

Sesa Goa Iron Ore

Information Security Management System (ISMS)

Procedure Documented information – Change Management Procedure

Documented information Name: Procedure Documented information – Change Management Procedure

Version No: 3.0

Last Updated: 25-July-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

This Documented information is a confidential documented information of Sesa Group

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the written permission of Sesa Group. This Documented information includes confidential information related to Sesa Group and shall not be distributed to any persons other than those mentioned in the distribution

Documented information Management Information

Documented information Title: Procedure Documented information – Change Management

Abstract: This Documented information is a procedure document highlighting the procedures for change management.

Documented information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented information Data
Documented information Title	Procedure Documented information – Change Management
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Change Management
Date of Release	23.01.2012
Documented information Revision	25-July-2023
Documented information Owner	IT Department
Documented information Author(s)	Sujay Maskara – Wipro Consulting Arjun N Rao – Wipro Consulting
Documented information Change Reviewer	Sandhya Khamesra, Pricoris LLP
Checked By	Dileep Singh - CISO
Security Classification	Internal
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature
1	Shobha Raikar (CDIO - IOB)	Shobha.raikar@vedanta.co.in	Electronically Approved 10-Aug 2023

Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.1	18.12.2012	Form Updated	Forms	18.12.2012
1.2	28-03-2013	Sesa Goa Logo Change		28-03-2013
1.3	18-10-2013	Sesa Group Logo , file name change for Sesa Sterlite Ltd - IOB		18-10-2013

1.4	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	2.1,2.2 and Forms	27-01-2014
1.5	01 – 12 -2014	Aligned to ISO 27001:2013	1.1,1.2, 2.4, 2.5,2.6, 4	05-12-2014
1.6	11-Feb-2016	Company name logo update		19-Feb-2016
1.7	18-Nov-2016	Rootvg backup	2.1	24-Nov-2016
1.8	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.9	22-Aug-2018	Review		29-Aug-2018
1.10	23-Aug-2019	Review		30-Aug-2019
1.11	09-Sep-2020	Review		16-Sep-2020
1.12	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18 Mar-2022	Review and Update		25-Aug-2022
3.0	25-July-2023	Review and Update		10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep K Singh	dileep.singh@vedanta.co.in

Table of Contents

1. Introduction	5
1.1 Scope of the Documented information	5
1.2 Purpose of the documented information	5
2. Procedures	5
2.1 Definitions	5
2.2 Change Management Input / Output Model	6
2.3 Change Management Procedure	8
2.4 Process Flow Narrative	10
2.5 Emergency Change	11
3. Roles and Responsibility Matrix	12
4. Templates	12
5. References and Related Policies	13

1. Introduction

1.1 Scope of the Documented information

This procedure document is applicable for Vedanta Limited –Sesa Goa Iron Ore Division including SRL and SMCL in Goa, Karnataka, Odisha and Liberia, Pig Iron Division, Met Coke Division , Power Division in Goa Sesa Coke- Gujarat & Vazare , FACOR – Odisha , and VGCB , Visakhapatnam; referred as Sesa Group in this document

The organizational and infrastructural changes subject to this process include hardware, software, system components, services and processes—anything deliberately introduced into the Sesa group environment that could affect its functioning.

1.2 Purpose of the documented information

The IT environment is a dynamic one, constantly changing in response to changing needs, the availability and introduction of new technologies, as well as normal business growth. The IT environment is also extremely complex, containing many inter-dependencies that have become increasingly crucial for the basic survival of a business. For these reasons, organizations require a disciplined process that can introduce required changes into this environment with minimal disruption to ongoing operations.

The purpose of Sesa Group's Change Management procedure is to:

- Ensure all changes made in the systems are standardized, disciplined and goes through an approved work flow before the final implementation.
- Provide a guideline for categorization of the type of change based on its urgency, on how quickly a change is required (Priority) by Sesa Group and to define the change's impact on Sesa Group.

2. Procedures

2.1 Definitions

Change: Any new IT component deliberately introduced to the IT environment that may affect an IT service level or otherwise affect the functioning of the environment or one of its components.

Change Advisory Board (CAB): The CAB is a cross-functional group set up to evaluate change requests for business need, priority, cost/benefit, and potential impacts to other systems or processes. Typically the CAB will make recommendations for implementation, further analysis, deferment, or cancellation. The CAB would include the HODs of the various departments, the Change Manager, CISO/ CDIO IOB / Head-IT.

