TRIANZ℠

RISK AND OPPORTUNITY MANAGEMENT POLICY

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

The purpose of this policy is to establish a process for the identification, evaluation quantification, prioritization and mitigation/elimination or control of all risks and Opportunities associated with Trianz's software delivery projects, ESS projects, corporate and business functions.

Organization shall institute periodic reviews and risk and opportunity assessments based on risks and opportunities identified across the organization

The purpose of employing risk management shall be to institute mitigation and contingency plans and identify opportunities from risks that shall ensure planned and deployed measures to meet the goals and objectives of the Organization and compliance with the laws, regulations, policies and standards

2. Scope of the Policy

The successful implementation of the Risk and Opportunity Management Policy requires a consistent and systematic approach to risk and opportunity management at all levels of Trianz's operations. Scope of the policy is as follows.

- Risk Assessment shall be carried out for Information assets for All Trianz Service delivery pertaining to all engagement models, commercial models and Technologies (CADIS)
- Risk assessment shall be carried across all Corporate functions
- Risk Assessment shall be carried out on ongoing basis
- Risk Assessment shall involve the steps – Risk Identification, Risk analysis and Evaluation of Risk and Risk Monitoring
- Maintain a Risk Log that shall be updated on continuous basis
- Categorization of Risks shall be Business, Client, Operational, Regulatory & Standards and Delivery.
- Trianz is compliant with the ISO 9001:2015 , ISO 20000-1:2018 Standards and will strive to adhere to ISO 31000- Risk Management guidelines
- Inputs for risks identification will be from Stakeholders, various Project/ Business Unit's Operational Issues, Non-conformities/Observations reported during Internal and external
- Audits, Client Audits, Resource Management issues, Schedule and Effort Deviations, Quality issues etc.
- Identify Opportunity to be explored (wherever applicable) from the uncertainty, treat them as appropriate and monitor them

3. Definitions/Abbreviations/Acronyms

- Organization shall implement policies, associated procedures that identify the risks across the Projects, Corporate functions and Business functions
- Organization shall adopt Risk Management (Risk Assessment ,Risk Analysis and Evaluation, Analysis & Treatment) procedures that implement necessary mitigation/ Contingency measures to mitigate the impact to an acceptable level
- Risk Management shall comprise the following steps:
- **Risk Identification:**
  a) PM identifies the risks right from Proposal/Contract Phase till the Deployment/UAT for the Projects.
  b) Risk identification is an ongoing activity for Business /Corporate Functions
- **Risk Analysis, Evaluation and Treatment:** Each identified risk shall be analyzed for its acceptability in the project. Risk Magnitude shall be calculated based on the impact and probability of each risk in the project
  - Risks shall either be avoided, transferred or mitigated
  - Risks shall be avoided by completely eliminating the probability of occurrence
  - Risks shall be transferred when negative impact is shifted to a third party
  - Risks shall be mitigated to proactively change the plan to minimize the probability of the risk occurring, (however the residual risk remains)
  - Residual risks shall be verified for the acceptable levels of risk magnitude < =9
  - Risk Mitigation and Contingency: For all risks, where risk magnitude > =27, considered as high and mitigation plan(s) shall be implemented
  - Contingency Plans shall be applied for the risks already occurred.
- **Risk Monitoring:** Risks shall be monitored on monthly basis during SMRs
  - Verification of Mitigation and contingency done during DA reviews and SMR Reviews
  - Ensuring Verification of new additional risks and also mitigation plans on continuous basis
  - Opportunities: Opportunities are to be identified and explored as and when feasible, treated as appropriate and the same shall be monitored
  - Maintenance of a Risk and Opportunity Log as part of the Project Management Workbook and SMR for Projects and a Separate Risk Log of All Business functions and Corporate functions

