Document No: eSAFE-GD300
Version: 1.0
January, 2010

E Security Assurance Framework: Guidelines for Information Security Risk Assessment and Management eSAFE-GD300

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

Guidelines for Information Security Risk Assessment and Management

eSAFE

GD 300

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

Introduction

Given the sophistication of today's cyber-threats and the rich targets that government information systems provide, eSAFE security standards and guidelines need to be flexible and extensible. In that light, risk assessment plays an important part in eGovernance IS program and overall protection strategy.

Once a eGovernance project choose and tailor the baseline security controls based on the initial security categorization as per GD100 and the respective baseline security control sets (GD201, GD202, GD203), they must select additional controls based on risk assessment. The assessment is employed in a more targeted manner to consider additional threat information, specific mission requirements, operating environments, and any other factors that might affect accomplishment of the project's mission or functions.

The eGovernance projects can add appropriate security controls or control improvements from the GD200 catalog, demonstrating the commitment to increasing information-system security levels beyond required minimum baselines. Once agreed on the security controls, those need to be documented and implemented in the eGovernance project.

This guideline documents information security risk assessment and management methodology for eGovernance projects and 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

Tables

Figures

1.0 Scope

1.1 Objective

This document provides guidelines for Information Security Risk Assessment and Management in an eGovernance project, supporting the eGovernance 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.

1.2 Description

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organization's environment, and in particular should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of ISMS.

2.0 Target Audience

This document is relevant to concerned managers and staff for information security risk assessment and management within an organization. It is also relevant for the external parties supporting such activities.

3.0 Type of Document

It is a Guidelines document recommended for enforcement in systems for e-Governance.

4.0 Definitions and Acronyms

For the purposes of this document, the terms and definitions given in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC Guide 73:2002, NIST SP 800-30 and the following apply.

Impact: Adverse change to the level of business objectives achieved

Information security risk: Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
(*NOTE: It is measured in terms of a combination of the likelihood of an event and its consequence.*)

Risk avoidance: Decision not to become involved in, or action to withdraw from, a risk situation [ISO/IEC Guide 73:2002]

Risk identification: Process to find, list and characterize elements of risk [ISO/IEC Guide 73:2002]
Risk reduction: Actions taken to lessen the probability, negative consequences, or both, associated with a risk [ISO/IEC Guide 73:2002]
Risk retention: Acceptance of the burden of loss or benefit of gain from a particular risk [ISO/IEC Guide 73:2002]

(*NOTE : In the context of information security risks, only negative consequences (losses) are considered for risk retention.*)

Risk transfer: Sharing with another party the burden of loss or benefit of gain, for a risk [ISO/IEC Guide 73:2002]
(*NOTE: In the context of information security risks, only negative consequences (losses) are considered for risk transfer*.)

Threat: The potential for a threat-source to exploit (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat-source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

5.0 Information Security Risk Management Process

Risk management process consists of three broad sub-processes risk assessment, risk treatment and risk monitoring and review. The process diagram is given in Figure-1

