TRIANZ℠

System and Software Change Management Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Objectives

The objective of this process is to ensure that changes are recorded in a controlled manner and the changes are evaluated, authorized, prioritized, planned, tested, implemented, and documented.

- Provide standardized methods, procedures for efficient and prompt handling of allchanges
- Record all changes to service assets and configuration items in the CMDB
- Respond to customer's changing business requirements while maximizing valueand reducing incidents, disruption and rework
- Respond to the business and IT requests for change that will align the services withthe business needs

2. Scope

This process applies to all Trianz users as well as to the third parties, and Trianz Information System resources.

A change within the environment is any modification that has the potential to impact sharednetwork, computing or business applications by altering its existing state.

This includes, but is not limited to:

- *System Hardware*
- *System Software*
- *Business and Management Application or Service*
- *Databases*

3. Introduction

Service and infrastructure changes can have a negative impact through service disruption unless managed efficiently and effectively. Having an effective change management processadds value to the business by:

- Prioritizing and responding to business change proposals
- Contributing to meet governance, legal, contractual, and regulatory requirements
- Reducing failed changes and therefore service disruption, defects and rework
- Delivering changes promptly to meet business timescales
- Contributing to better estimations of quality, time and cost of change
- Assessing risks associated with the transition of services (introduction, modificationor disposal)

4. Entry Criteria

RFC raised by authorized person

5. Inputs

A Request for Change (RFC) is raised because of the identification of a 'need for change'. Requests for change can come from any part of the organization and from any party contracted to provide services to that organization. All requests for change need appropriatesponsorship and authorization.

A need for change will arise for a variety of reasons:

- *Proactively, e.g. seeking business benefits such as reducing costs or improvingservices or increasing the ease and effectiveness of support.*
- *Reactively as a means of resolving errors and adapting to changingcircumstances, e.g. legislative or regulatory requirements.*

6. Process Description

This section describes the activities involved in the Change Management Process. These components are presented using the conventional Change Management framework – classification [initiation (justification), review (entitlement, evaluation), planning (Risk & Impact Analysis, Change design and development, plan preparation, scheduling), approval,

implementation (implementation and testing) and closure].

Changes are classified based on the following types:

1. Normal Change
2. Standard Change
3. Emergency Change

6.1 Normal Change Process

The objective of Normal Change:

- Standardized procedures are used for efficient and prompt handling ofnormal changes
- To respond to the customer's changing business requirements whilemaximizing value and reducing incidents, disruption and re-work
- To respond to the business and IT requests for change that will align theservices with the business needs
- To improve future changes by learning from previous mistakes andsuccesses

Normal change is a change that meets established enterprise change management lead-time requirements. Normal changes will follow the completechange management process.By definition, a normal change will proceed through all steps of the change management process and will eventually be reviewed by the Change AdvisoryBoard (CAB) (changes with risk levels 4 and 5 only).

Examples of normal changes:

- Software upgrades
- Hardware upgrades
- Application enhancements

6.2 Standard Change Process

The objective of Standard Change are:

- Standardized procedures are used for efficient and prompt handling of standardchanges
- To respond to the customer's changing business requirements while maximizingvalue and reducing incidents, disruption and re-work
- To respond to the business and IT requests for change that will align the serviceswith the business needs
- To improve future changes by learning from previous mistakes and successes
- Any change that has an established and approved procedure for implementation; isrepeatable and can be implemented with minimum risk. The characteristics of a standard change are
  - *Low risk and pre-approved AAA*
  - *Routine*
  - *Proven track record of success*
  - *Minimal complexity*
  - *Accepted change window*
  - *Approved standard operating procedure (SOP) for implementation*

The standard change needs to be approved only once. Each subsequent occurrencerequires a record but does not need approval.

Examples:

- *Install and rack new equipment*
- *Internet site maintenance*
- *Weekly reboots*
- *Building new servers*
- *Download and installation of Virus DAT files*

6.3 Emergency Change Process

Any change that has a high impact on business operations of the organization, is notoptional, and needs to be implemented immediately.
Most emergency change requests will be linked to a corresponding incident record.
An emergency change should not be used in order to bypass the appropriate lead-time.Documentation requirements for

emergency changes are the same as any change.

The change coordinator is responsible for meeting all requirements for the changedocumentation within one working day of the change implementation.
Criteria for emergency change:

- To resolve or prevent a major incident
- To implement a critical security patch, ex: a virus outbreak
- Any changes which are at risk level 1, 2 or 3 and requested lead time is lessthan one business day
- Any changes which are at risk level 4 or 5 and requested lead time is lessthan eight business days

6.4 Post Implementation Review

Post implementation reviews are performed at two levels

- *By change coordinator (for all risk levels)*
- *By Change Advisory Board (CAB) (for risk level 4,5 and all failed changes)*

Once all the implementation activities are completed, the coordinator performs the postimplementation review of all changes irrespective of risk levels

Post implementation review includes aspects of the change such as:

