


# Risk Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-IT-IS-14

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

i. Document Identification

<b>Document Title and Version:</b>	<b>PR-IT-IS-14 Risk Management Procedure v1.0</b>
Effective Date:	1 <sup>st</sup> October, 2019
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO

Head Of IT

v. Revision History

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Rev	Date	Author	Description	Approved By	Initiated Date
0	01-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Information Security Team	Approval	Andy Chong	17-12-2019
2	12-08-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	09-10-2023	Information Security Team	This document will be retired as it will be succeeded by ERM procedure	Rajesh Lal Nyachhyon	04-12-2023
5	04-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	04-12-2023
6	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Table of Contents

<b>Document Control</b> .....	<b>1</b>
<b>1. Purpose</b> .....	<b>5</b>
<b>2. Review and Updating</b> .....	<b>5</b>
<b>3. Risk Management Hierarchy</b> .....	<b>5</b>
<b>4. Risk Assessment Process</b> .....	<b>6</b>
4.1 Preparing for the Risk Assessment Process .....	6
4.2 Conducting the Risk Assessment .....	7
4.3 Calculating Risk Score .....	8
4.3.1 Determining critical assets .....	8
4.3.2 Determining control rating .....	8
4.3.3 Determining impact and likelihood .....	9
4.3.4 Calculate risk value and risk rating .....	10
4.4 Communicate Risk Assessment Results .....	10
4.5 Maintaining the Risk Assessment .....	10
<b>5. Risk Management Process</b> .....	<b>11</b>
5.1 Perform risk evaluation and prioritization .....	11
5.1.1 Risk Acceptance Criteria .....	11
5.2 Develop Risk Treatment Plan (RTP) .....	11
5.3 Perform Residual Risk Analysis .....	11
<b>6. Site Risk Assessment Methodology</b> .....	<b>12</b>
6.1 Site Risk Assessment Steps .....	12
6.2 Risk Treatment Plan .....	13
<b>7. Governance and Compliance</b> .....	<b>13</b>
<b>8. Associated Documents</b> .....	<b>13</b>

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 1. Purpose

The purpose of this document is to standardize the risk assessment and management approach across Ncell. The NIST cyber security framework has put all the cyber security issues in the context of the risk they represent and advises implementers to plan mitigation based on the impact. This not only helps to prioritize and budget but also structures the approach and helps in creating milestone based mitigation plans. In this document we are going to standardize the way risk assessments are carried out and identified risks are managed by Ncell.

## 2. Review and Updating

This procedure shall be reviewed once every two years or whenever significant changes occur in the organization.

