

# Project Go-Live

Ncell

Procedure

Approved Date:- 16/07/2020

Procedure Name DOCID: PR-IT-IS-19

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

## Document Control

### i. Document Identification

<b>Document Title and Version:</b>	<b>PR-IT-IS-19 Project Go-Live</b>
Effective Date:	16 <sup>th</sup> July, 2020
Document Author:	Enterprise Support and Platform Planning
Owner:	Enterprise Support and Platform Planning

### ii. Distribution List

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

### iii. Document Roles and Responsibilities

Responsible	Enterprise Support and Platform Planning
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

### iv. Digital Signature

CEO

CIO/Head Of IT


v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	22-08-2019	Bishwas Thapa	Initial document	Vishal Mani Upadhyay	10-01-2020
1	25-11-2019	Information Security Team	Ready for approval	Vishal Mani Upadhyay	16-07-2020
2	01-06-2020	Information Security Team	Approval	Andy Chong	16-07-2020
3	12-10-2023	Information Security Team	2. Review changed from annual to once every two years 7.4 Added EDR coverage requirement for IT Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	09-05-2024	Information Security	Re-branding	CIO/Head of IT	

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Asset Management Procedure</b>	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:

## Table of Contents

<b>Document Control</b> .....	2
<b>1. Purpose</b> .....	2
<b>2. Review and Updating</b> .....	2
<b>3. Scope</b> .....	2
<b>4. Definitions</b> .....	2
<b>5. Responsibilities</b> .....	2
5.1 OS / Database Planning and Management Team .....	2
5.2 Information Security Unit .....	2
5.3 Asset owner, custodian and project manager .....	2
<b>6. Onboarding Procedure</b> .....	2
<b>7. Checklist for Project Go-Live</b> .....	5
7.1 Application Checklist .....	5
7.2 IT Infrastructure Check .....	5
7.3 Security Checklist .....	6
7.4 Integration .....	6
<b>8. Annex-I</b> .....	7
8.1 Document Links .....	7
<b>9. Annex-II</b> .....	7
9.1 Template Names: .....	7
<b>10. Annex-III</b> .....	7
10.1 Abbreviations .....	7

	Ncell	Classification: Internal
	Asset Management Procedure	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:

## 1. Purpose

The process is important for any system which is hosted within Ncell premise and Ncell Owned Cloud Infrastructure for Asset Classification, Vulnerability Assessment and Minimum Baseline Security Standard (MBSS) for application, database and operating system as well as to ensure the systems have additional controls in place and follow the necessary approval process before going live. This document describes the process to follow for any project which processes data owned by Ncell, whether hosted at Ncell's own data center or in cloud. This document also provides the responsibility matrix with SLA, which helps on planning and timely delivery of the project's IT resources.

## 2. Review and Updating

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

## 3. Scope

This scope of this SOP is all Information Asset covered as part of defined scope for Information Security Management System at Ncell.

## 4. Definitions

- i. **Information Asset** – Information asset is any piece of information that has got value to the organization. Information assets consist of information and the systems / facilities that are used to process the information.
- ii. **Ncell Data** – Ncell data includes, but not limited to, the data, text, drawings, diagrams, plans, statistics or images (together with any database made up of any of these) which are embodied in any electronic, magnetic, electromagnetic, optical, tangible or other media, including any Personal Data which Ncell controls the Processing of.

## 5. Responsibilities

Following are the responsibilities of the roles defined as part of Project Go-Live:

### 5.1 OS / Database Planning and Management Team

OS/Database Planning and Management team is responsible to ensure that projects are compliant with requirements of the IT Infrastructure Checklist mentioned in the document.

### 5.2 Information Security Unit

Information Security unit is responsible to validate the MBSS compliance level as well as to ensure that projects are compliant with requirements of the Security Checklist mentioned in the document.

### 5.3 Asset owner, custodian and project manager

Ensure the systems, applications in the scope of any project adheres to the requirements of the document before the project starts processing Ncell data.

