TRIANZ℠

Business Continuity and Disaster Recovery planning 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. **PURPOSE** 4
2. **OBJECTIVE(S)** 4
3. **SCOPE** 4
4. **ENTRY CRITERIA AND INPUTS** 4
5. **ROLES & RESPONSIBILITIES** 5
6. **BUSINESS CONTINUITY AND PLAN PROCEDURE** 6
   - 6.1 Identifying and Prioritizing Critical Functions, Systems and Processes 6
   - 6.2 Identifying Critical Resources 6
   - 6.3 Business Continuity Planning 7
7. **PLANNING INFORMATION SECURITY CONTINUITY** 8
8. **EXIT CRITERIA AND OUTPUT** 9
9. **PREREQUISITES** 9
   - 9.1 Resource 9
   - 9.2 Training 9
   - 9.3 Reference Policy, Process, Procedure, Templates, Checklist 9
   - 9.4 Related Guidelines, Templates, and Checklists 9
10. **MEASUREMENT** 10
11. **ISO CONTROL MAPPING(S)** 10

1. Purpose

The purpose of this document is to describe the Business Continuity and Disaster Recovery Procedure and define the activities for each phase.

2. Objective(s)

- Business continuity planning is to minimize interruptions to the business's ability to provide its products and/or services, minimize financial loss, and being able to resume critical operations within a specified time after a disaster.
- Disaster recovery planning is to protect the organization in the event that all or part of its ICT operations and/or computer services are rendered unusable.

3. Scope

This policy applies to all critical Client engagements, Trianz managed products and services and functions executed from all Trianz locations and all support functions covering people, process, and technology.

4. Entry Criteria and Inputs

- Top Management Support
- Business Impact Analysis and Risk assessment
- Organization goals and objectives
- Critical Business Applications / Trianz products
- New Disasters including Pandemic

5. Roles & Responsibilities

Role	Responsibility	Internal/External
Trianz Business Resilience Group (BRG)	• BRG group are the decision makers and provides directional input and guidance to Crisis Management Team (CMT) in case of any emergency or a crisis. BRG will make collective decision to invoke a BCP.	Internal
Trianz Crisis Management Team (CMT)	• CMT team is responsible for management of crisis, issues, additional risks, exposures, and stakeholder interests in response to an event or disaster.	Internal
Trianz Engagement/Account Recovery Team (ART).	• Trianz engagement or account recovery team is responsible for supporting the business continuity and disaster recovery procedures for the respective engagements.	Internal
Trianz InfoSec & Data Privacy Assurance Team	• Trianz InfoSec team drives the business continuity initiatives across Trianz for all the critical strategic engagements.	Internal
Trianz Delivery Team/ Trianz Product Team	• Responsible for the development and maintenance of business continuity and disaster recovery plans and understand their processes, identify risks, and provide	Internal

	guidance to help manage and minimize those risks.	

6. Business Continuity and Plan Procedure

6.1 Identifying and Prioritizing Critical Functions, Systems and Processes

- Business continuity representative from InfoSec team identifies and prioritizes the Trianz critical processes and Applications with the help of delivery and corporate functions.
- InfoSec BCM Representative assesses impacts from loss of information and services from both internal and external sources.

6.2 Identifying Critical Resources

- InfoSec BCM representative identifies the resources that are critical to the information systems that support the functions, systems and processes that has been identified in above section
- The critical resources should include everything necessary to support the critical function, system, or process. Some examples of critical resources are:
  - Servers, workstations, and peripherals,
  - Applications and data,
  - Media and output,
  - Telecommunications connections,

- Physical Infrastructure (e.g., electrical ower, environmental controls), and Personnel.

6.3 Business Continuity Planning

- Business continuity planning refers to maintaining business functions or quickly resuming them in the event of a major disruption.
- A business continuity plan outlines procedures and instructions an organization must follow in the face of such disasters.
- For each critical (in scope) process/system/ICT functions two values are assigned:
  - Recovery Point Objective (RPO) for Applications, products.
  - Recovery Time Objective (RTO) for business processes, products, and applications.
  - InfoSec BCM Representative prepares the Business Continuity Plan which contains the following sections:
  - Business Continuity Strategies to reduce impact of business disruptions.
  - Business Requirements based on Disaster Classification.
  - Key resources and contact details.
  - Escalation plan contains the list of contacts shall be notified during a potential emergency or disaster Communication Plan.

  o Organization Chart Test Planning shown below table:

Level 1	• Invocation of the Business Continuity Process for the Primary Facility from within its premises.
Level 2	• Invocation of the Business Continuity Process for the Primary Facility from a different city in the same country

- BRG along with CMT activates the Disaster Recovery Procedure.

- InfoSec BCM Representative identifies the alternate site to continue the in case of failure in resumption the work.
- InfoSec BCM Representative ensures that Business activities return to normal operation.
- InfoSec BCM Representative ensures to conduct call tree, tabletop, and simulation tests for the key critical projects as per the contractual agreement.
- Call tree tests shall be conducted bi-annually, and tabletop simulation tests shall be conducted annually depending on the client requirement.
- In case of pandemic situation and associates will be working remotely, all the BCP tests (work area recovery simulations) for the key projects and functions will be on hold during that period.

7. Planning Information Security Continuity

Trianz follows a single framework of business continuity plans that are maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing maintenance.

Each plan shall have a specific owner. Emergency procedure, manual fallback plans and resumption plans shall be within the responsibility of owners of appropriate business resources and process involved.

