****

Risk Assessment and Treatment Procedure

**Version History:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 29th Aug 2013 | First Draft | Rahul Raj | Saket Madan | Dhananjay Kumar |
| 1.0 | 30th Sep 2013 | Approved and Baselined | Rahul Raj | Dhananjay Kumar | Ajay Kumar Zalpuri |
| 1.1 | 29th July 2015 | Update Clause 6.1 included for Business process & Operation process. Update in section 6.9 Risk Treatment Plan for project duration for risk mitigation | Rahul raj | Dhananjay Kumar | Ajay Kumar Zalpuri |
| 2.0 | 16th May 2016 | Update section 4, 5, 6, 6.2, 6.3, 6.9 & 6.10 | Rahul Raj | SEPG Team | Ajay kumar Zalpuri |
| 2.1 | 29th Nov 2018 | Update section 6.8 | Rahul Raj | SEPG Team | Ajay kumar Zalpuri |

**Table of Contents**

[1. Introduction 4](#_Toc372545624)

[2. Scope 4](#_Toc372545625)

[3. Terms & Definitions 4](#_Toc372545626)

[4. Entry Criteria 4](#_Toc372545627)

[5. Inputs 4](#_Toc372545628)

[6. Process 4](#_Toc372545629)

[6.1 Identification of assets 5](#_Toc372545630)

[6.2 Acceptable Use of Assets 6](#_Toc372545631)

[6.3 Asset valuation 6](#_Toc372545632)

[6.4 Identification of Threats 6](#_Toc372545633)

[6.5 Threat Probability Valuation 6](#_Toc372545634)

[6.6 Identification of vulnerabilities 7](#_Toc372545635)

[6.7 Vulnerability Impact Valuation 7](#_Toc372545636)

[6.8 Risk Register 7](#_Toc372545637)

[6.9 Risk Treatment Plan 7](#_Toc372545638)

[6.10 Monitoring and Control 8](#_Toc372545639)

[7. Outputs 8](#_Toc372545640)

[8. Exit Criteria 8](#_Toc372545641)

[Annexure-I 10](#_Toc372545642)

[Examples of Threats 10](#_Toc372545643)

[Annexure-II 11](#_Toc372545644)

[Examples of Vulnerabilities 11](#_Toc372545645)

# Introduction

The Risk Assessment and Treatment procedure lays the guidelines for:

1. Identifying threats and vulnerabilities associated with organizational assets.
2. Assessing the risk and its impact on the business.
3. Assess project level Risks
4. Providing a quantitative rating for the risk based on the assessment.
5. Planning and implementing appropriate mitigation steps to prevent, eliminate, transfer or minimize the identified risks.

# Scope

This procedure is applicable to NST.

# Terms & Definitions

Owner: Identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ‘owner’ does not mean that the person actually has any property rights to the asset.

# Entry Criteria

1. New asset has been identified
2. New threat has been identified for an existing asset
3. Residual Risk value is to be calculated
4. Initiation of a new project

