TRIANZ℠

RISK AND OPPORTUNITY MANAGEMENT

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. INTRODUCTION **5**

2. ACRONYMS/ABBREVIATIONS **5**

3. OBJECTIVE(S) **5**

4. SCOPE **6**

5. ROLES & RESPONSIBILITIES **6**

6. ENTRY CRITERIA **7**

7. INPUT **8**

8. PROCESS DESCRIPTION - PROJECTS **8**

8.1 Risk Identification -Projects 8

8.2 Risk Analysis & Evaluation 9

8.3 Risk Treatment 10

8.4 Risk Monitoring 10

8.5 Identification of Opportunities 11

9. PROCESS DESCRIPTION – ASSET RISK MANAGEMENT **11**

9.1 Identification Asset Category and Types 12

9.2 Identification of CIAP values and Calculation of Asset Value 13

9.3 Risk Assessment Methodology 15

9.4 Risk acceptance level 15

9.5 Risk treatment 15

9.6 Review of risk assessment 17

9.6.1 Risk assessment, risk acceptance level and residual risks are reviewed yearly once, taking into account changes to: 17

9.7 Identify Opportunities 17

10. OUTPUTS **17**

11. EXIT CRITERIA **18**

12. RELATED GUIDELINES, TEMPLATES AND CHECKLISTS **18**

13. MEASUREMENT **18**

14. STANDARDS ADDRESSED 18
15. ISO CONTROL MAPPING(S) 18
16. APPENDIX A: RISK SOURCES 19
17. APPENDIX A: LIST OF THREATS 21
18. APPENDIX B: LIST OF VULNERABILITIES 22
19. APPENDIX C: MAPPING THREATS TO VULNERABILITIES 24

1. Introduction

Risk and Opportunity Management Process is a continuous and proactive process, in which risks and opportunities are identified, assessed, prioritized, and if necessary, actions to control them are implemented

2. Acronyms/Abbreviations

Acronym/Abbreviation	Expansion
PM	Project Manager
TM	Team Member
DA	Delivery Assurance
Function SPOC	Function – Single Point of Contact
DH	Delivery Head
STK	Stakeholders
SOW	Statement of Work

3. Objective(s)

The Objectives of Risk Management procedure are as follows

- Identify, Assess and Quantify & Evaluate the risks
- Develop risk treatment and contingency plans
- To prevent causes of risk that could result in significant harm or loss to the organization objectives, delivery objectives, quality objectives, security objectives, privacy objectives etc.
- Identify the Opportunities to be explored

4.Scope

The Scope of the Risk management process includes

- Risk Identification
- Risk Analysis & Evaluation
- Risk Treatment
- Risk Monitoring
- Risk Mitigation and Contingency
- Identify the Opportunity from the uncertainties.

5.Roles & Responsibilities

Roles	Responsibilities	Internal/External
Risk Owners (Function Owners/SPOCs/ (in case of Projects- DM/PM)	• Identify Risks at enterprise level, function level, project level etc. basis the inputs from all stake holders • Identify the risks related to Quality Management System, Service Management System, Information security, Cloud Security and Data Privacy • Review the risks periodically • Analyse and evaluate the risks and Incorporate the review comments • Treating the risks based on the Magnitude and impact of Risks. • Monitoring the risks on periodic basis. • Identify the lessons learned from the History/Repository of Risks i.e. Derived from previous Risk Treatment /Contingency plans • Updating new risks identified, on periodic basis	Internal & External

	Note: In case of Projects, identification, review, treat and analyze the risks right from Proposals to Closure of the Project	
Risk Stakeholders	• Participates in Risks identification, Treatment and Monitoring	Internal/External
DA /Infosec Team/PMO	• Ensure that the risks are identified, assessed, treated and monitored and analyzed (DA for projects, PMO/Infosec for Overall Risks across Trianz)	Internal

6. Entry Criteria

a) For Projects:

Proposal and SOW preparation

Project Initiated, Planning, Execution, Monitoring &Control PM workbook preparation

b) For Functions:

Ongoing basis

c) Risk owners identified for Projects/Functions

7. Input

- Client Contract risks
- Compliance (regulatory and other) risks
- Business continuity risk including IT failure risk.
- Price risk
- Technology Risks
- Quality Management Risks- Schedule, Effort, Quality, Scope, Cost, Resources etc.