## 3. Risk Management Hierarchy

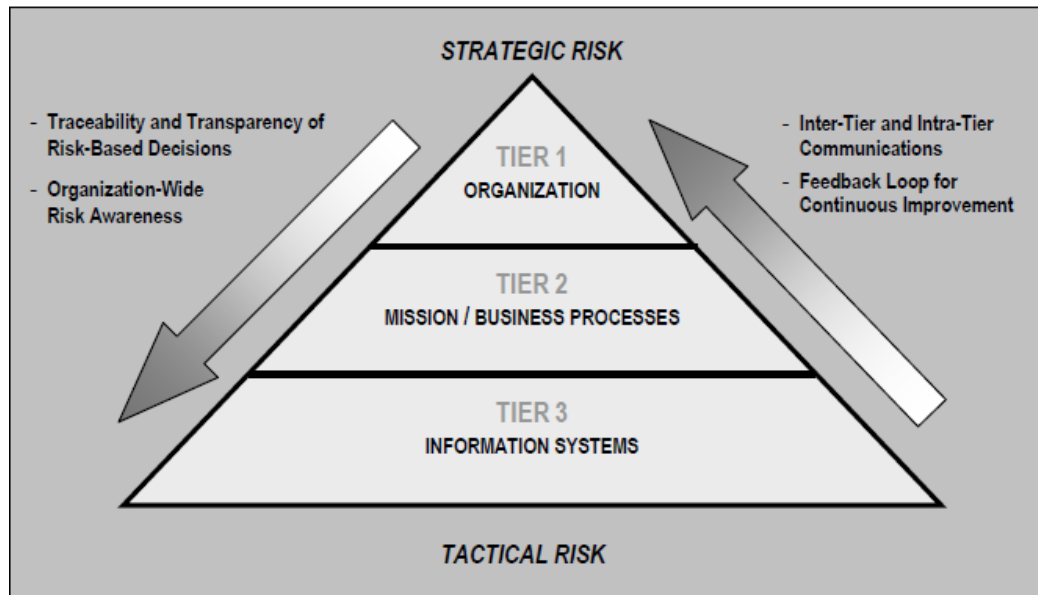


Figure 1: Risk Management Hierarchy

Risk assessments support risk response decisions at the different tiers of the risk management hierarchy.

At Tier 1, risk assessments can affect, for example:

- Organization-wide information security programs, policies, procedures, and guidance;
- The types of appropriate risk responses (i.e., risk acceptance, avoidance, mitigation, sharing, or transfer);
- Investment decisions for information technologies/systems;
- Procurements;
- Minimum organization-wide security controls;
- Conformance to enterprise/security architectures; and
- Monitoring strategies and ongoing authorizations of information systems and common controls.

At Tier 2, risk assessments can affect, for example:

- Enterprise architecture/security architecture design decisions;
- The selection of common controls;
- The selection of suppliers, services, and contractors to support organizational missions/business functions;
- The development of risk-aware mission/business processes; and

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

v. The interpretation of information security policies with respect to organizational information systems and environments in which those systems operate.

Finally, at Tier 3, risk assessments can affect, for example:

- Design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems);
- Implementation decisions (including whether specific information technology products or product configurations meet security control requirements); and
- Operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