# Inputs

1. Asset and its type
2. Project Risks
3. Threat
4. Vulnerability
5. Impact based on C, I, A value

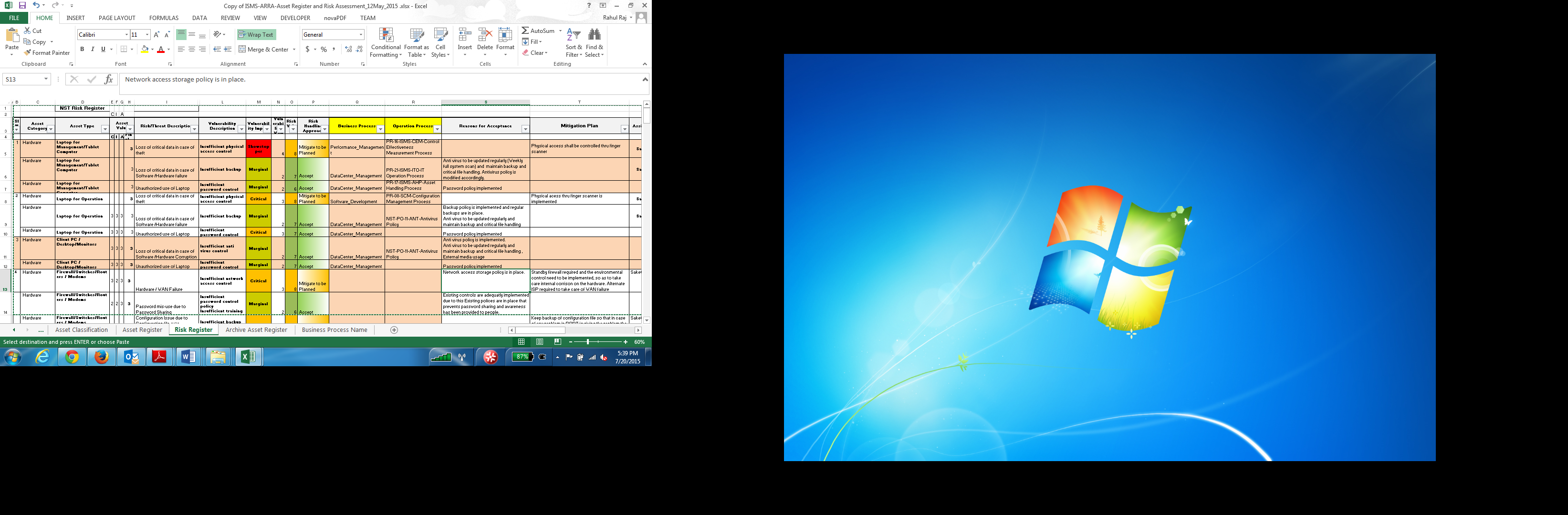
# Process

Risk Assessment and Treatment procedure involves the following steps:

1. Identification of assets
2. Identification of project Risks
3. Asset/Risk valuation
4. Identification of threats
5. Threat Valuation
6. Identification of vulnerabilities
7. Vulnerability valuation
8. Risk Assessment and preparation of Risk Assessment Sheet
9. Preparation of Risk Treatment Plan

# Identification of assets

All departments will create Asset groups and classify their assets according to these groups on the basis of Business Process and its Operational process. This classification will be maintained in the Asset Register. Assets related to legal and regulatory requirements will be identified in Asset Register. A sample entry in the Asset Register is provided below for reference.

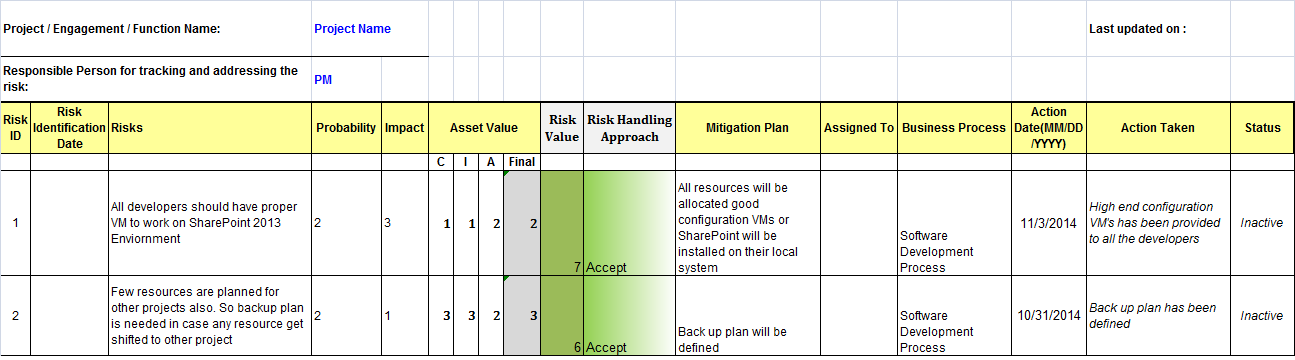


# Acceptable Use of Assets

Rules for acceptable use of information and assets are identified, documented and implemented, for example, printers are not allowed in Data Centre, back up media tapes will be handled as per Information Back up policy, no unlicensed software will be used etc.