8. Process Description - Projects

8.1 Risk Identification -Projects

The risk is a result of a threat actor exploiting the vulnerability present in the system/Project

- Risk identification is an on-going activity across Trianz
- Risks will be identified basis the inputs from all stakeholders
- Risks would be updated in Weekly PMO Tool/Risk Management Module and monitored by PMO /DA and Infosec Team on periodic basis.
- Risks would be identified based on the impact that would be created on Quality Management System, Service Management System, Information Security including Cloud Security and Data Privacy.
- The details associated with each risk are filled in the Risk Management Register
- Risks Specific to Quality Management System and Service Management System would be identified in the following ways:
    - Impact on Scope, Schedule & Effort o Impact on Quality & Cost o Impact of New Technologies o Impact on Resources – Skills etc.
- Risks Specific to Service Management System would be identified in the following ways:

- Risks due to External issues that include market, political, economic, and environmental influences, competition, laws and regulations, external customer demands, and the likelihood of events that could affect the services.
- Risks due to Internal issues that include policies, resources, capabilities, people, skills and knowledge, organizational structure, governance, culture, internal customer demands, and finance

- Refer Risk Sources –Appendix

8.2 Risk Analysis & Evaluation

- Risk owner would analyze the risks.
- Risk owner evaluates the risk and assesses the probability & impact of the risk and details them in the Risk Management Register.
- Impact and Probability would be quantified as follows

Impact	Rating (Scale)
High	9
Medium	3
Low	1

Probability	Rating (Scale)
High	9
Medium	3
Low	1

Product of quantified values of Impact and Probability is “Risk Magnitude “ After Risk Analysis & Risk Evaluation, Risk Treatment will follow.

8.3 Risk Treatment

Once Risk Magnitude is calculated, for those risks that have magnitude >=27, Risk Treatment plan, and Risk contingency plan would be identified

Risk owner identifies the Risk Treatment applicable against each risk as per below categories.

Avoid the Risk: Avoid the Risk in case of changing the plan completely

Take on more Risk: Taking or increasing the risk in order to pursue an opportunity;

Remove the Risk Source: By removing the risk source a risk would be modified to the desired level

Change the Probability: Altering or Changing the likelihood could be the best risk treatment option

Alter the Consequences: Altering the outcome or changing the consequences of an event can modify the risk

Share the Risk: Just like a problem shared is half way solved, so also, Sharing the risk with another party or parties, including insurance and other mechanisms could be an effective risk treatment

Implement Controls: Implement suitable controls to mitigate the risk so that the risk value is brought down to the acceptable level

Accept / Retain the Risk: Retaining the risk by informed decision, this is critical when it is about risk-benefit and acceptable for the organization

When the Identified risk already occurred, contingency plan would be executed If there is no residual risk the risk is mitigated

8.4 Risk Monitoring

This involves the implementation and monitoring of appropriate risk response strategies.

When the Identified risk already occurred, contingency plan would be executed and if there is any residual risk after implementing contingency plan, Risk Treatment would be applicable as stated in the above section.

Residual risks shall be verified for the acceptable levels of risk magnitude < =9

If residual risk is meeting the acceptable level the risk is considered as mitigated

The Risk Owner will systematically track the risks identified in the Risk Management Register. Risk Treatment would be monitored periodically.

Risk Management report would be generated and presented to SLT on periodic basis

DA/PMO/Information Security Team verify status of implementation of Risk Treatment and Contingency plans

As Risk Management is an ongoing basis, New risks would be identified and the same would be assessed and monitored in the Risk Management register periodically

The Risk Owner/ will capture lessons learned for future risk assessment using Risk Database I.e. History of Risks

8.5 Identification of Opportunities

Identify any opportunities Opportunity to be explored (wherever applicable) from the uncertainty, treat them as appropriate and monitor them

9. Process Description – Asset Risk Management

Risk identification is an on-going activity for all the assets Risks will be identified basis the inputs from all stakeholders

Risks would be updated in Weekly PMO Tool/Risk and Opportunity Management Module and monitored by PMO /DA and Infosec Team on periodic basis.

Risks would be identified based on the impact that would be created on Information Security including Cloud Security and Data Privacy.

