INFORMATION SECURITY MANAGEMENT

MODELS AND FRAMEWORKS FOR INFORMATION SECURITY MANAGEMENT

DAY-4, SESSION-3

AGENDA

- DIETY - e-Governance Security Standards Framework
- DIETY - Guidelines for Security Categorization of Information System (To be finalized by DIETY)

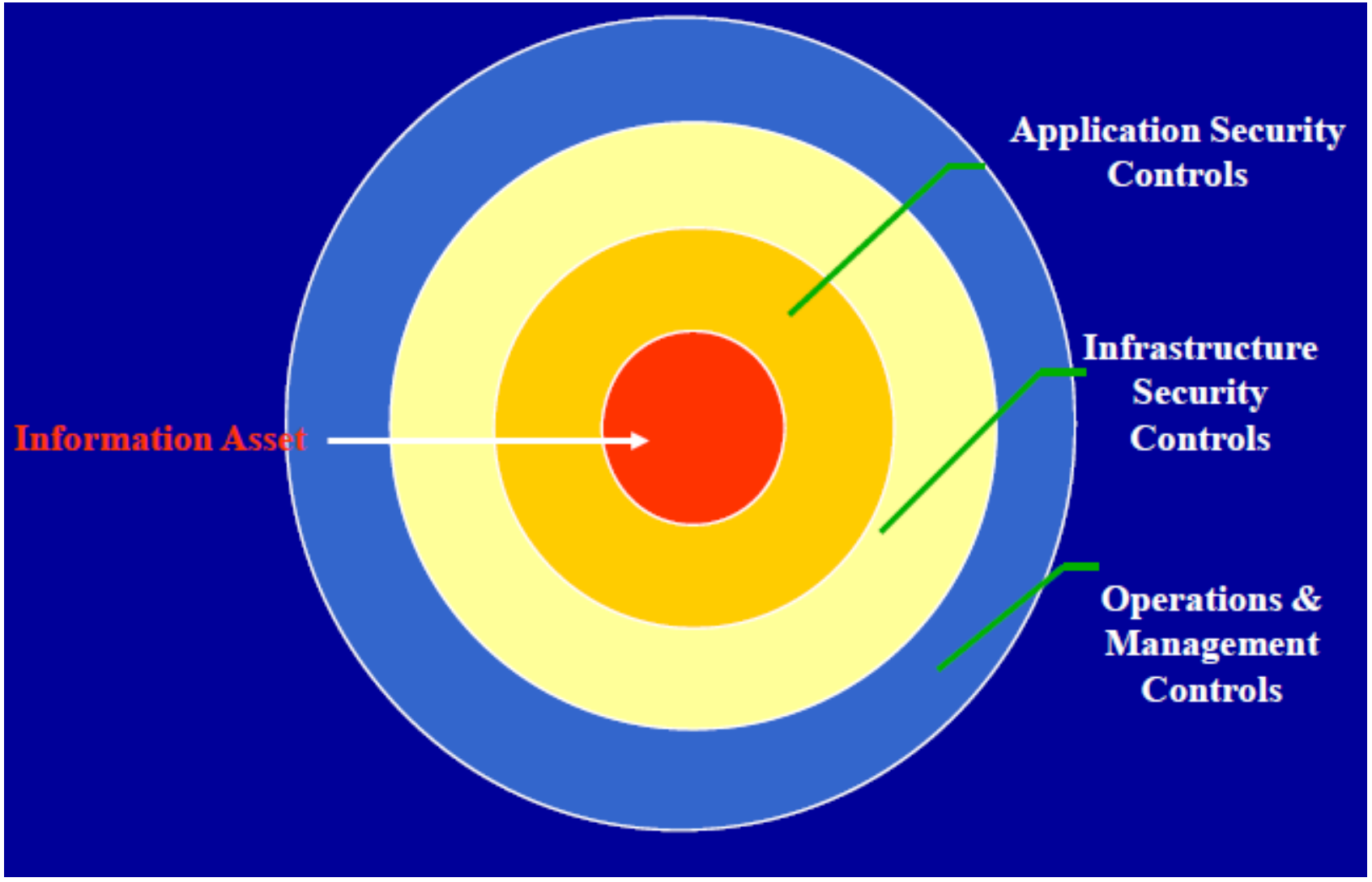
DIETY - e-Governance Security Standards Framework