- *Performance*
- *Security*
- *Functionality*

- If the change is successful the change coordinator updates the change status as'installed successfully'
- If the implementation of the change is not done as advertised, follow-up actions(including implementation of back out plan) will be implemented by the coordinator
- If the change fails the change coordinator updates the change status as 'backed out' or 'installed with issues' or 'partially installed' and documents the reasons forthe failure
- CAB performs the post implementation review on successful changes (risk levels4,5 only) and all failed changes as well

Note: For successful changes, which are at risk level 1, 2, and 3, the CAB will notperform the Post Implementation Review (PIR)

Optional: CAB may use Post Implementation Review (PIR) Report for conducting postimplementation review of major application and infrastructure changes

7. Exit Criteria and Output

- *Approved and scheduled Change Requests*
- *Forward Schedule of Change*
- *Configuration Items updated and maintained through Change process*
- *Change reports*
- *CAB minutes and actions*
- *Rejected Changes with proper justification*

8. Roles and Responsibilities

Role	Responsibility	Internal/External
Change Coordinator	• Identifies the business, service or technical needs of the change • Creates and updates change records with relevant information • Refers to Configuration Management Database (CMDB) and assesses the change for risk, impact, urgency and priority • Continually evaluates the risk of the change • Updates the change record timely with the appropriate status and results • Works with change approver and change manager to ensure all changeissues are communicated and recordsreflect all changes • Builds and tests changes (or) Coordinates with relevant people for building and testing of changes	

	• Implements the approved changes • Manages the installation of the changes	
Change Approver	• Assesses the change for risk, impact, urgency and priority • Reviews implementation plans, backout plans, test plans, test results for implementation readiness and approve/reject the change • Works with the change coordinator to ensure all issues surrounding a change have been resolved and communicatedto all essential areas • Conducts root cause analysis in case of failed changes and also if incidents are caused by changes	
Change Manager	• Reviews change records forprocedural compliance, • information quality and completeness • Ensures that all changes are appropriately planned and communicated • Rejects or schedules changesvia change management tool • Integrates new changes into the existing change schedule • Identifies conflicts in the schedule and negotiates adjustments with the relevant	

	parties • Provides inputs to and participates in CAB meetings • Schedules and attends all meetings concerning the change management process • Highlights pertinent/required change activities to appear onManager's review report by end of day Tuesday. Ensures representation is in place for these activities at the Managers' review meeting • Challenges the activities of theother areas for readiness at any of the change review meetings • Facilitates expedited and emergency changes as per • process	
10.1 Change Advisory Board (CAB)	• A group of people that advisesthe enterprise change manager in the assessment, prioritization, scheduling and post implementation of changes • Participates in all ChangeAdvisory Board (CAB) meetings • Reviews 'Requests for standard changes (Pre- approved changes)' and advises the enterprise changemanager to approve / reject the requests • Reviews and verifies whetherright risk level, impact, urgency and priority is assigned for the changes • Participates in the prioritizationand scheduling of changes • Ensures proper implementation and back outplans are in place • Conducts post-implementationreview of the changes as per workflows • Reviews all partially installed,installed with issues and backed out changes • Review unauthorized changes detected	

	during configuration audits	

9. Measurement

Key Performance Indicator (KPI)	Definition
Number of Major Changes	• Number of major changes assessed by the CAB (Change Advisory Board)
Number of CAB Meetings	• Number of CAB (Change Advisory Board) meetings
Time for Change Approval/ Rejection	• Average time from registering an RFC with Change Management until a decision on the RFC is reached (i.e. until it is either approved or rejected)
Change Acceptance Rate	• Number of accepted vs. rejected RFCs
Number of Emergency Changes	• Number of Emergency Changes assessed by the ECAB (Emergency Change Advisory Board)

10. Standards Addressed

ISO 20001		
Clause	**Description**	
8.5.1 Change management 8.5.1.1 Change managementpolicy	A change management policy shall be established and documented	
8.5.1.2 Change managementactivities	The organization and interested parties shall make decisions on the approval and priority of requests for change.	
CMMI-DEV		
Process Area	**Practice**	**Description**

11. Appendix A:

11.1 Guidelines for Risk and Priority Assessment

11.1.1 Risk Assessment

Risk level is computed in the following two ways:

- Risk assessment questionnaire
- Configuration Item (CI) criticality
  - By Environment – Production/QA/Testing/Dev
  - Production – by business value of the CI
  - QA/Testing/Dev – Each environment will have an associated risk value

The overall risk level for a particular change is equal to the greater of the above two values.

11.1.2 Risk Assessment Questionnaire

There are 5 risk levels and they are:

- Level 1 (Minimal Risk)
- Level 2 (Low Risk)
- Level 3 (Medium Risk)
- Level 4 (High Risk)
- Level 5 (Extreme Risk)

Risk involved in implementing a change will be based on the overall risk assessment score for a change. When a change coordinator completes the risk assessment questionnaire, the risk level is computed corresponding to the following guidelines:

Overall Risk Level = ((Risk 1 * Weight 1) + (Risk 2 * Weight 2) + (Risk 3 * Weight 3) + --- +(Risk n * Weight n)) / (Weight 1 + Weight 2 + Weight 3 + --- + Weight n)
The calculated risk does not result in a whole number. The results must be rounded off tothe next highest number.