## 4. Risk Assessment Process

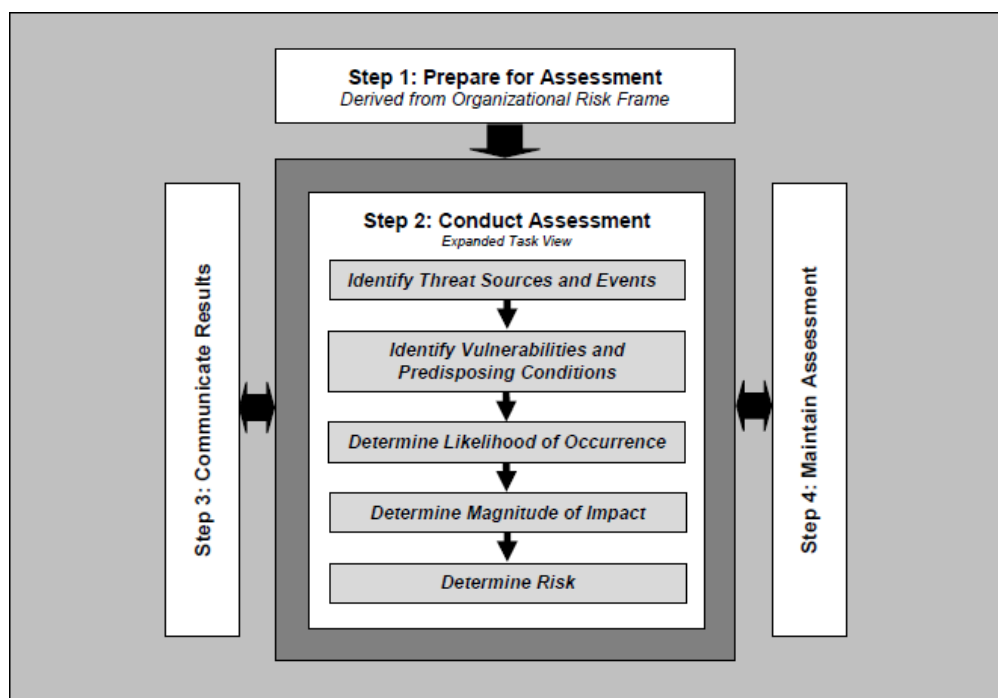


Figure 2: Risk Assessment Process

### 4.1 Preparing for the Risk Assessment Process

The objective of this step is to establish a context for the risk assessment. This context is established and informed by the results from the risk framing step of the risk management process. Organizations use the risk management strategy to the extent practicable to obtain information to prepare for the risk assessment. Preparing for a risk assessment includes the following tasks:

- Identify the purpose of the assessment;
- Identify the scope of the assessment;
- Identify the assumptions and constraints associated with the assessment;
- Identify the sources of information to be used as inputs to the assessment; and
- Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

Ncell shall perform the following tasks in this step:

- Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.
- Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations. The scope should include the following:

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- a. **Organizational Applicability** - Organizational applicability describes which part of the organization or sub-organizations are affected by the risk assessment and the risk-based decisions resulting from the assessment (including the parts of the organization or sub-organizations responsible for implementing the activities and tasks related to the decisions).
  - b. **Effectiveness Time Frame** - Organizations determine how long the results of particular risk assessments can be used to legitimately inform risk- based decisions. The time frame is usually related to the purpose of the assessment
  - c. **Architectural/Technology Considerations** - Organizations use architectural and technology considerations to clarify the scope of the risk assessment
- iii. Identify the specific assumptions and constraints under which the risk assessment is conducted. The following sections provide some representative examples of areas where assumptions/constraints for risk Assessments may be identified:
- a. **Threat Sources** - Ncell determine which types of threat sources are to be considered during risk assessments.
  - b. **Threat Events** - Organizations determine which type of threat events are to be considered during risk assessments and the level of detail needed to describe such events.
  - c. **Vulnerabilities and Predisposing Conditions** - Organizations determine the types of vulnerabilities that are to be considered during risk assessments and the level of detail provided in the vulnerability descriptions.
  - d. **Likelihood** - Organizations make explicit the process used to conduct likelihood determinations and any assumptions related to the likelihood determination process.
  - e. **Impacts** - Organizations determine potential adverse impacts in terms of organizational operations (i.e., missions, functions, image, and reputation), organizational assets, individuals, other organizations.
  - f. **Risk Tolerance and Uncertainty** - Organizations determine the levels and types of risk that are acceptable.
  - g. **Analytic Approach** - Risk assessments include both assessment approaches (i.e., quantitative, qualitative, semi-quantitative) and analysis approaches (i.e., threat-oriented, asset/impact-oriented, vulnerability-oriented)
- iv. Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
- v. Identify the risk model and analytic approach to be used in the risk assessment.

## 4.2 Conducting the Risk Assessment

The second step in the risk assessment process is to conduct the assessment. The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. Conducting risk assessments includes the following specific tasks:

- Identify threat sources that are relevant to organizations;
- Identify threat events that could be produced by those sources;
- Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

Ncell shall conduct a quantitative risk assessment with an asset/impact oriented analysis approach. The Unit Head shall conduct the risk assessment for each function identified in the asset registers. It shall perform the following tasks while conducting Risk Assessments:



<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- i. Identify critical assets.
- ii. Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats
- iii. Identify potential threat events, relevance of the events, and the threat sources that could initiate the events
- iv. Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts
- v. Determine the likelihood that threat events of concern result in adverse impacts, considering:
  - a. The characteristics of the threat sources that could initiate the events;
  - b. The vulnerabilities/predisposing conditions identified; and
  - c. The organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
- vi. Determine the adverse impacts from threat events of concern considering:
  - a. The characteristics of the threat sources that could initiate the events;
  - b. The vulnerabilities/predisposing conditions identified; and
  - c. The susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events
- vii. Determine the risk to the organization from threat events of concern considering:
  - a. The impact that would result from the events; and
  - b. The likelihood of the events occurring

### 4.3 Calculating Risk Score

#### 4.3.1 Determining critical assets

- i. The risk assessment exercise shall be performed for all critical assets.
- ii. Asset Criticality shall be as defined in the Asset Management Procedure<sup>1</sup>

#### 4.3.2 Determining control rating

- i. Identify preventive and detective controls implemented in the organisation against the identified threats and vulnerabilities.
- ii. Determine control rating of the applicable cumulative controls.