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

INFORMATION SECURITY LAYERS



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)

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

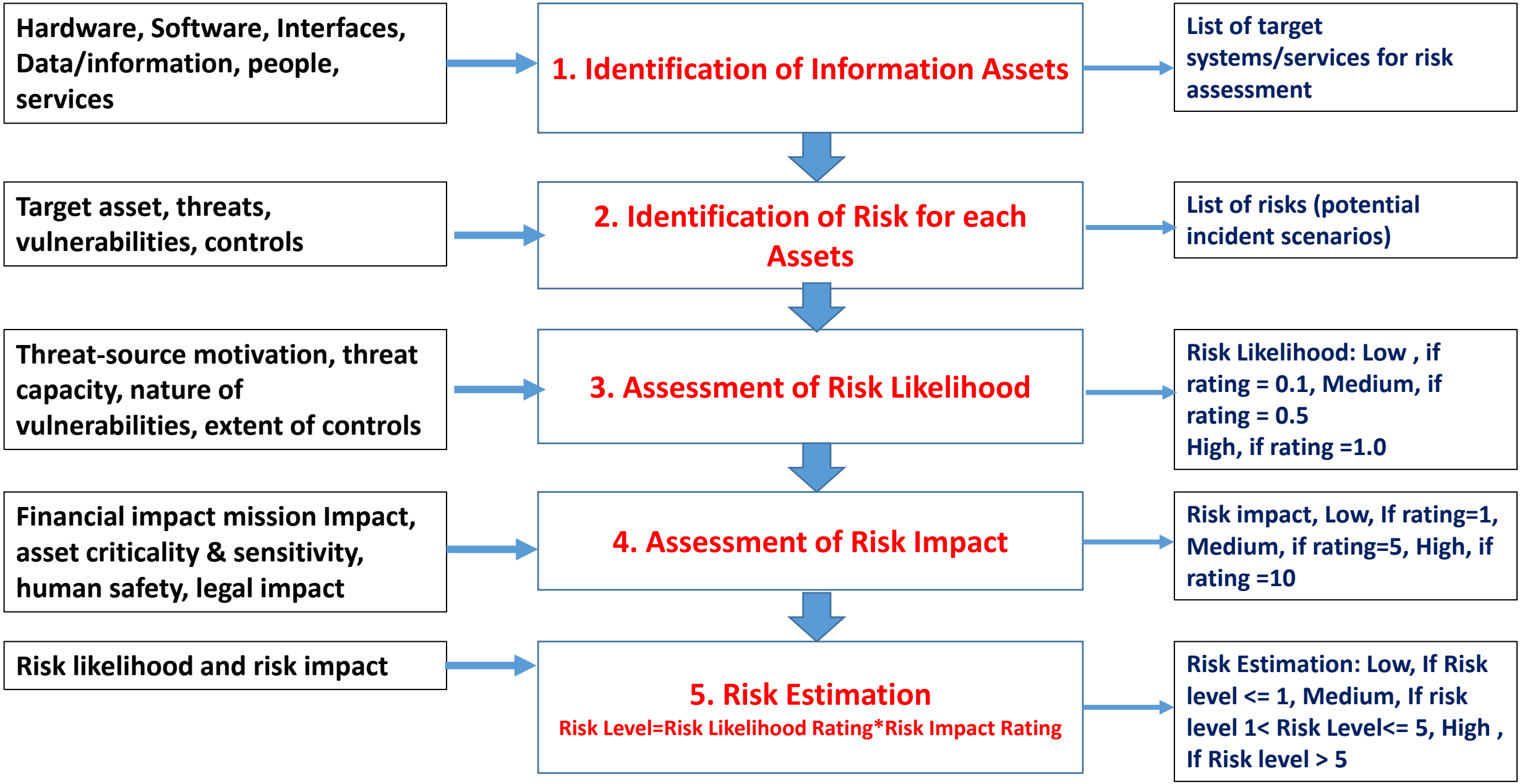
RISK AND RISK ASSESSMENT

- **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.