A business continuity planning framework shall address the identified information security requirements by considering the following.

a) The conditions for activating the plans which describe the process to be followed (e.g., how to access the situation, and who is too involved) before each plan is activated.

b) Emergency procedures which describe the action to be taken following an incident.

c) Temporary operational procedures to follow pending completion of recovery and restoration.

d) Resumption procedures which describe the action to be taken to return to normal business operations.

e) The critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

The responsibilities of the individuals, describing who is responsible for executing which components of the plan is alternative shall be nominated.

8. Exit Criteria and Output

BCP Testing (planned and Live BCP)

9. Prerequisites

9.1 Resource

People, Process and Technology

9.2 Training

BCM Awareness trainings

9.3 Reference Policy, Process, Procedure, Templates, Checklist

Document Name
Business Continuity Policy

9.4 Related Guidelines, Templates, and Checklists

Document Name
Business continuity plan template

10. Measurement

- # of successful business continuity tests vs total

  business continuity tests planned

- # of successful call tree tests vs total call tree tests

  planned.

- # of successful tabletop simulation tests vs total tabletop simulation tests planned

11. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Organizational Controls	5.30 ICT readiness for business continuity ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Business Continuity Policy

Document Control

Owner:	CISO	**Release ID:**	BCDR-PROC-0041

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	09-Apr-10	Chakravarthi			Initial draft	None
1.0	18-Apr-10	Chakravarthi			Approved for baseline	Baselined
1.1	14-May-10	Balu Nair			QMG Review	Document formatted
2.0	20-May-10	Balu Nair			Approval for baseline	Baselined
2.1	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency
3.0	24-May-11	Srilakshmi			Approval for Baseline	Baselined
3.1	3-Aug-11	Sudharsana			QMG review	• Replace Owner with Management Representative in place of CIO • In Document Classification Scheme,

						"Retention period is 3 Years" row is removed
4.0	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
5.0	30-Dec-11	Sudharsana			Registrant audit findings (Audit Date: 24-26 October 2011)	Added Frequency & Criteria of the Review of Business Continuity Plans section
6.0	08-May-12	Yuvaraj D &			Self-Review	• Moved disaster classification table

		Gangadhar Aka				to test planning in section 4.3 • Identified ISO 27001 Controls
7.0	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	• Modified the template format • Changed the Logo

8.0	22-Jan-13	Srilakshmi			Customer Audit finding on Jan 09th & Jan 10th 2013	• Modified section 5.5.2 – Media Storage, referred Backup and Restoration Procedure
9.0	16-May-15	Sudharsana			Upgrading to ISO 27001:2013	• Added 5.5,5.6,5.7,5.8, • planning information security continuity • Implementing information security Continuity • Verify, review and evaluate information security continuity • Availability of information processing facilities
9.1	25-Feb-19	Karthik Narasimha	Joshy/Balu		To check document adequacy on the latest BCP structure	Added the event response and analysis.

10.0	14-May-19	Karthik Narasimha		Ganesh Arunachala	Approved for Baseline	Baselined
10.1	17-Oct-19	Karthik Narasimha	Phani/Balu		Review	Updated the frequency of BCP testing

11.2	22-Oct-19	Karthik Narasimha	Phani		Review	Changes updated post review from Phani
12.0	20-Dec-19	Balu Nair		Vivek Sambasivam	Approved for Release to Blue Book	Baselined
12.1	11-May-20	Karthik N	Balu Nair		Review	SLT communication. (Modified section 11.0)
13.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
13.1	13-Jan-21	Karthik N	Phani Krishna		For Review	Updated the BCP section and the information classification
14.0	13-Jan-21	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and baselined
14.1	2-June-21	Karthik N	Phani Krishna		For Review	Modified a few sections as per the review process
14.2	11-June-21	Karthik N	Phani Krishna		For Review	Changes incorporated as

						per Phani's feedback
15.0	11-June-21	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and baselined
15.1	30-July-21	Karthik N	Balu N	Phani Krishna	For Review	Changes incorporated as per Phani's feedback
16.0	30-July-21	Karthik N	Balu N	Phani Krishna	For Approval	Approved and baselined
16.1	23-12-21	Divya G	Karthik N		For Review	Modified section 5 – Roles and Responsibilities.
17.0	13-Jan-22	Divya G	Sivaramakrishnan N	Sivaramakrishnan N	For Approval	Approved and baselined
17.1	14-Mar-22	Kruti	Karthik N		For Review	The scope has been extended to products and services
18.0	17-Mar-22	Kruti	Siva N	Siva N	For Approval	Approved and baselined
18.1	01-Mar-23	Krutideepta and Asha	Karthik N		For Review	Frequency of call tree and tabletop simulation tests has been added
		Veeramallu				New measurements have been added New template change
19.0	08-May-23	Krutideepta	Karthik N	Srikanth M	For Approval	Approved and baselined

19.1	15-Feb-24	Kruti	Beniyel S & Vijaya R		For Review	1. Updated the objective with as per ISO 27001:2022 Standard. ISO Mappings has been added.
20.0	23-Feb-24	Kruti	Beniyel S & Vijaya R	Srikanth M	For Approval	Approved and Baselined.
20.1	30-Apr-25	Kruti	Vijaya R		For Annual Review	Migrated to a new Template and Yearly Review
21.0	29-May-25	Kruti	Vijaya R	Srikanth M	For Approval	Approved and Baselined.

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com

The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.