- Risks identified are tracked through Enterprise Risk Management Tool

4. Roles and Responsibilities

Serial Number.	Roles	Responsibilities
1	Risk and Opportunity Owners (Function Owners/SPOCs/	Identify Risks and Opportunities at enterprise level, function level, project level etc. basis the inputs from all stake holders
	DM/PM (in case of Projects and support functions)	• Identify the risks related to Quality Management System, Informationsecurity, Cloud Security and DataPrivacy • Review the risks periodically • Analyze and evaluate the risks and Incorporate the review comments • Treating the risks based on the Magnitude and impact of Risks. • Monitoring the risks on periodicbasis. • Identify the lessons learned from the History/Repository of Risks I.e. Derived from previous Risk Treatment /Contingency plans • Updating new risks identified, onperiodic basis. • Identify and monitor the opportunities to be explored **Note:** In case of Projects, identification,review, treat and analyze the risks rightfrom Proposals to Closure of the Project
2	Risk Stakeholders	• Participates in Risks identification, Treatment and Monitoring) and • identification of Opportunities
3	DA / Infosec Team / PMO	• Ensure that the risks are identified, assessed, treated and monitored and analysis • (DA for projects, PMO/Infosec for Overall Risks across Trianz) • Identification of Opportunities

5. Review and Reporting

- Risks maintained in Project Management Workbook/SMR Deck(Enterprise Risk Management Tool) shall be reviewed by Senior Leadership team monthly and verified for necessary mitigation/contingency as part of Risk monitoring
- Risk and Opportunities register maintained by business functions and corporate functions shall be reviewed by the respective Senior Leadership team on quarterly basis and verified for necessary mitigation/contingency as part of Risk monitoring

Section B

6. Information Security Risk and Opportunity Management Policy:

6.1 Purpose of Information Security Risk and Opportunity Management Policy:

- To establish a process to detect, diagnose, mitigate and manage information security risks of the organization that results in threats to the confidentiality, integrity and availability of "Trianz project Assets, client Supplied Items, Trianz and Clients Data Privacy and Information Systems".
- This policy shall articulate requirements for performing annual reviews of' IT (Information Technology) assets, determining appropriate data classifications and controls, and assessing and reacting to risks in order to safeguard those assets.
- Information Security Team shall institute periodic reviews and risk assessments based on changes in the IT environment including new threats, vulnerabilities and consequences to ensure the continued effectiveness of the implemented controls.
- Identify Opportunities to be explored, treat them as appropriate and monitor them
- The purpose of employing such a process shall be to institute remediation where warranted to reasonably ensure that planned and deployed controls meet the security goals of the Organization.

- This includes compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information (PI).

6.2 Scope:

- This policy applies to all IT information assets i.e. electronic data collected, created, stored, processed, backed up, retained, restored, transmitted and received by the Organization to and from its client and or third parties.
- InfoSec Risk Assessment shall be carried out for Information assets for All Trianz Service delivery pertaining to all engagement models, commercial models and Technologies (CADIS)
- InfoSec Risk assessment will be carried out for all Information Assets of Corporate functions
- Risk Assessment shall be carried out on ongoing basis
- Risk Assessment shall involve the steps of – Risk Identification, Risk analysis and Evaluation and Risk Monitoring
- Maintain a Risk log that will be updated on continuous basis
- Identify the Opportunity to be explored, treat them as appropriate and monitor them
- Sources for organizational risk will be detected from Standards and Regulatory Requirements- ISO 27001, ISO 27017, ISO 27018, ISO 27701, GDPR, SOC1 Type1 & II.

6.3 Trianz's InfoSec Risk Management Policy Statement

- Organization shall implement, detect, diagnose, mitigate and manage information security risks of the organization that results in threats to the confidentiality, integrity and availability of "Trianz project Assets, client Supplied Items, Trianz and Clients Data Privacy and Information Systems
- Organization shall adopt Risk Management (Risk Assessment Analysis and Evaluation, analysis & Treatment) procedures that implement necessary mitigation/ Contingency measures to mitigate the impact to an acceptable level