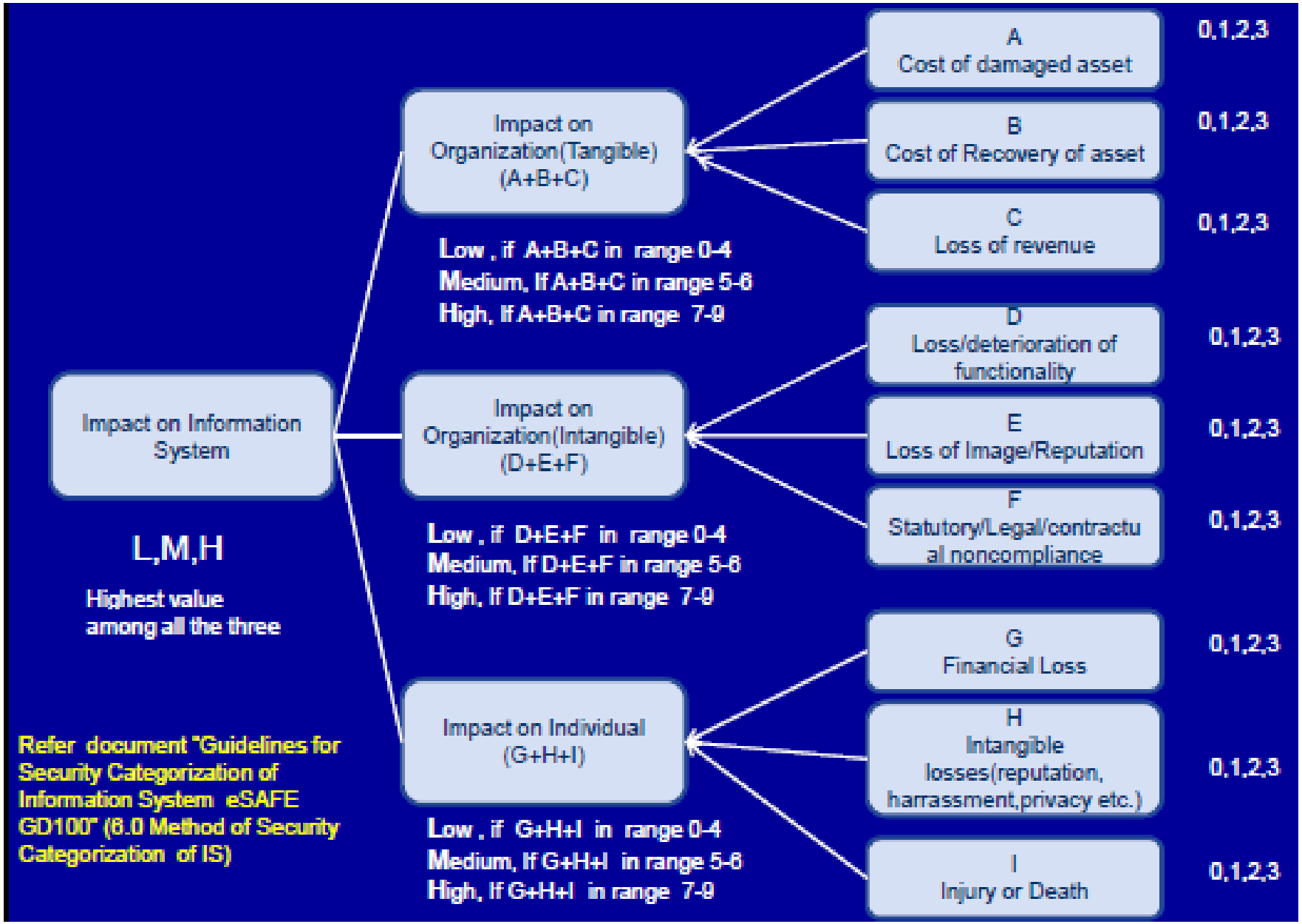
RISK LEVELS

RISK LEVEL	RISK DESCRIPTION
HIGH RISK	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	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	Risk is acceptable and no other control or control improvements are required.