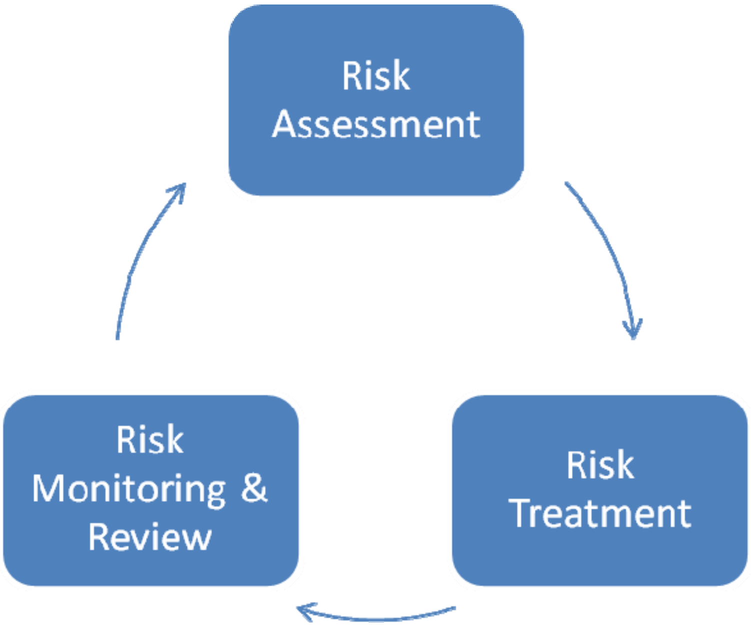


Figure 1: Risk Management Process

Figure 1 illustrates, the information security risk management process is an iterative process. The iterative approach provides a good balance between minimizing the time and effort spent in identifying or improving controls.

The table-1 summarizes the information security risk management activities relevant to the four phases of the ISMS process:

Table 1: Information Security Risk Management Process vis-à-vis ISMS PDCA

ISMS Process	Information Security Risk Management Process
Plan	Risk assessment, Risk treatment plan
Do	Implementation of the risk treatment plan
Check	Continual monitoring and reviewing of the risks
Act	Maintain and improve the Information Security Risk Management Process

6.0 Risk Assessment

Risk assessment is the first sub-process of the risk management process. Risk assessment is used to estimate levels of the identified risks on the target information system assets. The **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.

Risk assessment method consists of four primary steps, (1) identification of information system assets, (2) identification of risks for each of the assets, (3) assessment of risk likelihood, (4) assessment of risk impact on the asset and/or the organization, (5) Estimation of level of risk. The risk assessment method is represented diagrammatically in Figure-2