Applicable Control rating	
<b>0 – Un-Identification of Issue</b>	Organization has not recognized the existence of issue. No processes exist. No action taken to address the issue
<b>1 - Initial</b>	Organization recognized the existence of issue and need for its addressal. No standardized processes exist. However, only ad hoc approaches has been applied for issue addressal
<b>2 - Repeatable but not defined</b>	Control/ Processes have developed to the stage where similar procedures/ controls are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is high degree of reliance on the knowledge of individuals and therefore, errors are likely
<b>3 - Defined Process</b>	Procedures/ control implementation have been standardised and documented and communicated through training. It is mandated that these processes/ controls should be followed. Procedures themselves are not sophisticated but are the formalization of existing practices
<b>4 - Managed and Measurable</b>	Management monitors/ measures compliance with controls and take action where processes appear not to be working effectively. Control implementation are under constant improvement and provide good practice

<sup>1</sup> PR-IT-IS-02 Asset Management Procedure

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

<b>5- Optimized</b>	Processes Supporting this control have been refined to a level of good practice, based on the result of continual improvement.
---------------------	--

#### 4.3.3 Determining impact and likelihood

- Map all applicable threats-vulnerability pairs against the identified grouped assets;
- Derive the impact of the threat-vulnerability pair after taking into consideration existing controls as per the formula;
- Impact due to cumulative controls = (Asset Criticality Rating – Applicable Control Rating);

Impact due to cumulative controls	
Rating Scale	Formula
1-Insignificant	(Asset Criticality Rating- Applicable Control Rating) <=1
2-Minor	(Asset Criticality Rating- Applicable Control Rating) >1 and (Asset Criticality Rating- Applicable Control Rating) <=2
3-Moderate	(Asset Criticality Rating- Applicable Control Rating) >2 and (Asset Criticality Rating- Applicable Control Rating) <=3
4-Major	(Asset Criticality Rating- Applicable Control Rating) >3 and (Asset Criticality Rating- Applicable Control Rating) <=4
5-Catastrophic	(Asset Criticality Rating- Applicable Control Rating) >4

- Determine the likelihood of occurrence of the threat as per past history.

Likelihood of threat as per past occurrence					
	1-Rare	2-Unlikely	3-Moderate	4-Likely	5-Almost Certain
<b>General Description</b>	Event may occur in exceptional circumstances only	Expected to occur less frequently	Event might occur at some time	Event has happened before and will probably occur again	Event is common and is expected to occur in most circumstances
<b>Estimated Frequency</b>	Once every 5 years	Once every 3 years	At least once in the next 12 months	Several times in a year	At least monthly
<b>Estimated Probability</b>	< 10%	10% < 25%	25% < 50%	50% < 75%	≥ 75%

- Preventive controls reduce the likelihood of occurrence of the threat. Hence, determine the overall likelihood of the threat taking into consideration the existing preventive controls in place to mitigate the impact due to occurrence of the threat as per the formula;
- Overall likelihood considering preventive controls = (Likelihood of threat as per past occurrence – Applicable Control Rating of the Preventive Control);

Overall Likelihood Considering Preventive Controls	
Rating Scale	Formula
1-Rare	(Likelihood of threat as per past occurrence- Applicable Control Rating of the Preventive Control) <=1
2-Unlikely	(Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) >1 and (Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) <=2