The details associated with each risk are filled in the Risk Management Register

- The risk owner as a "person or entity with the accountability and authority to manage a risk."
- Asset owner to be identified and is the one who would be responsible for protecting the Confidentiality, Integrity, Availability & Privacy (C, I, A, P) of the asset.
- Calculate Asset value based on Confidentiality, Integrity, Availability and Privacy values
- If Asset value is greater than (>=) 81 then perform 'Risk Assessment'
- Identify Threats, Existing Controls, Vulnerabilities, Impact and probability of occurrence of vulnerabilities.
- Risk Magnitude is calculated based on the Impact value and Probability value
- If Risk Magnitude is greater than (>=81) risk should be treated or transferred

  Note: Asset ownership is closer to operational control and risk ownership is more in relation with business risk.

- Risk assessment methodology is explained in the below sections:

9.1 Identification Asset Category and Types

Asset identification will be done based on the asset category; assets are classified as following categories:

- **Information Assets**: Databases and data files, Contracts and agreements, System documentation, Research information, User manuals, Training material, Operational or support procedures, Business continuity plans, Fall-back arrangements, Audit trails, and Archived information
- **Software Assets**: Application software, System software, Development tools, and Utilities, Software Licenses
- **Physical/Hardware Assets/Infra Assets**: Computer equipment, Communications equipment, Removable media, and Other equipment
- **Services**: Computing and communications services, General utilities (e.g. heating, lighting, power, and air-conditioning)

- **Human Resources:** Employees (Qualifications, Skills, and Experience)
- Assets of similar functionality under each category will be taken up to identify assets that are identical in functionality and nature.

9.2 Identification of CIAP values and Calculation of Asset Value

For identified assets provide confidentiality, integrity availability and privacy values

- **Confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**: Property of protecting the accuracy and completeness of assets
- **Availability**: Property of being accessible and usable upon demand by an authorized entity
- **Privacy**: Property of protecting the information about an individual or group to seclude themselves and thereby express themselves selectively (When something is private to a person, it usually means that something is inherently special or sensitive to them)

Following tables will be used to assign the confidentiality, Integrity, Availability and Privacy rating

Confidentiality	
Ratings	**Rating Description**
1	Public to everyone
3	Restricted, available within Trianz but not outside
9	Sensitive Information/ based on need

Integrity	
Ratings	**Rating Description**

1	The unauthorized modification or destruction of the information could be expected to have limited effect on the organizational operations or assets
3	The unauthorized modification or destruction of the information could be expected to have some effect on the organizational operations or assets
9	The unauthorized modification or destruction of the information could be expected to have serious effect on the organizational

Availability	
Ratings	**Rating Description**
1	The disruption of access to or use of the asset could be expected to have limited effect on the organizational operations or assets
3	The disruption of access to or use of the asset could be expected to have some effect on the organizational operations or assets
9	The disruption of access to or use of the asset could be expected to have serious effect on the organizational operations or assets

Privacy	
Ratings	**Rating Description**
1	Non-regulated & Encrypted Privacy information
3	Regulated & Encrypted Privacy information
9	Unencrypted Privacy Information (or) Sensitive Personal Information

The asset value will be identified on the basis of CIAP values (Confidentiality, Integrity, Availability and Privacy) of the assets

Asset Value Calculation	
Asset Value	Confidentiality Rating * Integrity Rating* Availability Rating* Privacy Rating

9.3 Risk Assessment Methodology

- Identify 'Threats' for each asset type such as Fire, Flood, Theft, Building/Structure Collapse, Water Leakage, Non-Availability of Resources such as associates, software/hardware etc.
- Refer list of threats in Appendix A: List of Threats
- Identify 'Existing Controls' for threats
- Identify and map applicable 'Vulnerabilities' to threats
- Refer list of vulnerabilities in Appendix B: List of Vulnerabilities
- Refer Mapping of Vulnerabilities to Threats in Appendix C: Mapping of Vulnerabilities to Threats
- A list of threats will be maintained and updated as necessary.