# Identification of project Risks

The project manager will identify the risks in the project triggering from various sources like scope, resource, schedule etc. The risks would be maintained in the project risk register (template TP-35-RIR-Risk Register)



# Asset/Risk valuation

Asset/Risk valuation is done in terms of the business impact and which is considered in terms of the following criteria:

1. **Confidentiality**: Business impact that could occur due to leakage of information.
2. **Integrity**: Business impact that could occur if the information asset is corrupted or altered.
3. **Availability**: Business impact that could occur due to loss or unavailability of asset.

Asset/Risk valuation involves determining asset/Risk values for all the identified asset groups as per C/I/A Guidelines. Each asset/Risk will have a C value, I value and an A value. Asset/Risk value will be a function of all of these 3 values and will be calculated using the following formula:

**Asset/Risk Value =** maximum (C, I, A)

**CIA guidelines** for each asset group have been identified and are available in ‘GD-20-ISMS-CIA-Confidentiality Integrity Availability Guidelines’ document.

# Identification of Threats

This step involves identifying all applicable threats, which may result in impact on business. These threats have to be identified for each asset/Risk and documented in the Risk Assessment sheet.

Examples of some threats are listed in Annexure-I.

# Threat Probability Valuation

Each threat identified above has to be evaluated. Threat valuation is based on the probability of occurrence of the threat derived from historical information. For example, the threat valuation for flooding of server room will be based on the number of similar incidents that have occurred in the past.

|  |  |  |
| --- | --- | --- |
| **Threat Probability Rating** | |  |
| **Score** | **Rating** | **Description** |
| 5 | Near certainty | Event that has a greater than 75% chance of occurring |
| 4 | Highly likely | Event that has between a 51 – 75% chance of occurring |
| 3 | Likely | Event that has between a 20 – 50% chance of occurring |
| 2 | Unlikely | Event that has between a 10 – 20% chance of occurring |
| 1 | Remote | Event that has a 0 – 10% chance of occurring |

This value is to be documented in Risk Register.

# Identification of vulnerabilities

Vulnerability is the lack of appropriate controls or safeguards that would prevent a risk from occurring. Put in other words, vulnerability dictates the Impact of the occurrence of a risk.

This step involves identification of vulnerabilities associated with each threat. These have to be identified for each asset and documented in the Risk Assessment sheet.

Examples of a few vulnerabilities are listed in Annexure-II.

# Vulnerability Impact Valuation

Each vulnerability has been identified above has to be evaluated. This evaluation is to be done on a 1-3 scale as per following table:

|  |  |  |
| --- | --- | --- |
| **Vulnerability Impact Rating** | | |
| **Score** | **Rating** | **Description** | |
| 4 | Showstopper | The effect is catastrophic; the organization may face significant loss and impact. The project will fail. | |
| 3 | Critical | The impact is serious, and the project may be largely affected due to the risk. There could be huge delays and the project could be postponed due to it. | |
| 2 | Marginal | The risks could affect in small delays in schedule. | |
| 1 | Negligible | The impact of these risks on the project could be minimal. | |

The value is to be documented in the Risk Register.

# Risk Register

Once threats and vulnerabilities have been identified, risk value is to be assigned for each combination of threat and vulnerability and is to be reflected in Risk Assessment sheet.

Risk value is a function of Asset value and Vulnerability value and can be calculated by using following formula:

**Risk Value = (probability of event) + (impact of event) + (CIA Value)**

# Risk Treatment Plan

Risk Treatment plan will be prepared based on the risk value for each identified risk. The following guidelines will be applied:

|  |  |
| --- | --- |
| **Risk Value** | **Risk Treatment Strategy** |
| **3-5** | No action is required. |
| **6 to 7** | To be reviewed regularly and Organization will accept risk up to this level. |
| **8 to 10** | Medium level risk, mitigation to be planned in a period of six months. But in case of project, period may be vary on the basis of project duration |
| **11 to 12** | High Level risk, Mitigation immediately required and escalated to the Security Council for further action. |