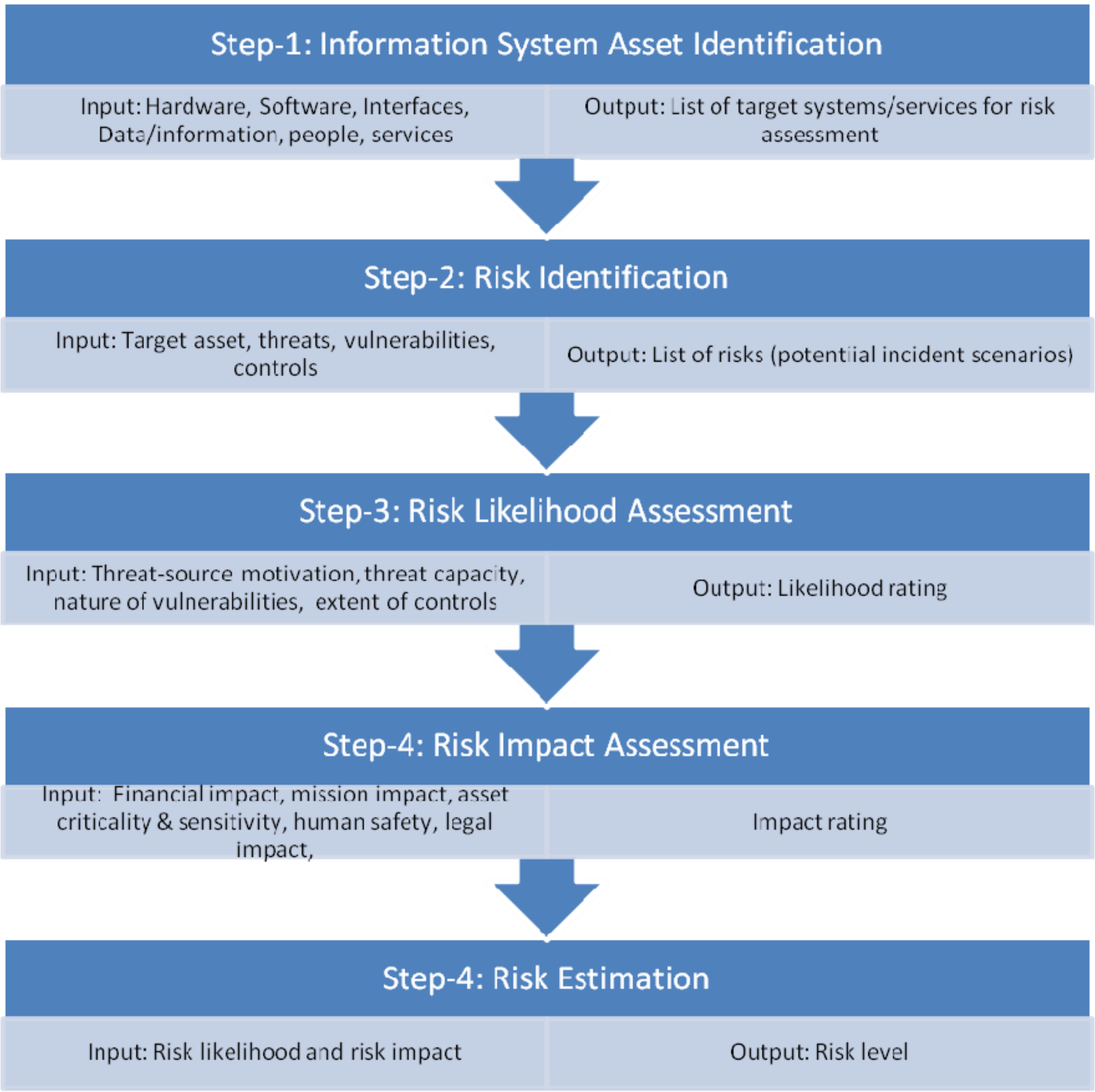

Step-1: Information System Asset Identification
Input: Hardware, Software, Interfaces, Data/information, people, services
Output: List of target systems/services for risk assessment
Step-2: Risk Identification
Input: Target asset, threats, vulnerabilities, controls
Output: List of risks (potential incident scenarios)
Step-3: Risk Likelihood Assessment
Input: Threat-source motivation, threat capacity, nature of vulnerabilities, extent of controls
Output: Likelihood rating
Step-4: Risk Impact Assessment
Input: Financial impact, mission impact, asset criticality & sensitivity, human safety, legal impact,
Impact rating
Step-4: Risk Estimation
Input: Risk likelihood and risk impact
Output: Risk level

Figure 2: Risk Assessment Method

6.1 Step-1: Information System Asset Identification

Purpose of this step is to establish the scope of risk assessment by identifying the target information system assets. These are usually all information systems which help to carry out various business/mission processes or services. Each information system may consist of a group of supporting assets like hardware, software, network, data/information, users/operators, interfaces etc. However, the risk assessment can be done on individual supporting assets also if required. A typical list of information systems is given in Appendix-1

6.2 Step-2: Risk Identification

In this step for each target assets identified in step-1 a set of potential risks are identified. These risks are nothing but some incident scenarios. An incident scenario describes a threat-source which may cause damage to the asset by exploiting a vulnerability or set of vulnerabilities. Output of this step will be an array of risks with unique risk-id, risk-description and associated threats and vulnerabilities. All these information should be captured in the Risk Assessment Sheets (Refer Appendix-2 for a typical Risk Assessment Sheet). Create Risk Assessment Sheets for each identified risks.

6.3 Step-3: Risk Likelihood Assessment

After identifying the risks or incident scenarios, it is necessary to assess the likelihood of each risk. Level of risk depends upon this likelihood value. This should take account of how often the threats occur and how easily the vulnerabilities may be exploited, considering:

I. Experience and applicable statistics for threat likelihood.
II. For deliberate threats: the motivation, capabilities and resources available to the threat-sources, as well as the perception of attractiveness and vulnerability of the target assets for the threat-source.
III. for accidental threats : geographical factors e.g. proximity to chemical or petroleum plants, the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction.
IV. Identified vulnerabilities, both individually and in aggregation.
V. Existing controls or the baseline controls and how effectively they reduce the vulnerabilities.

The likelihood of a risk or incident scenario can be described as high, medium, or low. Table 2 below defines these three likelihood levels.

Output of this step will be risk likelihood level for each identified risks which will be recorded in the respective Risk assessment sheets.