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

3-Moderate	(Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) >2 and (Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) <=3
4-Likely	(Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) >3 and (Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) <=4
5-Almost Certain	(Likelihood of threat as per past occurrence - Applicable Control Rating of the Preventive Control) >4

#### 4.3.4 Calculate risk value and risk rating

- Calculate the Risk Value as per the following formula: Risk value = (Impact due to cumulative controls \* Overall Likelihood considering preventive controls);
- Based on the Risk Value, a Risk Rating shall be assigned as per the following guidelines:

Risk Rating	Formula	What it Means
5-Extreme	Risk Value >20	<ul style="list-style-type: none"> <li>Board attention is required</li> <li>Immediate action by senior management with a detailed research and management risk treatment plan</li> </ul>
4-Significant	Risk Value >15 and Risk Value <=20	<ul style="list-style-type: none"> <li>Board attention is required</li> <li>Senior management responsibility specified</li> <li>Risk must be managed by senior management with a detailed risk treatment plan</li> </ul>
3-High	Risk Value >10 and Risk Value <=15	<ul style="list-style-type: none"> <li>Senior management attention required</li> <li>Management responsibility specified</li> <li>Risks should be treated using one or more of the risk treatment options</li> </ul>
2-Moderate	Risk Value >5 and Risk Value <=10	<ul style="list-style-type: none"> <li>Management attention required</li> <li>Management responsibility specified</li> <li>Risks should be treated using one or more of the risk treatment options</li> </ul>
1-Low	Risk Value >=1 and Risk Value <=5	<ul style="list-style-type: none"> <li>Risk is accepted with minimal treatment and can normally be managed using existing routine procedures</li> <li>Low risks need to be monitored and periodically reviewed to ensure they remain acceptable</li> </ul>


#### 4.4 Communicate Risk Assessment Results

The third step in the risk assessment process is to communicate the assessment results and share risk-related information. The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions. Ncell shall perform the following tasks:

- Communicate risk assessment results to Ncell decision makers and management to support risk responses.
- Share risk-related information produced during the risk assessment with appropriate organizational personnel.

#### 4.5 Maintaining the Risk Assessment

- Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations.
- Update existing risk assessment using the results from ongoing monitoring of risk factors.

	Ncell	Classification: Internal
	Risk Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 5. Risk Management Process

### 5.1 Perform risk evaluation and prioritization

- Risk evaluation is about deciding whether risks are acceptable or unacceptable. The evaluation should take account of the degree of control over each risk and the cost impact, benefits and opportunities presented by the risks. The significance of the risk, and the importance of the policy, program, process or activity, need to be considered in deciding if a risk is acceptable.
- A risk may be accepted if the consequence and likelihood of that risk is consistent with the established criteria.

#### 5.1.1 Risk Acceptance Criteria

Risk Acceptance Threshold for Ncell shall be defined as (Risk Rating = 1-Low) or (Risk Value  $\geq 1$  and Risk Value  $\leq 5$ ). Risk Status of all such risks shall be classified as 'No Action'.

### 5.2 Develop Risk Treatment Plan (RTP)


This phase involves dealing with risks determined as being unacceptable to Ncell at the existing level.

- For all risks which exceed the Risk Acceptance threshold, management can select the following appropriate information security risk treatment options:
  - Avoid:** Deciding not to start or stop the activity that gives rise to the risk;
  - Remove:** Eliminating the risk source.
  - Take:** Taking or increasing the risk to pursue an opportunity;
  - Mitigate:** Limiting the impact of a risk so that if a problem occurs it will be easier to fix.
  - Share:** Sharing the risk with others (E.g.: contracts, risk finance, etc.);
- An organization wide Risk Treatment plan shall be prepared for all risks where the Risk Rating is either '5-Extreme' or '4-Significant' or '3-High' or '2-Moderate'. As part of the treatment plan, the following key details shall be captured at minimum –
  - Gaps identified.**
  - Mitigation Plan**
  - Risk Owner**
  - Closure Responsibility**
  - Estimated Closure Date**
  - Management Decision**
  - Justification (in case of risk acceptance by management)**
  - Closure Status**
- Wherever applicable and appropriate, inputs shall be obtained from the Vulnerability Assessment and Penetration testing reports for mitigation plans against the identified risks.

