In case of no noncompliance the value is 0.

Add the 3 values to find out the Impact on Organization (Intangible) from Table 1.

Step 3: Evaluate "Impact on Individual" as a function of 'financial loss', 'intangible losses' and 'injury or death'. As illustrated below.

Assign a value of 1, 2, or 3 to the 'financial loss' depending on the level of expected loss due to security breaches. For minor loss the value is 1, for significant loss the value is 2, for total severe loss the value is 3. In case of no financial loss the value is 0

Assign a value of 1, 2, or 3 to the 'intangible loss ' depending on the level of expected loss due to security breaches. For minor loss the value is 1, for significant loss the value is 2, for severe loss the value is 3. In case of no intangible losses the value is 0.

Assign a value of 1, 2, or 3 to the 'injury or death' depending on the level of expected injury due to security breaches. For minor injury the value is 1, for major injury the value is 2, for death of individual the value is 3. In case of no injury or death the value is 0.

Add the 3 values to find out the Impact on Organization (Intangible) from Table 1.

Table 1: Impact Matrix 1

Total Value	Impact
0-4	LOW
5-6	MEDIUM
7-9	HIGH

Step-4: Find out impact on the Information System as function of 'Impact on Organization (Tangible)', 'Impact on Organization (Intangible)' and 'Impact on Individual' by considering the highest impact value (Refer Table 2), which is nothing but the Scurity Category of the Information System.

Table 2: Impact Matrix 2

Impact on Organization (Tangible)	Impact on Organization (Intangible)	Impact on Individual	Overall Impact on Information System
LOW	LOW	LOW	LOW
LOW	LOW	MEDIUM	MEDIUM
LOW	LOW	HIGH	HIGH
LOW	MEDIUM	LOW	MEDIUM
LOW	MEDIUM	MEDIUM	MEDIUM
LOW	MEDIUM	HIGH	HIGH
LOW	HIGH	LOW	HIGH
LOW	HIGH	MEDIUM	HIGH
LOW	HIGH	HIGH	HIGH
MEDIUM	LOW	LOW	MEDIUM
MEDIUM	LOW	MEDIUM	MEDIUM
MEDIUM	LOW	HIGH	HIGH
MEDIUM	MEDIUM	LOW	MEDIUM
MEDIUM	MEDIUM	MEDIUM	MEDIUM
MEDIUM	MEDIUM	HIGH	HIGH
MEDIUM	HIGH	LOW	HIGH
MEDIUM	HIGH	MEDIUM	HIGH
MEDIUM	HIGH	HIGH	HIGH
HIGH	LOW	LOW	HIGH
HIGH	LOW	MEDIUM	HIGH
HIGH	LOW	HIGH	HIGH
HIGH	MEDIUM	LOW	HIGH
HIGH	MEDIUM	MEDIUM	HIGH
HIGH	MEDIUM	HIGH	HIGH
HIGH	HIGH	LOW	HIGH
HIGH	HIGH	MEDIUM	HIGH
HIGH	HIGH	HIGH	HIGH

Annexure-1: Examples of Security Categorization

Table 3 and Table 4 illustrate application of the security categorization method for two different types of information systems.

Table 3: Example Worksheet for Security Categorization of Information System 'AGMARKET'

Name of the eGov Application	AGMARKNET	
Related department	Department of agriculture	
Purpose	AGMARKNET aims at connecting agricultural produce wholesale markets in the country for sharing market information. AGMARKNET portal has been evolved to strengthen interfaces among Agricultural Marketing related Government and Non Government organizations, farmers, traders, exporters, policy makers, academic institutions etc.(http://www.agmarknet.nic.in)	
Step-1: Assessment of Impact on Organization (Tangible)	a. Cost of damaged asset	1
	b. Cost of recovery	1
	c. Loss of revenue	0
	Total (a+b+c)	2
	Impact on organization (tangible)	LOW
Step-2: Assessment of Impact on Organization (Intangible)	a. Loss/deterioration of functionality	2
	b. Loss of image/reputation	2
	c. Statutory/Legal/Contractual noncompliance	2
	Total (a+b+c)	6
	Impact on organization (intangible)	MEDIUM
Step-3: Assessment of Impact on Individual	a. Financial loss	1
	b. Intangible loss	2
	c. Injury & death	0
	Total (a+b+c)	3
	Impact on individuals	LOW
Step-4: Assessment of Impact on the Information System / Security categorization of the Information System	Impact on organization (tangible)	**LOW**
	Impact on organization (intangible)	**MEDIUM**
	Impact on individuals	**LOW**
	SECURITY CATEGORY: MEDIUM IMPACT	

Table 4: Example Worksheet for Security Categorization of Information System 'ePost'

Name of the eGov Application	ePOST	
Related department	Department of post	
Purpose	Messages can be sent any where in India through Post Offices using the ePOST software.(http://indiapost.nic.in)	
Step-1: Assessment of Impact on Organization (Tangible)	d. Cost of damaged asset	1
	e. Cost of recovery	1
	f. Loss of revenue	3
	Total (a+b+c)	5
	Impact on organization (tangible)	MEDIUM
Step-2: Assessment of Impact on Organization (Intangible)	d. Loss/deterioration of functionality	2
	e. Loss of image/reputation	3
	f. Statutory/Legal/Contractual noncompliance	2
	Total (a+b+c)	7
	Impact on organization (intangible)	HIGH
Step-3: Assessment of Impact on Individual	d. Financial loss	1
	e. Intangible loss	2
	f. Injury & death	0
	Total (a+b+c)	4
	Impact on individuals	LOW
Step-4: Assessment of Impact on the Information System / Security categorization of the Information System	Impact on organization (tangible)	**MEDIUM**
	Impact on organization (intangible)	**HIGH**
	Impact on individuals	**LOW**
	SECURITY CATEGORY: HIGH IMPACT	

Annexure-2: Blank Worksheet for Security Categorization

Name of the eGov Application		
Related department		
Purpose		
Step-1: Assessment of Impact on Organization (Tangible)	g. Cost of damaged asset	
	h. Cost of recovery	
	i. Loss of revenue	
	Total (a+b+c)	
	Impact on organization (tangible)	
Step-2: Assessment of Impact on Organization (Intangible)	g. Loss/deterioration of functionality	
	h. Loss of image/reputation	
	i. Statutory/Legal/Contractual noncompliance	
	Total (a+b+c)	
	Impact on organization (intangible)	
Step-3: Assessment of Impact on Individual	g. Financial loss	
	h. Intangible loss	
	i. Injury & death	
	Total (a+b+c)	
	Impact on individuals	
Step-4: Assessment of Impact on the Information System / Security categorization of the Information System	Impact on organization (tangible)	
	Impact on organization (intangible)	
	Impact on individuals	
	SECURITY CATEGORY:	

7 References

[1] FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems

8 Acknowledgements to the contributors

Members of the core group in STQC

Ms. Mitali Chatterjee, Senior Director (Convener)

Mr. Arvind Kumar, Director

Mr. N.E. Prasad, Director

Mr. B.K. Mondal, Director

Mr. Aloke Sain, Director

Mr. Subhendu Das, Director