TRIANZ℠

ISAC Roles and Responsibilities

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 4

2. OBJECTIVES 4

3. ORGANIZATION CHART 6

3.1 Information Security and Data Privacy Assurance 6

4. INFORMATION SECURITY ASSURANCE COUNCIL ROLES, RESPONSIBILITIES AND AUTHORITIES. 6

4.1 ISAC Group 6

4.2 Chief Information Security Officer (CISO) / Chief Data Privacy Officer (CDPO) 7

4.3 Information Systems & Business Resilience Team 7

4.4 HR & Recruitment Team 8

4.5 Professional Development (End User Training) 8

4.6 Admin Team 8

4.7 Information Security and Data Privacy Assurance Group 9

4.8 Travel Team 9

4.9 Delivery and DA Team 9

4.10 Legal Team 9

4.11 Finance and Purchase Team 10

4.12 Marketing Team 10

4.13 Platforms Team and Platforms Assurance Team 10

5. OUTPUTS 10

6. EXIT CRITERIA 10

7. PROCESS ASSETS 11

8. MEASUREMENT 11

9. ISO CONTROL MAPPING(S) 11

1. Introduction

The ISAC is a representation of the people from relevant functions and business units and will meet every quarterly to review the status and effectiveness of ISMS implementation.

2. Objectives

- Ensure that organization's Information Security Management System is established, implemented, maintained and improved.
- Demonstrate Organization's commitment in securing Organizational and Client's Information Assets against vulnerabilities and threats
- Ensure that all personnel shall apply information security in accordance with Information Security Management system framework.
- Ensure that management's responsibilities include that all personnel
- Are properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets;
- Are provided with guidelines which state the information security expectations of their role within the organization.
- Are mandated to fulfil the information security policy and topic-specific policies of the organization
- Achieve a level of awareness of information security relevant to their roles and responsibilities within the organization
- Compliance with the terms and conditions of employment, contract or agreement, including the organization's information security policy and appropriate methods of working.
- Continue to have the appropriate information security skills and qualifications through ongoing professional education.

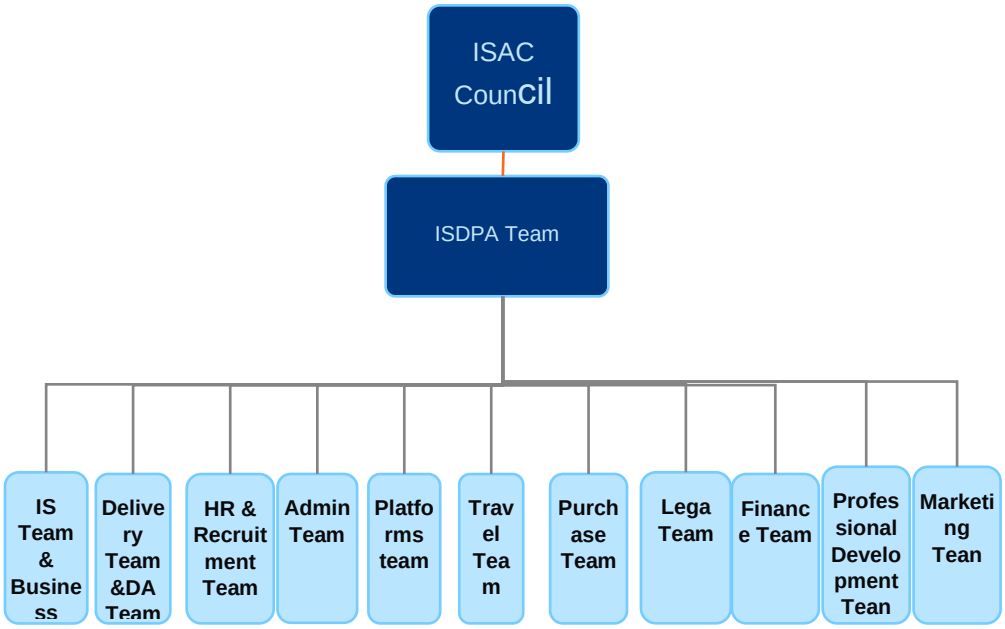
- Where practicable, are provided with a confidential channel for reporting violations of information security policy, topic-specific policies or procedures for information security ("whistleblowing"). This can allow for anonymous reporting, or have provisions to ensure that knowledge of the identity of the reporter is known only to those who need to deal with such reports
- Are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.