## 6. Onboarding Procedure

**Step 1:** The project owner must fill the Project document, elaborating infrastructure, On-prem or Cloud OS, DB and dependency software which is required for the application. The project document must be approved by Business and Technical owner with project milestone and responsibility matrix.

**Step 2:** After validating the requirement, provisioning of system by OS/Database Planning and Management Team with 100% compliance for VA and MBSS requirement for OS/Database (as applicable), installation of EDR Agent, Anti-virus agent and integration to GSOC, integration with Asset Management Tool, Integration to Patch Management Tool and handover the system to project owner.

Ncell	Ncell	Classification: Internal
	Asset Management Procedure	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:

**Step 3:** When the application is configured and ready to use, the application owner/vendor must ensure that the application, OS, database is compliant with the relevant MBSS and VA requirements and provide the report with necessary evidence.

**Step 4:** Application owner must ensure the asset has been onboarded to BMC Asset management tool, or in Hawkeye, with relevant information filled in. As part of this, application owner must identify the criticality (

Min CJ, CJ, C1, C2, NC), ownership, purpose of the application and so on, so that appropriate level of protection can be provided to the asset.

**Step 5:** Application owner must run scans for VA and MBSS compliance and send request for validation to Information Security team via the Hawkeye process. The request should be sent at least 5 business days in advance to the Information Security team to ensure accommodation of the requisite in the assessment plan. The VA can be run and report can be downloaded by the application owner themselves for necessary action for closure of the vulnerabilities.

Note 1: Scanning will be automated where scripts for the same are available (OS and some databases) for now. For the rest, Excel file embedded in the MBSS requirement document will need to be provided, with the necessary evidence filled in. Providing of necessary evidence are mandatory.

Note 2: Ownership for completeness of the asset inventory that will serve as an input for the MBSS and VA scans shall lie with the Project Manager / Application owner.

**Step 6:** After getting request, Security team will validate and provide necessary MBSS report to PM / application team/ IT infrastructure team.

**Step 7:** The respective team will validate the MBSS and VA report, fix the gaps on relevant nodes and provide updated compliance information including evidence, where necessary, for all applicable MBSS and VA requirements. All MBSS reports should be provided in the excel document which contains the MBSS requirement. The document for MBSS is at the following location:

Location: [Security SPOCs - MBSS 2.0 - All Documents \(sharepoint.com\)](#)

**Step 8:** After the reports are validated by the Security team, the non-compliance/not-applicable report will be sent back to respective team to validate and process for exception.

**Step 9:** MBSS compliance shall be 100% before the system goes live. All critical and high vulnerabilities shall be closed before the system goes live. Roadmap for closure of medium and low vulnerabilities shall be provided by respective team.

**Step 10:** Any deviation from the aforementioned requirements shall be routed through the exception management process.