Table 2: Risk Likelihood Definition

Likelihood Level (L)	Likelihood Definition
High(1)	The threat-source is highly motivated and sufficiently capable and having adequate resources, and controls to prevent exploitation of the vulnerabilities are ineffective.
Medium(0.5)	The threat-source is motivated and capable with adequate resources, but controls are in place that may impede successful exploitation of the vulnerabilities
Low(0.1)	The threat-source lacks motivation or capability or without adequate resources, or controls are in place to prevent, or at least significantly impede, the exploitation of the vulnerabilities.

6.4 Step-4: Risk Impact Assessment

In this step level of adverse impact is assessed which is required in estimating risk level. The adverse impact of a security incident can be described in terms of loss or degradation of any, or a combination of the following three security goals: confidentiality, integrity and availability. The following

I. **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

II. **Loss of Availability:** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

III. **Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Private data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low. All types of impacts can easily be described as high, medium, and low. Table 3 below defines this impact levels.

Output of this step will be risk impact level for each identified risks which will be recorded in the respective Risk assessment sheets.

Table 3: Risk Impact Definition

Impact Level(I)	Impact Definition
High (10)	Exploitation of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium (5)	Exploitation of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (1)	Exploitation of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

6.5 Step-5: Risk Estimation

In this step risk is estimated as a function of Risk Likelihood and Risk Impact (Risk Level = Likelihood Level x Impact Level) from the following Risk Level Matrix (Ref: Table 4). The Risk Levels will be Low, Medium or Low. Table 5 briefly describes the implications of the Risk Levels. Record the risk levels in the respective Risk Assessment Sheets.

Table 4: Risk Level Matrix

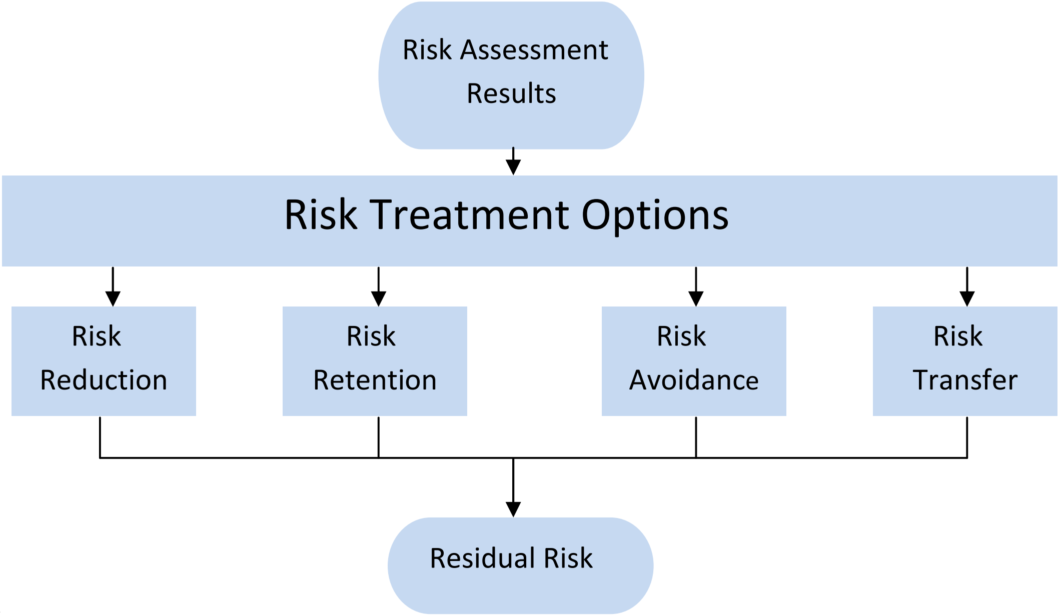
	Impact Level (I)		
Likelihood Level (L)	LOW (1)	MEDIUM (5)	HIGH (10)
HIGH (1)	Low (1x1=1)	Medium (1x5=5)	High (1x10=10)
MEDIUM (0.5)	Low (0.5x1=0.5)	Medium (0.5x5=2.5)	Medium (0.5x10=5)
LOW (0.1)	Low (0.1x1=0.1)	Low (0.1x5=0.5)	Low (0.1x10=1)
Risk Level: Low (≤ 1), Medium (> 1 and ≤ 5), High (> 5)			

Table 5: Risk Level

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.