9.4 Risk acceptance level

- If assets having risk value as (<) less than 81, then those risks are considered as acceptable risks
- If assets having risk value (>=) greater than 81, then it the risk should be considered and must be treated with adequate control implementation

9.5 Risk treatment

- Treatment of risk will be undertaken subject to the following conditions:
- If risk value is greater than (>=) 81 and above the risk will be treated or transferred

- Subsequent to the above, Vulnerabilities will be identified for the identified assets
- Against the vulnerabilities identified for each asset, a set of threats that can exploit the vulnerabilities will then be identified.
- Based on threat, vulnerabilities and existing controls, provide values for 'Impact' and 'Probability'
- Probability is the measure of the likelihood that a threat will be able to exploit a given Vulnerability
- Impact is the measure of the adversity of a security event that can be described in terms of loss or degradation of any, or a combination of any, of the four security goals - CIAP (confidentiality, Integrity, availability and Privacy)
- The function of Impact * Probability gives risk magnitude
- For all risks, where risk magnitude > 27, considered as high and mitigation plan(s)/Security Controls shall be implemented
- Based on the risk magnitude, Risk Handling Options will be selected
- Risk Handling Options will be 'Avoid Risk', 'Accept Risk', 'Transfer Risk' and 'Treat Risk'
- On implementation of proposed controls, provide impact and probability values
- The risk magnitude i.e. product of Impact & Probability gives residual risk after implementing the controls
- Residual risks shall be verified for the acceptable levels of risk magnitude < =9
- The respective project manager and/or the Function Head will be the owner of risk.
- Information security and Business continuity risks shall be identified and recorded in the PM workbook /PMO Tool
- Respective project level risks shall be reviewed as part of the PM & DM Reviews and DA Check Points and Toll Gates.
- Report of high risk items, if any, shall be presented in the SMR by the PM.
- A consolidated report of high risk items shall be presented in QBR by PMO.

9.6 Review of risk assessment

9.6.1 Risk assessment, risk acceptance level and residual risks are reviewed yearly once, taking into account changes to:

- The organization
- Technology
- Business objectives and processes
- Identified threats
- Effectiveness of the implemented controls
- External events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate
- The below factors are also considered during risk assessment:
    - o Addition/deletion/changes in assets
    - o Results of BCP tests
    - o Vulnerability assessment and Penetration test results
    - o Information security incidents occurred

9.7 Identify Opportunities

Identify opportunities Opportunity to be explored (wherever applicable) from the uncertainty, treat them as appropriate and monitor them.

10. Outputs

- Risk Management Register updated in PMO Tool-Risk and Opportunity management/ Risk Register

11. Exit Criteria

- Risks are identified, analyzed, prioritized and mitigated
- Risk Treatment plans are defined and implemented

12. Related Guidelines, Templates and Checklists

Document Name
Risk Register in Project Team site
Risk Management Plan Template & Asset risk Management Template in PMWB

13. Measurement

None

14. Standards Addressed

- ISO 9001:2015 Standard
- ISO 27001:2013 Standard
- ISO 27017:2015, ISO 27018:2019 Standards
- ISO 20000-1:2018 Standard
- ISO 27701:2019 Standard

15. 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 Procedure

16. Appendix A: Risk Sources

List of Risk Sources	
S. No	**Risk Sources**
1	Unauthorized access to the information system
2	Disposal of storage media without deleting data
3	Equipment sensitivity to changes in voltage
4	Equipment sensitivity to temperature
5	Inadequate cabling security
6	Inadequate capacity management

List of Risk Sources	
S. No	**Risk Sources**
7	Inadequate change management
8	Inadequate classification of information
9	Inadequate control of physical access
10	Inadequate maintenance
11	Inadequate network management
12	Inadequate or irregular backup
13	Inadequate password management
14	Inadequate replacement of older equipment
15	Inadequate security awareness
16	Inadequate segregation of duties
17	Inadequate segregation of operational and testing facilities
18	Inadequate security training

19	Incomplete specification for software development
20	Insufficient software testing
21	Lack of access control policy
22	Lack of clear desk and clear screen policy
23	Lack of procedure for removing access rights upon termination of employment
24	Lack of protection for mobile equipment
25	Location vulnerable to flooding
26	Poor selection of test data
27	Uncontrolled download from the Internet
28	Unmotivated employees
29	Unprotected public network connections
30	User rights are not reviewed regularly
31	Inadequate supervision
32	Equipment sensitivity to humidity
33	Unstable Power Grid
34	Uncertain requirements
35	Unprecedented efforts (i.e., estimates unavailable)