Definitions/Abbreviations/Acronyms

Word	Definitions
ISMS	Information Security Management System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISM	Information Systems Manager
CMT	Crisis Management Team
IP	Internet Protocol

3. Organization Chart

3.1 Information Security and Data Privacy Assurance



4. Information Security Assurance Council Roles, Responsibilities and Authorities.

4.1 ISAC Group

The members of this group will convene Bi-Annual to discuss on the following:

- Status of the implementation of the Information security policies and procedures
- Security incidents reported and the resolution.
- Observed non-compliances to the Information Security Policy
- Compliance with Policy and Procedures of Trianz

- Discuss current and emerging threats relevant to the organization.
- Review the Risk Assessment and update the controls as needed.
- Include risk owners in the ISAC group discussions to ensure aligned understanding and acceptance.
- Additional security requirements that require changes in the Information Security Policy
- Ensuring that personnel are aware of the Information Security Policy

4.2 Chief Information Security Officer (CISO) / Chief Data Privacy Officer (CDPO)

Ensures the Overall responsibility of Information/Cyber Security , Privacy and Sustainability for Trianz and sets clear vision, mission, and direction to Infosec, Data Privacy and Sustainability Assurance Team

4.3 Information Systems & Business Resilience Team

- Shall be responsible for Security Posture for the organization
- Improvements/Initiatives from IS operations w.r.t Security Posture
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management Systems
- The Business Resiliency team focuses on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations, and communications.

4.4 HR & Recruitment Team

- Conduct and manage the schedule of Information Security and Data Privacy Awareness Training for the new hires at the time of their induction training/ orientation program
- and employee/ Candidates' data is well protected w.r.t Data at Rest and Data in Transit , NDA and BGV
- Disciplinary action against any Infosec and Privacy Violations
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System

4.5 Professional Development (End User Training)

Prepare an overall plan for internal training as per the requirements of the organization, in line with the ISMS and, and send to Head – Human Resources for approval.

- Plan, organize and monitor training program.
  Prepare annual budget for conduction of training.
- Locate and evaluate suitable faculty (internal or external), for training.
- Publish Training Calendars
- Prepare and send to ITSM and Head - Human Resources periodic reports on training activities planned / executed.
- Constantly monitor effectiveness of training activities against expectations of Trianz ISMS and send periodic reports on this to Head– Human Resources

4.6 Admin Team

- Ensure that physical security controls are implemented and in compliance with the requirements of the Information security, Data Protection policy and Sustainability
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System

4.7 Information Security and Data Privacy Assurance Group

- Ensure that Delivery and Business functions align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System i.e. with Trianz Information Security Policy and procedures, Data Privacy policies and Procedures, Sustainability Management System Policies and Procedures
- Shall be responsible for New/Existing Certifications, Internal and External Audits, Organizations GRC and BCP

4.8 Travel Team

- Ensures the data shared with the Vendors comply with necessary Technical and organizational measures and respective vendors comply with adequate security and privacy standards by enduring data minimization and Purpose limitation
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System

4.9 Delivery and DA Team

- Ensures compliance to client Infosec and Privacy requirements
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System

4.10 Legal Team

- Shall be responsible for review , design of all Service Agreements, Non-Disclosure Agreements and all other applicable agreements
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management System

4.11 Finance and Purchase Team

- Shall be responsible for enduring onboarding only Infosec approved business critical vendors, Supplier Security, Agreements
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management Systems

4.12 Marketing Team

- Shall be responsible for all technical and organizational measures of data subjects' security- data at rest and data in transit (Prospective Clients) , DSAR Request
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management Systems

4.13 Platforms Team and Platforms Assurance Team

- Shall ensure the platforms are created/delivered/complied in compliance to Organizations Information Security and Privacy Policies and Procedures
- Align , deliver and comply to Information Security, Privacy Management System and Sustainability Management Systems

5. Outputs

Defined Roles and Responsibilities of Information Security Assurance Council

6. Exit Criteria

 Identifying and Mapping of Information Security Assurance Council roles & responsibilities