7.0 Risk Treatment

Risk treatment is a systematic approach to mitigate the assessed risks by exercising various options available. There are four options available for risk treatment: risk reduction, risk retention, risk avoidance and risk transfer. Figure 3 illustrates the risk treatment activity.



.

Figure 3: Risk Treatment

Risk reduction: Risk can be reduced by selecting additional controls or improving the existing controls. For example selection of the controls and the control improvements may be done from the document GD 200, over and above the existing baseline controls.

Risk retention: If the level of risk meets the risk acceptance criteria the risk can be retained or accepted. ISO 27001 uses the term "risk acceptance" instead of "risk retention". For example, risk level of 4 can be retained if the risk is acceptable if it is less than 5.

Risk avoidance: When an identified risk is too high or the risk treatment cost exceeds the benefit, the risk may be avoided by withdrawing the concerned activities and looking for suitable alternatives. For example if it is perceived that outsourcing of network management activity has very high risk due to sensitivity of a project, take the decision to not outsource instead build your own team for network management.

Risk transfer: Some type of risks can be transferred to external parties. E.g. purchasing of insurance, outsourcing or obtaining managed services from external parties.

Risk treatment options should be selected based the expected cost for implementing these options and the expected benefits from these options. When large reductions in risks may be obtained with relatively low expenditure, such options should be implemented.

In general, the adverse consequences of risks should be made as low as possible. For some rare and severe risks controls are not justifiable on strictly economic grounds but need to be implemented. (For example, business continuity controls considered to cover specific high risks).

The four options for risk treatment are not mutually exclusive. Sometimes it is beneficial to use those options in combination.

Once the risk treatment options have been decided and a risk treatment plan is made, residual risks need to be determined. This involves an update of the risk levels (in the corresponding Risk Assessment Sheets), determined earlier by considering the effects of the risk treatment.

8.0 Risk Monitoring and Review

Risks are not generally static as threats, vulnerabilities, likelihood or impact may change anytime. Therefore, constant monitoring is necessary to detect the changes. Monitoring of the following is necessary.

I. Addition of new assets
II. Change in asset values
III. New threats that has not been considered during last assessments
IV. New vulnerabilities discovered
V. Information security incidents
VI. Change in risk impact
VII. Change in controls/countermeasures
VIII. Change in business/legal/contractual requirements

The outcome of risk monitoring activities may be input to risk review. The risks should be reviewed regularly and in light of the above changes.

9.0 References

[1] eSAFE GD 100: Guidelines for Security Categorization of Information Systems

[2] eSAFE GD 200: Catalog of Security Controls

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

[4] NIST SP 800-53: Recommended Security Controls for Federal Information Systems

[5] NIST SP 800-30: Risk Management Guide for Information Technology Systems

[6] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

[7] ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

[8] ISO/IEC 27005: Information technology – Security techniques – Information security risk management

[9] ISO/IEC Guide 73:2002: Risk management – Vocabulary – Guidelines for use in standards

10.0 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

Appendix-1: A Typical List of Information System Assets

#	Asset Description	Supporting Assets
1	Finance Management System	Hardware: … Software … Data/Information … Services …
2	HR Management System	-do-
3	Salary Processing System	-do-
4	Production Management System	-do-
5	Internet Portal	-do-
6	Intranet Portal	-do-
7	Email Service	-do-
8	Internet Service	-do-
9	VPN (Remote Access)Service	-do-
10	Routing Service	-do-
11	DNS Service	-do-
12	FTP Service	-do-
13	File Server	-do-
14	LDAP Server	-do-
15	Anti-Virus System	-do-

#	Asset Description	Supporting Assets
16	Central Logging Server	-do-
17	OS Update Services	-do-
18	Back-up System	-do-
19	Network Management System	-do-
20	Printing Service	-do-
21	Scanning Service	-do-
23	User Workstations	-do-
24	LAN	-do-
25	Wi Fi Service	-do-
26	Firewall	-do-
27	IDS/IPS	-do-
28	Leased Line	-do-
29	Support: Service - Power Supply	-do-
30	Support Service - Air Conditioning	-do-