List of Risk Sources	
S. No	**Risk Sources**
36	Infeasible design
37	Competing quality attribute requirements that affect solution selection and design
38	Unavailable technology
39	Unrealistic schedule estimates or allocation
40	Inadequate staffing and skills
41	Cost or funding issues

42	Uncertain or inadequate supplier capability
43	Inadequate communication with actual or potential Clients or with their representatives
44	Regulatory constraints (e.g. security, Privacy, safety, environment)
45	Data Privacy Risks
46	Risks related to the following Contract / SOW Client stimation Requirements Design Coding Testing Delivery Schedule risks, Resource risks (Non-availability of Hardware/Software/Skills)
47	Any Risks related to Cloud Security
48	Risks related to Service Management System

17. Appendix A: List of Threats

List of Threats	
S. No	**Threats**
1	Theft
2	Fire
3	Floods
4	Building /Structure Collapse
List of Threats	
S. No	**Threats**
5	Water Leakage
6	Explosion

7	Riots
8	Strikes
9	Power failures
10	Terrorist Attacks
11	Lightning
12	Operational Errors
13	Humidity
14	Extreme Temperatures
15	Physical intrusion
16	Third party personnel
17	Misuse of resources
18	Power fluctuations
19	Obsolescence (life of asset)
20	Inappropriate / Unauthorized movement of assets
21	Virus attacks
22	Malicious software
23	Inadequate licenses
24	Use of unauthorized software

18. Appendix B: List of Vulnerabilities

List of Vulnerabilities	
S. No	**Vulnerabilities**
1	Unauthorized access to the information system

2	Disposal of storage media without deleting data
3	Equipment sensitivity to changes in voltage
4	Equipment sensitivity to temperature
5	Inadequate cabling security
6	Inadequate capacity management
7	Inadequate change management
8	Inadequate classification of information
9	Inadequate control of physical access
10	Inadequate maintenance
11	Inadequate network management
12	Inadequate or irregular backup
13	Inadequate password management
14	Inadequate replacement of older equipment
15	Inadequate security awareness
16	Inadequate segregation of duties
17	Inadequate segregation of operational and testing facilities
18	Inadequate security training
19	Incomplete specification for software development
20	Insufficient software testing
21	Lack of access control policy
22	Lack of clear desk and clear screen policy
23	Lack of procedure for removing access rights upon termination of employment

24	Lack of protection for mobile equipment
25	Location vulnerable to flooding

List of Vulnerabilities	
S. No	**Vulnerabilities**
26	Poor selection of test data
27	Uncontrolled download from the Internet
28	Unmotivated employees
29	Unprotected public network connections
30	User rights are not reviewed regularly
31	Inadequate supervision
32	Equipment sensitivity to humidity
33	Unstable Power Grid

19. Appendix C: Mapping Threats to Vulnerabilities

Mapping of Threats & Vulnerabilities		
S. No	**Threats**	**Vulnerabilities**
1	Theft	Inadequate control of physical access
		Inadequate security awareness
		Inadequate security training
		Inadequate supervision
		Lack of procedure for removing access rights upon termination of employment
2	Fire	Inadequate cabling security
		Inadequate security awareness
		Inadequate security training

		Inadequate supervision
3	Floods	Location vulnerable to flooding
4	Building /Structure Collapse	None

Mapping of Threats & Vulnerabilities		
S. No	**Threats**	**Vulnerabilities**
5	Water Leakage	Inadequate supervision
		Inadequate maintenance
6	Explosion	Inadequate security awareness
		Inadequate security training
		Inadequate control of physical access
7	Riots	Inadequate control of physical access
8	Strikes	Inadequate control of physical access
9	Power failures	Unstable Power Grid
		Inadequate cabling security
		Inadequate maintenance
10	Terrorist Attacks	Inadequate control of physical access
11	Lightning	Inadequate supervision
		Inadequate maintenance
12	Operational Errors	Equipment sensitivity to changes in voltage
		Equipment sensitivity to temperature
		Inadequate cabling security
		Inadequate change management
		Inadequate classification of information
		Inadequate segregation of operational and testing facilities
		Incomplete specification for software development

		Insufficient software testing
		Poor selection of test data
		Unauthorized access to the information system
		Inadequate maintenance
		Inadequate supervision