Change Category: The measurement of a change's deployment impact on IT and the business. The change complexity and resources required, including people, money, and time, are measured to determine the category. The risk of the deployment, including potential service downtime, is also a factor.

Category	Description
Major	A change where the impact on the group could be massive. e.g. a departmental or corporate-wide change, or a network-wide or service-wide change

Minor	A change affecting small numbers of individuals for example, a change to a printer used by a department consisting of just a few members.
Standard	A change that has been performed before and is part of the operational practice of the business. E.g. an update to a user profile.

Change Priority: A change classification that determines the speed with which a requested change is to be approved and deployed. The urgency of the need for the solution and the business risk of not implementing the change are the main criteria used to determine the priority.

Priorities	Description
High	A change that is important for the organization and must be implemented soon. E.g. an upgrade in line with new legislation requirements.
Medium	A change that should be implemented to gain benefit from the changed service. E.g. between versions upgrade to a customer feedback service.
Low	A change that is not pressing but would be advantageous. e.g. a “nice to have” addition to a user profile

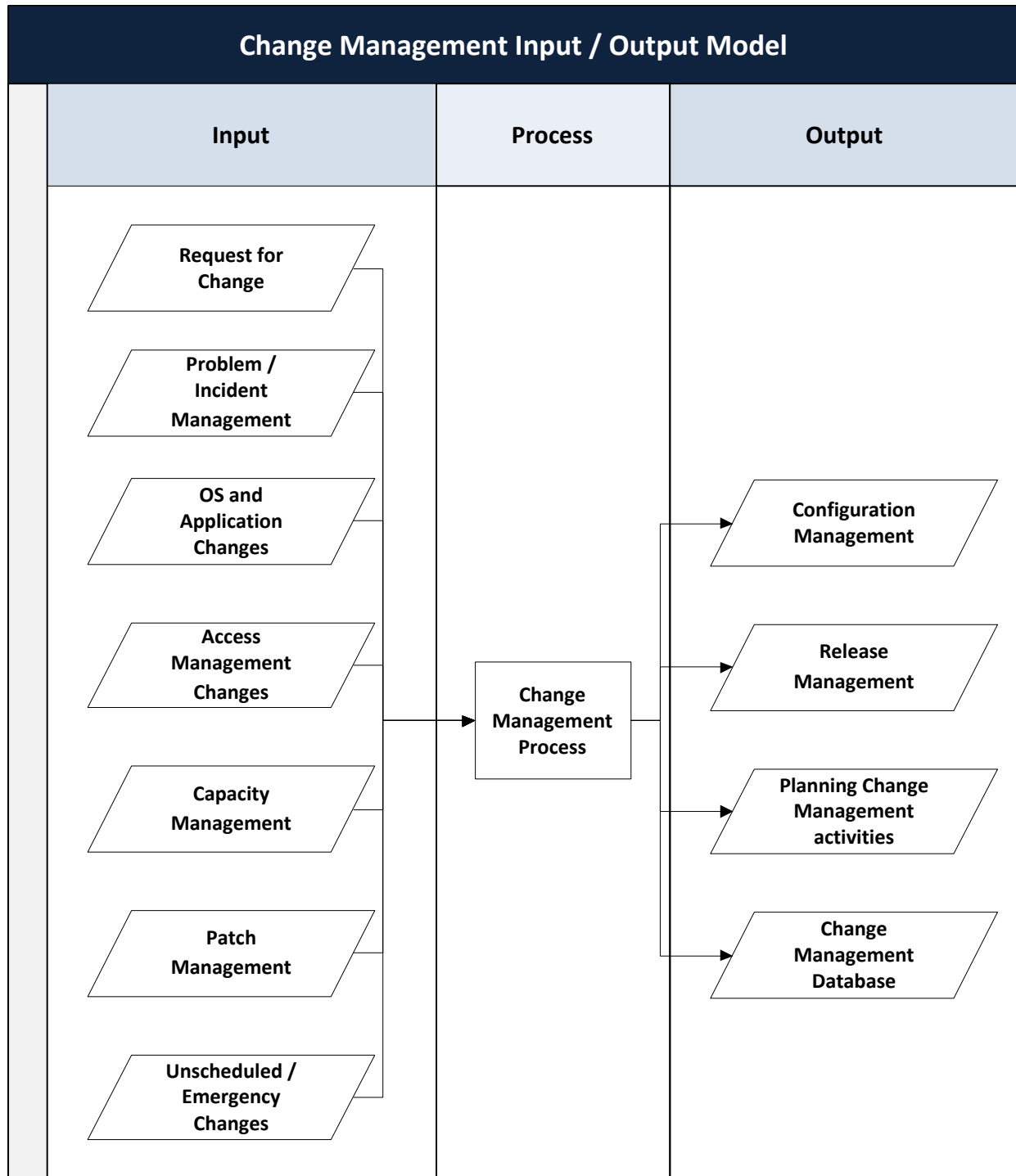
Change Initiator: A person who initiates a request for change; this person can be a business representative or a member of the IT organization.