RISK LEVEL ASSESSMENT STEPS

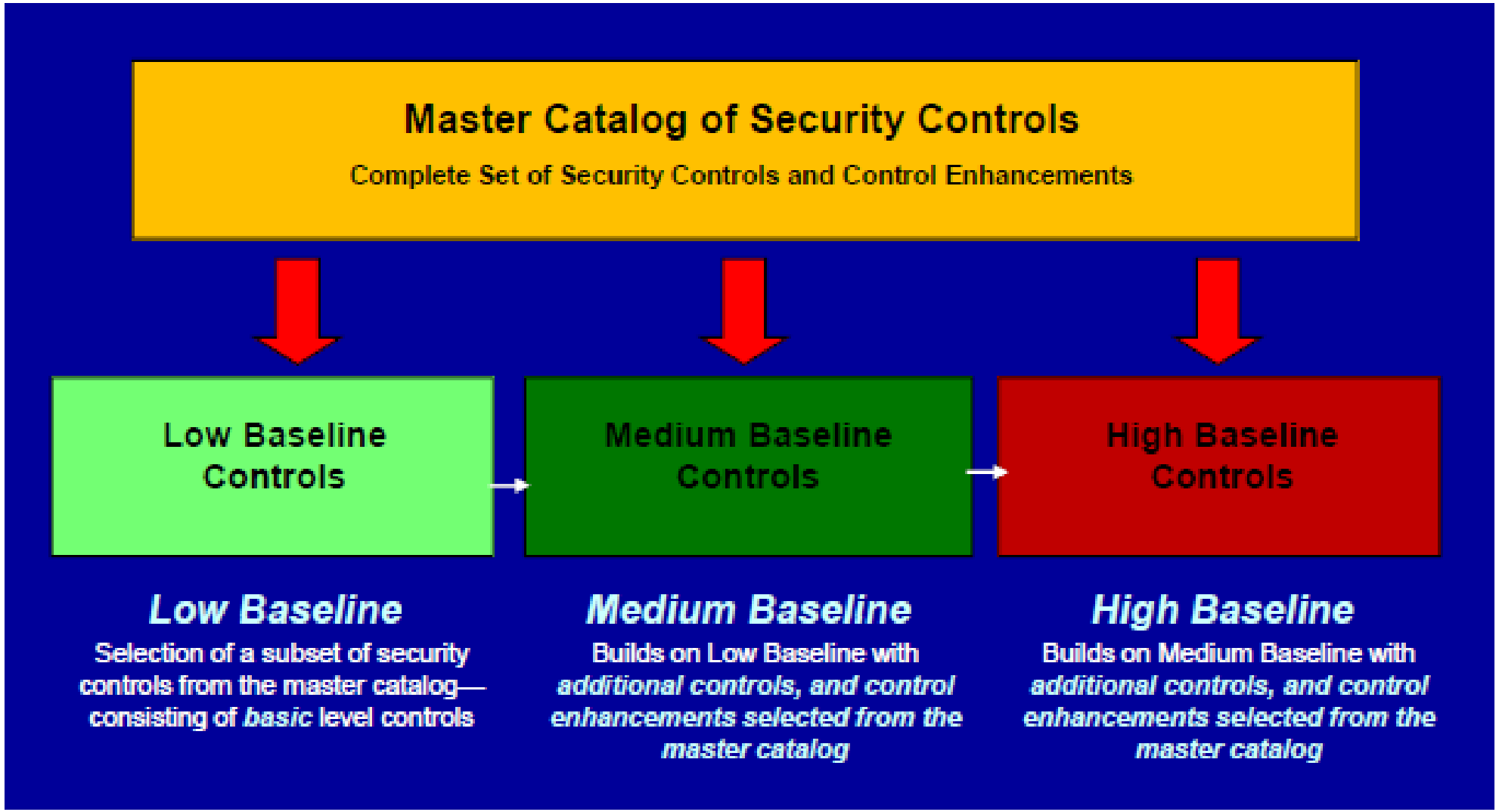


METHOD OF SECURITY CATEGORIZATION OF INFORMATION SYSTEMS

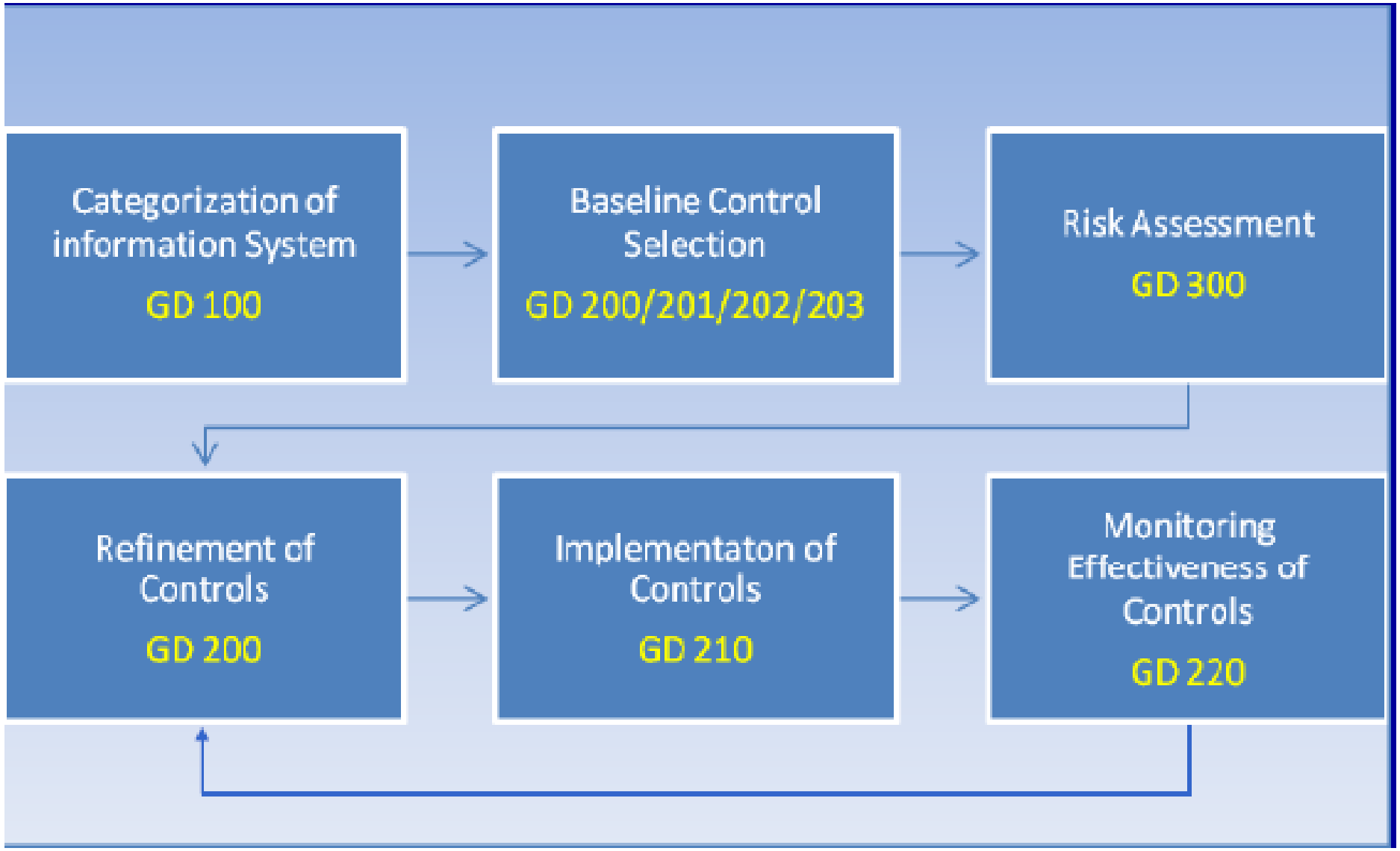


RATINGS

SECURITY CONTROL BASELINES



Documents under e-Governance Security Assurance Framework (eSAFE)



OTHER IMPORTANT DOCUMENTS

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: Catalogue 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	

OTHER IMPORTANT DOCUMENTS

TITLE OF DOCUMENT	SCOPE OF DOCUMENT	TARGET AUDIENCE
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. 