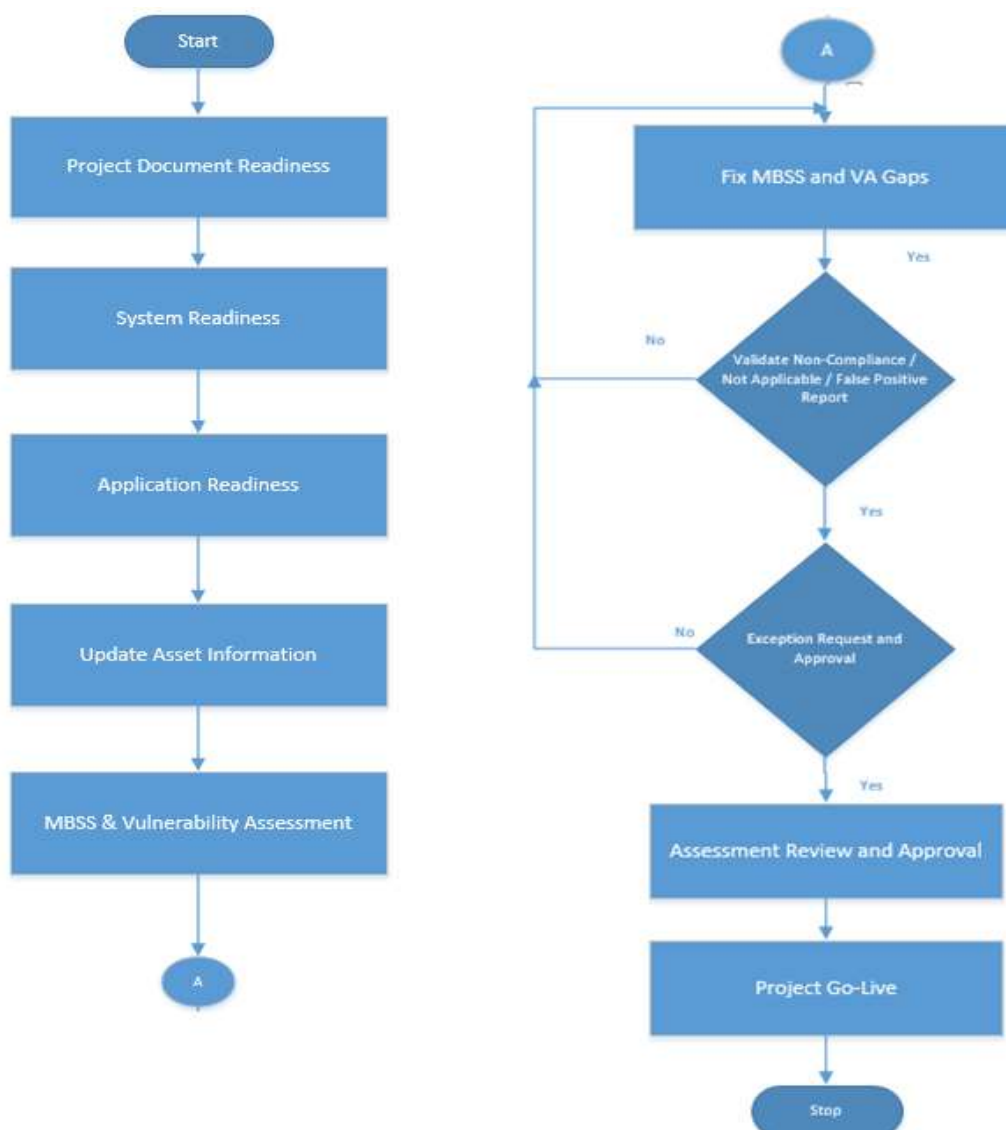
**Step 11:** Project Go-Live Readiness Assessment Review and Approval

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Asset Management Procedure</b>	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:


The Assessment review template for signing for the respective units are given in ANNEX-II. All the checklist on the respective units should be thoroughly checked and proceed for Approval. Sharepoint process will be used for assessment and approval from Information Security team before going live, to ensure that the requirements of this document are compliant with.

**Step 12: Project - Go live:** After Project Go-Live Assessment Review and approval, the project can start processing Ncell's customer data.

#### Workflow:





	Ncell	Classification: Internal
	Asset Management Procedure	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:


## 7. Checklist for Project Go-Live

### 7.1 Application Checklist

Area to Review	Completed	Document	Comments
<b>APPLICATION</b>			
• Whether latest patches applied	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Application High Availability and Resiliency	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Database Schema (where applicable)			
• User Privilege	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• UAT of Application features	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Application KPI Monitoring	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<ul style="list-style-type: none"> <li>• Service Catalog <ul style="list-style-type: none"> <li>○ List of services required to be running in the server</li> <li>○ List of available APIs for external connectivity with descriptions and access information</li> <li>○ Criticality and dependency matrix</li> <li>○ Application version and future roadmap</li> </ul> </li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Application Integration to IDM and PAM	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	