One of the following actions shall be taken for the treatment of risks:

1. **Mitigating the risks:** Appropriate controls shall be identified to reduce the vulnerability and therefore reduce the risk value.
2. **Avoiding the risks:** Avoid the risk by preventing certain conditions from occurring.
3. **Transferring the risks:** Where possible, transfer the risk to third parties such as insurance companies, suppliers etc.
4. **Accepting the risks:**

* The risks which have risk value 5 are accepted without any approval. No action is required on them.
* For risks which cannot be reduced, transferred or avoided due to cost or other constraints, it will be explicitly mentioned that we choose to accept the risk with approval from the Security Council.

# Monitoring and Control

The Risk Register will be visited periodically by each department and assessed for any new risk or change in asset value or vulnerability value for existing risks. To assess whether change has occurred in asset value or vulnerability value, refer to ‘GD-20-ISMS-CIA-Confidentiality Integrity Availability Guidelines’ and ‘**Effectiveness of Controls**’ documents. Risk Value will be calculated accordingly. This may cause risk treatment plan to change.

Risk Assessment will also be carried out periodically every 3 months.

# Outputs

1. Updated Risk Register

# Exit Criteria

1. Risk Treatment Plan has been decided.

# Annexure-I

## Examples of Threats

* Air conditioning failure
* Bomb attack
* Communications infiltration
* Damage to communication lines/cables
* Deterioration of storage media
* Earthquake
* Eavesdropping
* Environmental contamination (and other forms of natural or man-made disasters)
* Extremes of temperature and humidity
* Failure of communications services
* Failure of network components
* Failure of power supply
* Failure of water supply
* Fire
* Flooding
* Hardware failure
* Illegal import/export of software
* Illegal use of software
* Industrial action
* Lightning
* Maintenance error
* Malicious software (e.g. viruses, worms, Trojan Horses)
* Masquerading of user identity
* Misrouting or rerouting of messages
* Misuse of resources
* Network access by unauthorized persons
* Operational support staff error
* Power fluctuation
* Repudiation (e.g. of services, transactions, sending/receiving messages)
* Software failure
* Staff shortage
* Theft
* Traffic overloading
* Transmission errors
* Unauthorized use of software
* Unauthorized use of storage media
* Use of network facilities in an unauthorized way
* Use of software by unauthorized users
* Use of software in an unauthorized way
* User Error

## Annexure-II

## Examples of Vulnerabilities

* Absence of personnel
* Dial-up lines
* Disposal or reuse of storage media without proper erasure
* Inadequate network management
* Inadequate or careless use of physical access control to buildings, rooms and offices
* Inadequate recruitment procedures
* Insufficient maintenance/faulty installation of storage media
* Insufficient security training
* Lack of audit-trail
* Lack of care at disposal
* Lack of documentation
* Lack of effective change control
* Lack of identification and authentication mechanisms
* Lack of monitoring mechanisms
* Lack of periodic equipment replacement schemes
* Lack of physical protection for the building, doors, and windows
* Lack of policies for the correct use of telecommunications media and messaging
* Lack of security awareness
* Location in an area susceptible to flood
* Location in an area susceptible to earthquake
* Lack of inbuilt locking mechanism in machines
* No or insufficient software testing
* Poor joint cabling
* Poor password management
* Poorly documented software
* Single point of failure
* Susceptibility of equipment to humidity, dust, soiling or temperature variations or voltage variations
* Transfer of passwords in clear text
* Unclear or incomplete specifications for developers
* Uncontrolled copying

#### Uncontrolled downloading and using software

* Unprotected communication lines
* Unprotected public network connections.
* Unprotected storage of sensitive data/information.
* Unstable power grid.
* Unsupervised work by outside or cleaning staff
* Well-known flaws in the software.
* Wrong allocation of access rights.
* Lack of procedure for invoking access permissions.
* Not revoking access permissions when an employee leaves organization or project is changed
* Non-maintenance of cupboards, drawers or equipment’s