Mapping of Threats & Vulnerabilities		
S. No	**Threats**	**Vulnerabilities**
13	Humidity	Equipment sensitivity to humidity
		Inadequate supervision
		Inadequate maintenance
14	Extreme Temperatures	Equipment sensitivity to temperature
		Inadequate supervision
		Inadequate maintenance
15	Physical intrusion	Inadequate control of physical access
		Inadequate security awareness
		Inadequate security training
		Lack of procedure for removing access rights upon termination of employment
16	Third party personnel	Unauthorized access to the information system
		Lack of procedure for removing access rights upon termination of employment
		Lack of access control policy
		Inadequate security training
		Inadequate supervision
		Inadequate control of physical access
17	Misuse of resources	Unauthorized access to the information system
		Lack of access control policy

		Uncontrolled download from the Internet
		Inadequate security awareness
		Inadequate security training
18	Power fluctuations	Unstable Power Grid
		Inadequate maintenance
19	Obsolescence (life of asset)	Inadequate replacement of older equipment
		Inadequate supervision
		Inadequate maintenance

Mapping of Threats & Vulnerabilities

S. No	Threats	Vulnerabilities
20	Inappropriate / Unauthorized movement of assets	Inadequate security awareness
		Inadequate security training
		Inadequate supervision
21	Virus attacks	Uncontrolled download from the Internet
		Inadequate security awareness
		Inadequate security training
		Inadequate network management
22	Malicious software	Uncontrolled download from the Internet
		Inadequate security awareness
		Inadequate security training
		Inadequate network management
23	Inadequate licenses	Inadequate security awareness
		Inadequate security training
		Inadequate capacity management

		Inadequate supervision
24	Use of unauthorized software	Inadequate security awareness
		Inadequate security training
		Inadequate supervision
		Uncontrolled download from the Internet
		Lack of access control policy
25	External Hacking	Inadequate network management
		Uncontrolled download from the Internet
		Inadequate security training
		Inadequate security awareness
		Inadequate supervision
26	Network congestion	Inadequate maintenance

Mapping of Threats & Vulnerabilities		
S. No	**Threats**	**Vulnerabilities**
		Inadequate network management
		Inadequate supervision
		Inadequate security awareness
		Inadequate capacity management
		Inadequate security training
27	Incorrect disposal of assets	Disposal of storage media without deleting data
		Inadequate security awareness
		Inadequate security training
		Inadequate change management

28	Incompatible software	Insufficient software testing
		Poor selection of test data
		Inadequate segregation of operational and testing facilities
		Inadequate supervision
29	Internal hacking	Inadequate network management
		Uncontrolled download from the Internet
		Inadequate security training
		Inadequate security awareness
		Inadequate supervision
		Lack of access control policy
30	Denial of service	Lack of access control policy
		Unmotivated employees
		Inadequate network management
31	IPR violation	Unauthorized access to the information system
		Uncontrolled download from the Internet
		Inadequate security training
		Inadequate security awareness

Mapping of Threats & Vulnerabilities		
S. No	**Threats**	**Vulnerabilities**
		Lack of access control policy
32	Non-compliance to statutory requirements	Inadequate supervision
		Unauthorized access to the information system
		Inadequate security training
		Inadequate security awareness
33	Violating privileges	Inadequate supervision
		Inadequate security training
		User rights are not reviewed regularly

34	Disgruntled employees	Unauthorized access to the information system
		Inadequate supervision
		Lack of procedure for removing access rights upon termination of employment
		User rights are not reviewed regularly
35	Unauthorized access to the information system	Inadequate network management
		Lack of procedure for removing access rights upon termination of employment
		User rights are not reviewed regularly
		Inadequate security training
		Inadequate security awareness
36	Interruption of business processes	Inadequate control of physical access
		Inadequate security awareness
		Inadequate security training
		Inadequate supervision
		Lack of procedure for removing access rights upon termination of employment
		Inadequate cabling security
		Unstable Power Grid
		Inadequate maintenance
		Uncontrolled download from the Internet
		Inadequate network management