Appendix-2: Risk Assessment Sheet

RISK ASSESSMENT SHEET			
Asset:	<Name of the Target Information System Asset>		
Risk No:	<Risk ID>	Risk Description:	<Describe the risk or incident scenario>
Threat Description:	<Describe the threat, threat-source>		
Vulnerabilities:	<List relevant vulnerabilities>		
Existing Controls:	<List relevant existing or planned controls or baseline controls>		
Likelihood Level:	<Value>	<Rationale>	
Impact Level:	<Value>	<Rationale>	
Risk Level:	<Value>	<Remarks>	
Risk Treatment Actions:	<List Selcted Controls or Cotrol Improvements or any other actions>		
Revised Likelihood Level:	<Value>	<Rationale>	
Revised Impact Level:	<Value>	<Rationale>	
Residual Risk Level:	<Value>	<Remarks>	

Appendix-3: Risk Assessment Example 1

RISK ASSESSMENT SHEET			
Asset:		Intranet Information Portal for Employees	
Risk No:	R0012	Risk Description:	Attacker's access to employee private data by Dictionary or Brute Force Attack on the 'Login' page.
Threat Description:		Attacker can be any user having legitimate access to the portal. He can use easily available password cracking tool or write scripts to find out a user's password and can get access to her private data.	
Vulnerabilities:		The application uses form based authentication but it has not incorporated any mechanism to limit unsuccessful attempts of login.	
Existing Controls:		(i) The portal can be accessed from the LAN. No access is possible from Internet or public network, (ii) All users are made aware about selection of quality passwords, (iii) Physical and logical access to the LAN workstations are restricted to the employees only.	
Likelihood Level:		Low 0.1	Since it is restricted to LAN environment, and the other's private information may not be that attractive to motivate the employees to attack.
Impact Level:		5 Medium	Some personal information like date of birth, pan no. etc.may be misused and which can cause some impact on an employee.
Risk Level:		0.5	Risk level is Low since it is less than 1. Risk is acceptable.
Risk Treatment Actions:		NA	
Revised Likelihood Level:		<Value>	<Rationale>
Revised Impact Level:		<Value>	<Rationale>
Residual Risk Level:		0.5	Low Risk

Appendix-4: Risk Assessment Example 2

RISK ASSESSMENT SHEET			
Asset:		Government Information Portal	
Risk No:	R0006	Risk Description:	Defacing of the website
Threat Description:		Defacement of webpages by malicious users.	
Vulnerabilities:		Lack of regular vulnerability assessment of the web application.	
Existing Controls:		(i) The webserver is placed behind a sophisticated firewall and access to the site is possible through port 80 and 443 only with associated security measures like IPS, (ii) No uploading of contents to the site is allowed from Internet, (iii) Web application is thoroughly tested and the associated infrastructure and operating environment is hardend before opening to the Internet, (iv) All changes of contents of the site is carried out by authorised persons by following change control procedure. (iv) The webserver is located in the datacentre, which is under strict physical and logical access control, (v) The server is protected by antivirus with facility to auto update, (vi) The OS and application servers are regularly patched for security as soon as they are available.	
Likelihood Level:		Medium 0.5	Although many controls have been implemented, still moderate likelihood exists because, (i) It is a Government site and many anti-Government/Country activists are there in Internet, (ii) The web application is not assessed for vulnerability and configuration mistakes regularly.
Impact Level:		High 10	Huge loss of reputation and image of the Government/Country.
Risk Level:		5	Risk level is Medium. Risk is not acceptable and needs to be treated.
Risk Treatment Actions:		Define and Implement a technical vulnerability assessment policy and procedure to conduct vulnerability assessment of the application after any changes in the application or operating environment as well as at a regular interval (say at least once in a quarter)	
Revised Likelihood Level:		Low 0.1	The above additional control will reduce the risk likelihood.
Revised Impact Level:		High 10	No change.
Residual Risk Level:		1	The residual Risk is Low and acceptable.