TRIANZ℠

ISDP Assurance 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

The ISDP Assurance Team enables Information Security and Data Privacy Assurance across Trianz and ensures compliance to various ISO Standards and Regulations.

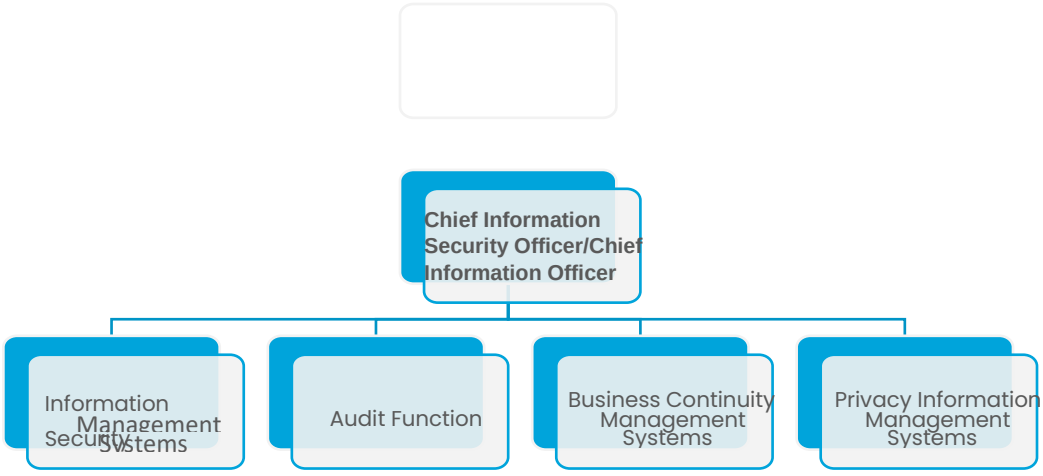
1.1 Objectives

Ensure that organization's Information Security & Privacy Management System is established, implemented, maintained, and improved Demonstrate Organization's commitment in securing Organizational and Client's Information Assets against vulnerabilities and threats

2. Definitions/Abbreviations/Acronyms

Word	Definitions
ISMS	Information Security Management System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISM	Information Systems Manager
DPR	Data Privacy Representative
IP	Internet Protocol

2.1 Organization Chart - Information Security and Data Privacy Assurance



3. Information Security and Data Privacy Assurance Roles, Responsibilities and Authorities.

3.1 Chief Information Officer (CIO)

- Ensures the Overall responsibility of Information/Cyber Security and Privacy for Trianz and sets clear vision, mission, and direction to Infosec and Data Privacy Assurance Team.
- Communicate the cybersecurity posture and any risk to the Stakeholders both internally and externally on periodic basis.

3.2 Chief Information Security Officer (CISO)

- Ensure that the ISMS policies and procedures are defined and implemented throughout the organization.
- Ensure that the Information security policies and recommended practices are updated in a timely manner to represent all current modifications.

- Ensuring that the 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.
- Ensure that the security requirements for new information processing facilities have been identified and approved.
- Ensure that an appropriate technical architecture is defined for the security of IT infrastructure and monitor compliance with the same.
- Arrange required resources and skills for conducting periodic information security reviews.
- Assess and ensure the disaster recovery preparedness and business continuity preparedness pertaining to IT systems.
- Ensure that appropriate security controls are defined for all applications in consultation with the application owner.
- Maintain a copy of the risk assessment documentation and a list of all the vulnerabilities identified in the various areas by the Information Security Assurance Council Specialists.
- Maintain and review all critical incidents that have occurred and the corresponding resolution timeframe.
- Ensure that the Risk Assessment of Trianz Information Assets will be conducted on an ongoing basis
- Ensure that the Vulnerability Assessment Test of Trianz network, Cloud infrastructure shall be carried out on quarterly basis
- Involve in-house security specialists or external specialists where required for addressing specific information security requirements.
- Deciding on the applicability of disciplinary policy in the case of security incidents being reported
- Will be responsible for providing directives for ensuring organization-wide information security
- Will delegate executive responsibilities for ensuring Information security & Privacy.
- Will take necessary measures to maintain security of the information systems
- Will ensure that staff is adequately trained to meet the security & Privacy requirements of the organization
- Will ensure that responsibilities are defined, and procedures are in place to promptly detect, investigate, report and resolve information security incidents

- Will ensure that provisions are in place for the continued protection of information systems resources in the organization.
- Authority to approve the vendors for choosing the right information security product,
- RCA for Information Security Incidents and Information security exceptions
- Authorized to approval all ISMS and PIMS related polices and process documents.