Document Control

Owner:	CISO	**Release ID:**	RMP-PROC-0034

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
1.00	07-Sep-12	Sriramya	_	_	CMMI Gap Analysis V1.3	• Initial Version to Blue Book
2.0	20-May-15	Sudharsana	_	_	ISO 27001:2013 Gap Analysis	• Modified Risk Identification section 5.1, Identification of risk related to Information security **Appendix A:** Risk Sources and Risk Categories
2.1	5-Oct-16	Sudharsana	_	_	Risk Management plan is modified	• Modified Risk • Analysis & Evaluation section • Measurement section Replaced SQA with DA
2.2	05-Oct-16	Sudharsana	_	_	Reviewed by Vijaya	• Reframed sentence formation
3.0	05-Oct-16	Sudharsana	_	_	Reviewed and approved	• Baselined

3.1	17-Nov-17	Sudharsana	Vijaya		SEPG review	• Updated the document against the PCR 68 – Classification of Documents against ISMS controls, PCR 24 for updates in Revision History
4.0	17-Nov-17	Sudharsana		Ganesh		• Approved
5.0	30-Sep-19	Danabal Ramakirouchenane	Anitha, Phani	Vivek Sambasivam	Risk Management Process Revision	• Risk Management Flow update • Risk Management Register in SharePoint Team Site • Added Residual Risk • Data Privacy Risk elements added in Section 5.1
6.0	29-Nov- 19	Vijaya Rajeswari	Balu & Phani Krishna	Vivek Sambasivam	Updated to align to ISO 27017 and 27018 standards	• Updated to align to ISO 27017 and 27018 standards and updated Risk Treatment Section • Roles and responsibilities updated to align to Current Organizational Structure Measurements updated
6.1	12-May- 20	Vijaya Rajeswari	Balakrishnan Nai	-	For Review	• Document updated with new Template

			r, Anitha Ravindran , Karthik Narasimh a			
7.0	14-May- 20	Vijaya Rajeswari	Balakrishn an Nai r, Anitha Ravindran , Karthik Narasimh a	Phani Krishna	For Approval	• Approved and Baselined
7.1	28-May- 20	Vijaya Rajeswari	Balakrishn an Nair		Inputs from External Audit	• Risk Management Procedure updated against the findings from External audit by TUV in May 2020.
8.0	3-Jun-20	Vijaya Rajeswari	Balakrishn an Nair	Phani Krishna	For Approval	• Approved and Baselined
8.1	24-Jan- 21	Vijaya Rajeswari	Balakrishn an Nair		For Review	• Information Classification updated • Updated Risk Management Procedure complying to ISO 20000-1:2018 and ISO 27701:2019 Standard
9.0	24-Jan- 21	Vijaya Rajeswari	Balakrishn an Nair	Phani Krishna	For Approval	• Approved and Baselined
9.1	24-Mar- 21	Vijaya Rajeswari	Balakrishn an Nair		For review	• Risk Management is updated as Risk and Opportunity Management

						Updated the procedure with Opportunities
10.0	24-Mar- 21	Vijaya Rajeswari	Balakrishnan Nair	Phani Krishna	For approval	• Approved and Baselined
10.1	5-May-21	Vijaya Rajeswari, Divya Gongalla	Balakrishnan Nair	Phani Krishna	For review	• Threat and Vulnerabilities section removed and updated in Risk Assessment and Risk Treatment Sections
11.0	5-May-21	Vijaya Rajeswari, Divya Gongalla	Balakrishnan Nair	Phani Krishna	For approval	• Approved and Baselined
11.0	5-Jan-22	Divya	Balu & Vijaya		For review	• No changes
11.1	24-apr-22	Vijaya	Balu	Siva Rama Krishnan	For Review	• Residual risk acceptable limit in policy and procedure are aligned, for Review and approval
12.0	24-apr-22	Vijaya	Balu	Siva Rama Krishnan	For Approval	• Approved and Baselined
12.0	10-Mar-23	Beniyel S, Asha Veeramallu	Balu N		For Review	New template change
12.0	09-May-23	Beniyel S	Balu N	Srikanth M	For Approval	Approved and Baselined
12.1	11-Feb-24	Shalini	Vijaya	Srikanth M	For Review	Mapped to new ISO 27k 2022 Controls
13.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined

13.1	30-Apr-25	Kruti	Vijaya R		For Annual Review	Migrated to a new Template and Yearly Review
14.0	14-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com