15th Jan 2010	1. Concerned managers and Employees for information security risk assessment management within an organization 2. Third party service provider supporting such activities.
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.	

OTHER IMPORTANT DOCUMENTS

TITLE OF DOCUMENT	SCOPE OF DOCUMENT	TARGET AUDIENCE
eSAFE-GD210: Guidelines for Implementation of Security Control	Under preparation	1. Concerned managers and Employees for information security risk assessment management within an organization 2. Third party service provider supporting such activities.
eSAFE-GD220: Guidelines for Assessment of effectiveness of security controls	Under preparation	

LIST OF DOCUMENTS UNDER E-GOVERNANCE SECURITY FRAMEWORK

CODE	TITLE
ISF 01	Information Security Assessment Framework
GD 100	Guidelines for Information System Categorization
GD 200	Catalogue 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

GUIDELINES FOR SECURITY CATEGORIZATION OF INFORMATION SYSTEMS

(TO BE FINALIZED BY)

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 other documents is given in the next slide.

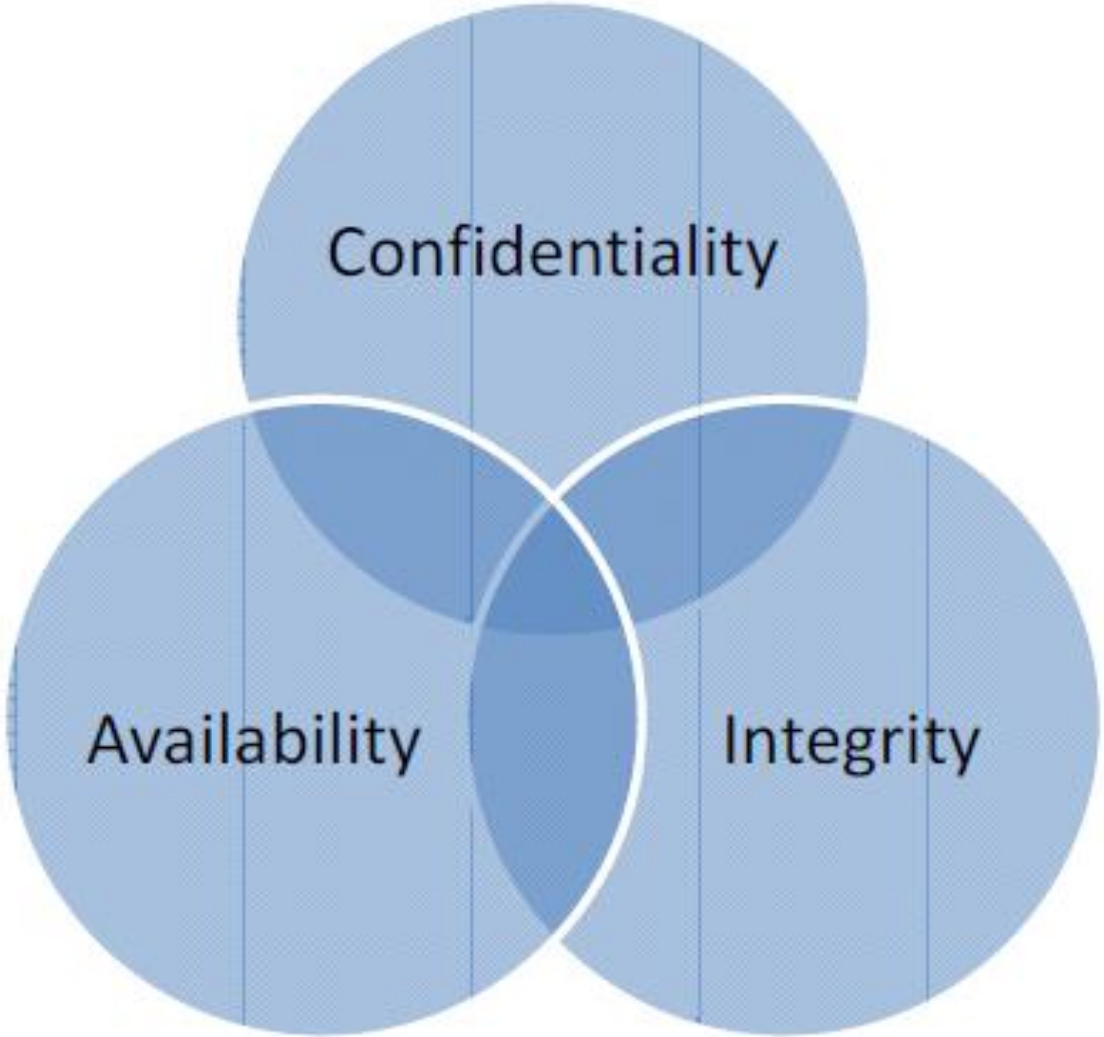
List of the documents identified in the eGovernance Security Assurance Framework (eSAFE).