7. Process Assets

Document Name
None

8. Measurement

None

9. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.2 Information security roles and responsibilities Control Information security roles and responsibilities shall be defined and allocated according to the organization needs.	ISAC Roles and Responsibilities
Organizational Controls	5.3 Segregation of duties Conflicting duties and conflicting areas of responsibility shall be segregated.	ISAC Roles and Responsibilities
Organizational Controls	5.4 Management responsibilities Control Management shall require all personnel to apply information security in accordance with the established information security policy, topic specific policies, and procedures of the organization	ISAC Roles and Responsibilities

Document Control

Owner:	CISO	**Release ID:**	ISWG-PROC-0059

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	05-May-08	Bharateesha B R			Draft	NA
1.00	05-May-08	Bharateesha B R			Approval for Baseline	Baselined
1.01	18-Mar-10	Bharateesha B R			Regular Review	Formatting Changes
2.00	18-Mar-10	Bharateesha B R			Approval for Baseline	Baselined
2.01	03-Jan-11	Balu Nair			QMG review	Document formatted and changed RID to Release ID
3.00	03-Jan-11	Balu nair			Approved for baseline	Baselined
3.01	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency

4.00	24-May-11	Srilakshmi			Approval for Baseline	Baselined
4.01	29-Jun-11	Srilakshmi			QMG Review	• Included CIO Roles and Responsibilities • Modified Organization Chart
5.00	29-Jun-11	Srilakshmi			Approval for Baseline	Baselined
5.01	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
6.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
7.00	07-May-12	Srilakshmi			QMG Review	Modified Template format of this procedure Reviewed all roles &

						responsibilities and corrected inconsistencies
8.00	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo
9.00	18-Mar-15	Sudharsana			Upgrading to 27001:2013	Modified review frequency to quarterly review the status and effectiveness of ISMS implementation
9.01	25-Jan-16	Sumanta Bhattacharya and Balu Nair			Client Audit and alignment with shared assessment checklist.	• Vulnerability Assessment Test of Trianz network shall be carried out on quarterly basis • Information security policy is reviewed, at a

						minimum, on an annual basis • Ensure that information security awareness is provided to all personals in the organization, as applicable. Organization Chart is updated
10.00	08-Feb-16	Balu Nair			Approved by Mahesh (CISO)	Baselined
10.01	14-Oct-16	Shishir			Addition of Cloud services as scope of Certification.	ISWG name changed to ISAC Roles and responsibilities align with Cloud services
11.00	07-Oct-16	Balu Nair			Approved by CISO	Baselined

11.1	29-Apr-19	Balu Nair	Joshy VM			Information classification modified Trianz logo modified
12.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
12.1	13-May-20	Karthik N	Balu Nair		Review	• Updated the roles and responsibilities. • Updated the Org chart for InfoSec. Integrated to new template
13	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
13.1	4-Feb-21	Vijaya Rajeswari	Phani Krishna		For Review	Updated Information Classification and updated CISO roles & responsibilities
14.0	4-Feb-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

14.0	3-Jan-2022	Divya	Vijaya		For Review	No changes
14.1	28-Apr-2022	Divya	Balu N & Karthik		For Review	As per the auditor comments, we have revisited section 2.0
15.0	28-Apr--22	Vijaya Rajeswari	Balu N & Karthik	Siva N	For Approval	Approved and Baselined
15.1	05-Apr-2023	Shivateja, Rama Madhavan	Balu N & Karthik	Srikanth M	For Review	Added Section 5 Business Resiliency Group New template change
16.0	03-May-2023	Shivateja	Balu N & Karthik	Srikanth M	For Approval	Approved and Baselined
16.1	15-Feb-2024	Krutideepta	Vijaya R		For Review	1. Objective has been updated. 2. In Organization Chart Chief Data Privacy Officer (CDPO)has been added.

						3. In section 4.2 responsibilities of CDPO has been added. 4. ISO Mappings has been updated.
17.0	23-Feb-2024	Shalini and Krutideepta	Vijaya R	Srikanth M	For Approval	Approved and Baselined
17.1	6-May-2025	Vijaya	Balu		For Yearly Review	Migrated to new template

TRIANZ℠ | ACCELERATING DIGITAL EVOLUTION

THANK YOU

infosec @trianz.com

Contact Information

Name

Email

Phone

Thank You

reach@trianz.com