Change Manager: The role that has the overall management responsibility for the change management process in the IT organization.

Request for Change (RFC): This is the formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.

Change Implementer: The role that is responsible for planning and implementing a change in the IT environment. The change owner role is assigned to an individual for a particular change by the change manager and assumes responsibilities upon receiving an approved RFC. The change owner is required to follow the approved change schedule.

2.2 Change Management Input / Output Model



Inputs required:

- Request for Change
- Problem / Incident Management – Changes enabling incident and problem resolution
- Operating System and Application Changes
- Access Management Changes – Changes to user ID and access request

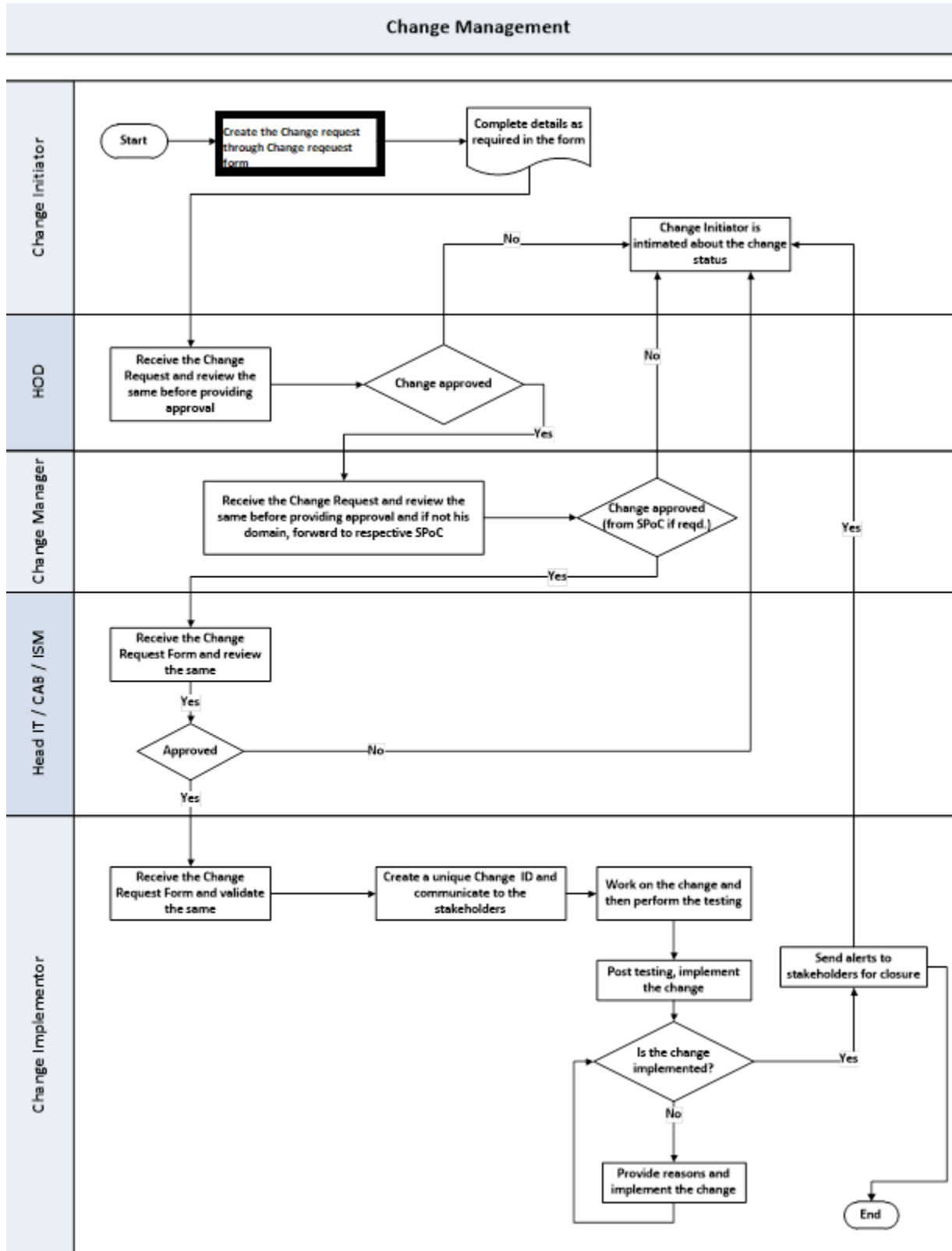
- Capacity Management that has to undergo certain changes
- Patch Management that addresses the latest patches for Operating Systems
- Unscheduled / Emergency Changes