### 7.2 IT Infrastructure Check

Area to Review	Completed	Document	Comments
<b>IT Infrastructure</b>			
• Project Document Approval	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Installation of EDR and Anti-virus	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integrate to Asset Management and Patch management	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integrate to Backup and Archival and Update the Restoration Plan.	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integrate to Monitoring	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integrate to SIEM - GSOC	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Require license OS, Database, cluster and virtual platform	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• User creation and access management	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Asset List Update in Record	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integration with IDM and PAM solution	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Hardware and Power Redundancy Test	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Security Hardening Of OS, DB and Application	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integration to Patch Management Tool	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Cloud Compatibility Check Done	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	

	Ncell	Classification: Internal
	Asset Management Procedure	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:

### 7.3 Security Checklist

Area to Review	Completed	Document	Comments
<b>Security</b>			
• MBSS – Report with required evidences	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• BMC/Hawkeye – asset / information updated in the tools	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Result of Vulnerability Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Integration to SIEM	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• User Privilege Matrix (Both Ncell and vendor)	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• System Architecture Diagram with network flow	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• List of services running on server	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• IP Access List	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Roadmap for open vulnerabilities ( medium & low )	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Validation for user & account reconciliation ( removal of test, default & vendor accounts )	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
• Documented change of default and root passwords.	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	

### 7.4 Integration

Below mentioned integrations, except Asset management tool and Hawkeye, are mandatory for Crown Jewels (MCJ/CJ), internet facing systems, security tools. EDR is mandatory for IT Crown Jewels (MCJ/CJ), internet facing systems. For other systems, integration will be decided based on the risk assessment of the application. For Asset management tool and Hawkeye, integration with all assets are mandatory, regardless of the criticality of the application / system.

Integrations	Details
SIEM Solution - GSOC	All security audit logs should be enabled and logs should be forwarded to the GSOC IP : 10.18.12.47 or IP provided by Information Security Unit
Identity Management Tool - IDM	Integrate OS/database/application user privilege matrix with IDM so that all access requests can be approved via the tool
Privilege access management tool - PAM	Integrate OS/database user privilege matrix with PAM. Users will access the server via PAM.
Endpoint Detection and Response tool - EDR	Install EDR agent on all IT production nodes for fast detection and response.
Asset Management Tool	Individual assets within the scope of the project should be visible in Asset Management Tool
Hawkeye	Asset information, including criticality, classification should be updated in Hawkeye

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Asset Management Procedure</b>	Owner: Information Security Team
		Effective Date: 1 <sup>st</sup> January, 2020
Prepared by: Bishwas Thapa	Controlled by: Business Continuity & Process Management	Approved by MD/CEO:






## 8. Annex-I

### 8.1 Document Links

SN.	Description	Location
1.	Crowd Strike Agent	<a href="#">Security SPOCs - Tools - All Documents (sharepoint.com)</a>
2.	Antivirus Agent	\\192.168.70.136\Common_Softwares\Mcafee_agents
3.	IT Asset Record	<a href="https://hawkeye.ncell.com.np/">https://hawkeye.ncell.com.np/</a>
4.	MBSS Documents	<a href="#">Security SPOCs - MBSS 2.0 - All Documents (sharepoint.com)</a>

## 9. Annex-II

### 9.1 Template Names:

SN.	Description	Template File
1.	Project Document Template	 Project Document Template.docx
2.	Application Assessment Review Template	 Project Go-Live Check List from App
3.	IT Infrastructure Assessment Review Template	 Project Go Live Check List From IT.d
4.	Security Assessment Review Template	 Project Go-Live Check List from Secu
5.	Responsibility Matrix	 Responsibility Matrix.xlsx

## 10. Annex-III

### 10.1 Abbreviations

SN.	Abbreviation	Full-Form
1.	OS	Operating System
2.	DB	Database
3.	MBSS	Minimum Baseline Security Standard
4.	VA	Vulnerability Assessment
5.	IDM	Identity Management
6.	PAM	Privileged Access Management
7.	EDR	End point Detection and Response
8.	SIEM	Security Information and Event Management