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

CATEGORIZATION OF 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, 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.

INFORMATION SECURITY ATTRIBUTES



POTENTIAL IMPACT

- **LOW IMPACT:** The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on the organization and individuals.

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

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

METHOD OF SECURITY CATEGORIZATION FOR INFORMATION SYSTEMS

Impact on Organization (Tangible)

- Cost of damaged assets
- Cost of recovery
- Loss of revenue

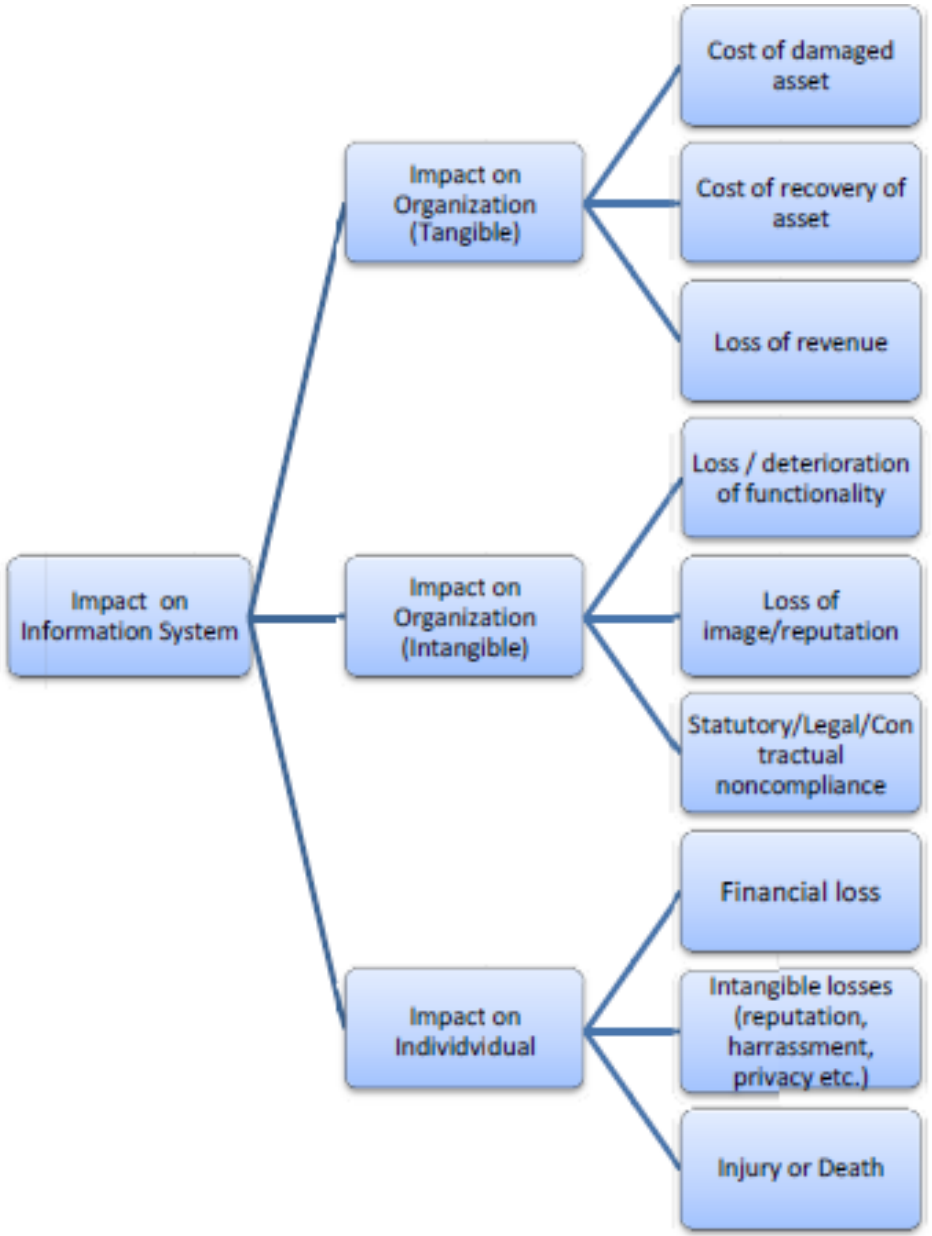
Impact on Organization (Intangible)

- Loss/deterioration of functionality
- Loss of image/reputation
- Statutory/Legal/Contractual noncompliance

Impact on Individuals

- Financial loss
- Intangible loss
- Injury or Death

METHOD OF SECURITY CATEGORIZATION FOR INFORMATION SYSTEMS



QUANTIFICATION OF THE IMPACT – CATEGORY WISE

MAJOR CATEGORY	MINOR CATEGORY	POINTS TO BE AWARDED IF THE IMPACT IS			