Outputs generated:

- Configuration Management – The Changes that affects the configuration of information systems.
- Release Management – Once one or more changes are developed, tested, and packaged into releases for deployment, release management is responsible for introducing these changes and managing their release.
- Planning Change Management activities.
- Change Management Database

2.3 Change Management Procedure

Below is the change management process flow diagram:



2.4 Process Flow Narrative

Sr. No.	Step	Responsibility
1.	Log a change request User (change initiator) to create the change request through Change request form	End User (Change Initiator)
2.	HOD review and approval Respective HOD to review and provide their approval for the change and forward it for further approval to Change Manager.	HOD
3.	Change Manager Review and Approval Change Manager (CM) approves the same with a valid business justification or if rejected, the same is intimated to the stakeholder / change initiator. Also, if it is out of CM's domain, the same is review by the relevant SPoC and approved.	Change Manager
4.	CDIO / Head-IT Approval Further, the change request is forwarded to CDIO/ Head-IT / CISO / CAB (change advisory board) for review and approval.	CDIO / Head-IT / CISO / CAB
5.	Change Implementer's role After receiving the approval, the change implementer would generate a unique ID for the change and work on the change request.	Change Implementer
6.	Testing of the change request After the change request is completed, the team would perform a test to validate the change and gaps, if any.	Change Implementer
7.	Change Implementation and intimation Once the test is validated, the change is implemented and the same is communicated to the change initiator / stakeholders / HODs.	Change Implementer
8.	Roll Back Plan If the change is not successful roll back plan to return the system to a prior state will be implemented	Change Implementer
9.	Post Implementation Review Review of the success/failure and learnings will be reviewed post implementation.	Change Implementer

2.5 Emergency Change



An accelerated authorization and planning procedure has to be performed in the case of an emergency change. The categorization of Emergency change is verified by the Domain experts / Subject Matter Experts. The CAB /CISO / CDIO / Head-IT is responsible for the authorization and scheduling of these kinds of changes. There may not be a formal CAB meeting, due to lack of time and urgency, in which case the telephone or e-mail approval from the authorized person is taken.

- The emergency change categories could be:
 - Business need – e.g. Database changes
 - Risk related to desktop data – e.g. Patch application
 - OS & application related patch application
 - Hardware failure at crucial period – e.g. RAM / HDD failure
- Unscheduled changes must be carried out only in case there are critical production issues, which require the change to be carried out.
- After unscheduled changes are carried out, normal change procedures must be expedited within 3 days.
- Unscheduled changes must be documented and reviewed subsequent to the change.
- Only authorized persons should be allowed to make emergency changes.
- All emergency changes should be ratified through normal change management procedures afterwards to analyze the emergencies.

3. Roles and Responsibility Matrix

Role	Responsibility
Change Initiator	<ul style="list-style-type: none"> • Raise RFC in the standard format available • Ensure to fill in all the details in the RFC
Change Manager	<ul style="list-style-type: none"> • Initial level screening, reality check and approval of RFCs. • Reclassification of 'Priority' and 'Category' level of the RFCs. • Informing the Change Initiator about the status of the RFC. • Coordinating CAB meetings. • Ensure emergency priority changes are escalated to the CAB for fast-track approval.
Change Advisory Board (CAB) / CDIO IOB / Head-IT	<ul style="list-style-type: none"> • Reviews the RFCs (submitted by the Change Manager). • Prioritizes and Categories the Change. • Conduct the Impact Assessment. • Post implementation review of the change.
Change Implementer	<ul style="list-style-type: none"> • Implement the Change. • Inform RFC status to Change Initiator, Change Manager, and CAB. • Deploy Roll-Back Plan if the Change was not successfully executed. • Update the change request completion details

4. Templates

Sr. No.	Documented information Name	Documented information Version	Documented information Attachment
1	Change Management Form	V 1.5	 Sesa Group_Form_Change
2	Active Directory ID Unlock and Password Reset Request form	V 1.2	 Active Directory ID Unlock and Password

5. References and Related Policies

- Change Management Policy