### 5.3 Perform Residual Risk Analysis

This phase involves determining whether the controls selected for mitigation of risks are effective in reducing the risk to an acceptable value. For all risks against which the mitigation plan has been implemented, the following steps shall be performed to determine the residual risk:

- Calculate 'Control rating after mitigation plan implementation': The score of the controls implemented by the organization for mitigation of the identified risk shall be updated in accordance with the established rating criteria;
- Estimate residual impact and likelihood: Derive the residual impact of the threat-vulnerability pair after taking into consideration the implemented control as per the formula – Residual Impact = (Asset Criticality Rating – Control Rating after mitigation plan implementation);
- Residual Likelihood = (Likelihood of threat as per past occurrence - Control Rating of the Preventive Control after mitigation plan implementation);
- Calculate residual risk value and residual risk rating: Calculate the Residual Risk Value as per the following formula – Residual Risk Value = Residual impact \* Residual likelihood
- Estimate residual risk status: As per the defined Risk Acceptance Threshold for Ncell, if (Residual Risk Rating = 1-Low) or (Residual Risk Value  $\geq 1$  and Residual Risk Value  $\leq 5$ ), residual risk status

	<b>Ncell</b>	Classification: Internal
	<b>Risk Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

of all such risks shall be classified as 'No Action', thus implying that the selected controls are effective in mitigating the identified risk.


- vi. For cases, where the residual risk status is 'Mitigate' further controls shall be required to be applied for reducing the risk to an acceptable level.

## 6. Site Risk Assessment Methodology

Site risk assessment shall be conducted as per Industry Best Practices on Physical and Environmental security controls.

### 6.1 Site Risk Assessment Steps

Sr.No.	Activity	Responsibility	Documents Required	Processing Time
1.	Perform the site survey	Facility Manager	NA	NA
2.	<p>Perform site risk assessment for the identified critical facility. This checklist shall be filled by respective facility manager of the facility under scope. There would be one checklist filled per site.</p> <p>The domains considered in the site risk assessment checklist are as follows:</p> <ul style="list-style-type: none"> <li>Facts about location</li> <li>Physical security perimeter</li> <li>Physical entry controls</li> <li>Securing offices, rooms and facilities</li> <li>Protecting against external and environmental threats</li> <li>Working in secure areas</li> <li>Delivery and loading areas.</li> <li>Equipment siting and protection</li> <li>Supporting utilities</li> <li>Cabling security</li> <li>Equipment maintenance</li> <li>Removal of assets</li> <li>Security of equipment and assets off-premises</li> </ul>	Facility Manager	Site Risk Assessment Checklist	NA
3.	Identify and document the observations and findings during the survey as per the risk assessment checklist.	Facility Manager	Site Risk Assessment Checklist	NA
4.	Prepare a Site RA report basis compliance/non-compliance to the Site RA checklist controls. document the risk and recommendations to mitigate the risks in the risk assessment	Facility Manager	Site Risk Assessment Checklist	NA

	Ncell	Classification: Internal
	Risk Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 <sup>st</sup> October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Sr.No.	Activity	Responsibility	Documents Required	Processing Time
5.	Communicate the findings to Facilities and Services Head	Facility Manager	Site Risk Assessment Report	NA
6.	Formulate an implementation plan for the observations in the risk assessment report along with the timelines and responsibilities.	Facility Manager	Site Risk Assessment Report	NA

## 6.2 Risk Treatment Plan

Risk Treatment Plan will be formulated as per Section 5.

## 7. Governance and Compliance

- Exception management process shall be followed to raise the exception for this procedure.
- Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

## 8. Associated Documents

- Information Security Policy
- Asset Management Procedure