		NIL	LOW	MEDIUM	HIGH
Impact on Organization (Tangible)	Cost of damaged assets	0	1	2	3
	Cost of recovery	0	1	2	3
	Loss of revenue	0	1	2	3
Impact on Organization (Intangible)	Loss/deterioration of functionality	0	1	2	3
	Loss of image/reputation	0	1	2	3
	Statutory/Legal/Contractual noncompliance	0	1	2	3
Impact on Individuals	Financial loss	0	1	2	3
	Intangible loss	0	1	2	3
	Injury or Death	0	1	2	3

TOTAL IMPACT MATRIX

TOTAL SCORE	IMPACT
0 - 3	LOW
4 - 6	MEDIUM
7 - 9	HIGH

OVER ALL IMPACT ON INFORMATION SYSTEM MATRIX - 1

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
HIGH	HIGH	HIGH	HIGH

OVER ALL IMPACT ON INFORMATION SYSTEM MATRIX - 2

Impact on Organization (Tangible)	Impact on Organization (Intangible)	Impact on Individual	Overall Impact on Information System
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

OVER ALL IMPACT ON INFORMATION SYSTEM MATRIX - 3

Impact on Organization (Tangible)	Impact on Organization (Intangible)	Impact on Individual	Overall Impact on Information System
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

THANKS