The logic here is that no risk should be downplayed. Any risk greater than the whole numbershould be shown as the next risk up.

For example, 3.00001 becomes 4
4.91 becomes 5
The risk assessment questionnaire covers the following factors:

Assessment Factor	Weightage for Each Question (%)	Scoring(1-5)
1. What is the degree of visibility of the change within <Client> Organization?	100	
Visible and communicated to all Heads of thedepartments of IIS and/or <Client>		5
Visible and communicated to one Head of thedepartment of IIS and/or <Client>		4
Visible and communicated to multiple IIS and/or <Client>departments		3

Assessment Factor	Weightage for Each Question (%)	Scoring(1-5)
Visible and communicated within a single IISdepartment or <Client>		2
Routine IT activity		1
2. What is the degree of visibility of the change to ITCustomers?	100	
Very High		5
High		4
Medium		3
Low		2
Minimal		1
3. How difficult/easy is the Back out?	100	
Back out is impossible or undesirable		5
Back out is difficult		4
Back out is possible, though not easily executed		3
Back out is in place and easily executed		2
Minimal		1
4. What is the degree of experience with this type ofchange?	100	
New technology, no experience		5
New technology, limited experience		4
Existing technology, some experience		3
Existing technology, considerable experience		2
Existing technology, lot of experience		1
5. How much time does it take to complete the change(including change building, testing and implementation)?	100	

More than six months		5

Assessment Factor	Weightage for Each Question (%)	Scoring(1-5)
Six months or less		4
One quarter or less		3
One month or less		2
One week or less		1
6. What is the impact on other systems orapplications?	100	
More than one critical business application		5
One critical business application		4
More than four non-critical business applications		3
Less than or equal to four non-critical businessapplications		2
None		1
7. What is the change to Business Process?	100	
Considerable and complex change required by ITand/or the customers		5
Moderate change required by IT and/or the customers		4
Little change required		3
Minimal change		2
No change		1

1 Appendix B:

Priority	IMPACT			
URGENCY	Extensive/ Wide Spread	Significant/Large	Moderate/ Limited	Minor/ Localized

Critical	Critical	Critical	Critical	Critical
High	High	High	High	High
Medium	Medium	Medium	Medium	Medium
Low	Low	Low	Low	Low

12. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological	8.32 Change management Control Changes to information processing facilities and information systems shall be subject to change management procedures. 8.19 Installation of software on operational systems Control Procedures and measures shall be implemented to securely manage software installation on operational systems,	System and Software Change Management Procedure

Document Control

Owner:	CISO	**Release ID:**	SSLM-PROC-0054

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.0	26-Feb-07	Jyotessh GNair			Draft	
1.0	26-Feb-07	Jyotessh GNair			Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.1	14- May-09	Bharatee sha B R			Risk Assessment and Risk Treatment Plan	Consolidated the controls related to software license management
2.0	04-Jun-09	Balu Nair			Approval for Baseline	Baselined
2.1	30-Dec-10	Chakrav arthi			QMG review	Formatted entire document
3.0	30-Dec-10	Chakrav arthi			Request for baseline	Baselined
3.1	24-May-11	Srilaksh mi			QMG Review	Modified release id in header and cover page to make consistency

4.0	24-May-11	Srilakshmi			Approval for Baseline	Baselined
4.1	3-Aug-11	Sudharsana			QMG review	Replace Owner with Management Representative inplace of CIO In Document Classification Scheme, "Retention period is3 Years" row is removed
5.0	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
6.0	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo
6.1	29-Apr-19	Balu Nair	Joshy VM			• Information classification modified • Trianz logo modified
7.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
7.1	12-May-20	Balu Nair	Phani Krishna		For review	Migrated to the new template
8.0	15-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
8.1	28-Jan-21	Ankur Rastogi	Rakesh		For Review	• Change Management Procedure is added as a separate section to align to ISO 20000-

						1:2018 standard
9.0	28-Jan-21	Ankur Rastogi	Rakes h	Vivek Sambasiv a m	For Approval	Approved and Baselined
9.1	21-Dec-21	Karthik N	Karthik N		For Review	Updated the information classification and few formatting changes.
10.0	13-Jan-22	Karthik N	Karthik N	Sivaramak rishnan N	For Approval	Approved and Baselined
10.1	12-Apr-23	Karthik N and Asha Veerama llu	Karthik N		For Review	Moved the software licensing part to system and software license management procedure. New template change
11.0	09-May-23	Karthik N	Karthik N	Srikanth M	For Approval	Approved and Baselined
11.1	11-Feb-24	Shalini	Vijaya	Srikanth M	For Review	Mapped with new ISO 27001 2022 controls
12.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined
12.1	28-May-2025	Kruti	Vijaya		For Review	Migrated to New template
13.0	29-May-2025	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com