- Organization shall implement Asset Management procedures including inventory of identified IT assets, ownership and business value of those assets, and information classification of the assets.
- Risk Management shall comprise the following steps:
  - Risk assessment and identification:
    - PM/IT Team shall identify Project Assets, Client Supplied Assets, Trianz and Clients Data Privacy and Information Systems.
    - Corporate functions shall identify their Information assets – Tools, Standards and Resources etc. including Supplier provided assets
    - Threats and Vulnerabilities shall be identified against the Assets
    - Identification of the consequences that losses of confidentiality, integrity and availability may produce
    - Identification of the controls and their status, as either existing or planned
    - Risk Analysis, Evaluation and Treatment
    - Each identified risk shall be analyzed for its acceptability in the project. Risk Magnitude shall be calculated based on the impact, probability and vulnerability of each risk in the projector corporate function (Risk magnitude – Vulnerability*Probability*Impact)
    - Risks shall either be avoided, transferred or mitigated or managed
    - Risks shall be avoided by completely eliminating the probability of occurrence
    - Risks shall be managed to choose the acceptance of risk
    - Risks shall be transferred when negative impact is shifted to a third party
    - Risks shall be mitigated to proactively change the plan to minimize the probability of the risk occurring by applying necessary controls, (and the residual risk remains)
    - Residual risks shall be verified for the acceptable levels of risk magnitude < =9
    - Risk Mitigation and Contingency: For all risks, where risk magnitude > 27, considered as high and mitigation plan(s)/Security Controls shall be implemented

- Contingency Plans/Security Controls shall be applied for the risks already occurred.

- Risk Monitoring:
  - Risks shall be monitored monthly during SMRs
  - Verification of Mitigation and contingency done during DA reviews and SMR Reviews
  - Ensuring Verification of new additional risks and also mitigation plans/controls on continuous basis
  - Maintenance of a Risk Log as part of the Project Management Workbook and SMR for Projects and a Separate Risk Log of All Business functions and Corporate functions

- Identification of Opportunities: Identify Opportunity to be explored (wherever applicable) from the uncertainty, treat them as appropriate and monitor them

7. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Clause	8.3 Information security risk treatment	Risk and opportunity Management Policy

Document Control

Owner:	CISO	**Release ID:**	RMP-POL-045

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	22-Jun-18	Vijaya Rajeswari				**None**
1.00	22-Jun-18	Vijaya Rajeswari	Bharati, Balu, Kamadev	Ganesh Arunachala	Risk Management Policy created for Trianz for Projects and Infosec	**Baselined**
1.1	6-May-2020	Vijaya Rajeswari	Karthik, Balu		For Review	**Logo and Information Classification Updated Migrated to the new template**
2.0	15-May-2020	Vijaya Rajeswari	Karthik, Balu	Phani Krishna	For Approval	**Approved and Baselined**

2.1	19-May-20	Karthik N	Srilakshmi		Review comments from DA	**Added Roles and Responsibilities.**
3.0	19-May-20	Karthik N	Anitha Ravindran	Phani Krishna	For Approval	**Approved and Baselined**
3.1	28-Jan-21	Vijaya Rajeswari	Phani Krishna		For Review	**Risk Management Policy aligned to ISO 27701 and ISO 20000-1:2018 Standards**
4.0	28-Jan-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
4.1	25-Mar-21	Divya	Balu & Vijaya	Phani Krishna	For review and approval	Risk Management policy updated as Risk Management and Opportunity Policy
5.0	28-Jan-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
5.0	5-Jan-2022	Divya	Balu & Vijaya		For review	No changes
5.1	24-Apr-2022	Vijaya	Balu	Siva ramakrishna	For Review	Residual risk acceptable limit in policy and procedure are aligned
6.0	29-Apr-2022	Vijaya	Balu	Siva ramakrishna	For Approval	Approved and Baselined
6..1	10-Mar-2023	Beniyel S, Rama Madhavan	Balu N		For review	No change Migrated to new template
7.0	09-May-2023	Beniyel S	Balu N	Srikanth M	For Approval	Approved and Baselined

7.1	11-Feb-24	Shalini	Vijaya	Srikanth M	For review	Mapped to new ISO 27k 2022 Controls
8.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined
8.1	30-Apr-25	Kruti	Vijaya R		For Annual Review	Migrated to a new Template and Yearly Review
9.0	14-May-25	Kruti	Vijaya R	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com