3.3 Information Security Group

- Following are the responsibilities of Information security compliance group and its team members.
- Ensure that the ISMS functions in their respective business groups are in accordance with Trianz Information Security Policy and procedures, data Privacy policies and Procedures.
- Data classification is maintained in terms of Trianz Information classification labeling and handling.
- Monitor adherence to Trianz information Security and Data Privacy Policies and Procedures
- Report any information security incident and Data Privacy Breach to
- Information Security Assurance Council and respective Supervisory Authorities as per the applicable regulations for e.g., reporting Security Breach to CERT-in 6 hours.
- Coordination with other members of Information Security Assurance Council for continuous implementation of ISMS and PIMS.
- Accountable on behalf of their respective groups for ISMS and PIMS.
- Give suggestions to Information Security Assurance Council for enhancement of information security and data privacy measures.
- Ensure that Information Security procedures relevant to the business groups are in line with the practice and Trianz Information Security Policy and Data Privacy policy.
- Ensure Contractual Obligations mapping to MSA and provide walk through to project Teams
- Ensures Third Party Risk and Compliance with Vendors

3.4 Data Privacy Assurance Group

Procedure	DPR Assurance Roles and Responsibilities	Internal/External
Breach Notification Procedure	Follow the Security Incident Response Procedure for Containment, Eradication etc Wherever Trianz is a Processor, DPR will notify the Controller on Data Privacy Breaches within 48 hours of breach and further actions as directed by the Controller (Client). **As per GDPR:** Wherever Trianz is a Controller, DPR/CISO will notify the Supervisory Authority on Data Privacy Breaches within 72 hours of Data Privacy Breach incident. **As per CERT-In** Wherever Trianz is a Controller,	Internal

	DPR/CISO will notify the CERT_In on Data Privacy Breaches within 6 hours of identification of Data Privacy Breach incident as per the criticality of the Incident (Refer to Security Incident Response Procedure) DPR/CISO will notify the data subjects as advised by Supervisory Authority and as required by the data privacy regulations	
Consent Procedure	Ensure consent procedure is followed for processing personal and sensitive data,	Internal
Cross Border Data Transfer procedure	• Assist the project/ delivery/support team in Ensuring Cross Border of data compliance as per applicable regulations	Internal

	• Review the Data Portability requests of all functions and maintain in a central register • Ensure data portability request is addressed within 30 days • Wherever data cannot be shared within 30 days, ensure updating to data subject within 30 days and getting the communication documented • In such cases ensure data is shared within 90 days of request from data subject	Internal
Data Protection Impact Assessment Procedure	Information Security & Data Privacy Assurance Team, IS Team, Data Privacy Representative (DPR)- • Ensure the availability of Data Privacy Diagnostic or threshold assessment where applicable on project initiation. • Support Project Manager and Delivery • Manager for conducting a DPIA or PIA where applicable Support in identifying the Risks, • Prioritizing the Risk, Risk Mitigation plans and its effectiveness, timelines of Risk Mitigation plan etc. • Ensure Mitigation plans • are implemented and its effectiveness is tracked and documented &	Internal

Data Subject Right Procedure	Infosec and Data Privacy Assurance team, DPR- Annual Review of Data Subjects Rights Procedures for its adequacy Quarterly Review of Data Subject Rights log for its compliance to regulations and corrective actions as needed.	Internal
Modify Withdrawal of Consent Procedure	Information Security Assurance Council, DPR- Periodic Review of Modify/Withdrawal of Consent forms and status of processing of personal data	Internal
Privacy by design procedure	Support Privacy By design and Default exercise in identifying the Data protection requirements Support for incorporating the applicable geography related Data protection requirements	Internal
Privacy Notice procedure	Information Security Governance Council, DPR- Yearly Review of Privacy concerns of the data subjects and implement corrective actions Yearly Review of Privacy Notice and sample privacy consent notice for its adequacy.	Internal
Retention of Records Procedure	Information Security Assurance Council, DPR- Review the Retention of Records Procedure on a yearly basis	Internal

Audits & Compliance	Facilitate Internal, external audits and compliance with respect to Privacy/Security assessments, certifications, or seals Support Privacy/Security assessment by Clients Ensure the project compliance with various security standards and regulations such as ISO 27701, SOC etc. Ensure Organizational compliance with applicable Privacy laws like GDPR, CCPA etc. Document and present internal review and audit findings to leadership	Internal & External
Policies and Procedures	Responsible for maintenance and compliance to Data Privacy Management System (DPMS) / PIMS (Privacy Information Management System) for Privacy Policies, procedures, and templates etc.	
Risk and Privacy Impact Assessment	Conduct DPIA and identify Privacy risks and their Management for IT services projects and in corporate functions Ensure Third Party risk management for Privacy/Security by supporting contract management process and Privacy Risk assessments of our Vendors Assess internal applications for any Privacy/Security Risks and facilitate Privacy risk management	

Privacy Trainings	Roll out of any required amendments of Data Privacy Trainings to the organization	
Continual Upgradation & Interactions with Security and Privacy professionals	Continually learn, actively share knowledge, and foster exchange of skills Proactively identify opportunities to improve the quality of reporting and usability of that information Implementation of any applicable Privacy Laws for any amendments or new business geographies related Privacy laws Interact with internal and external Security & Privacy professionals as needed	
Maintenance of Personal data Inventory	Maintain Personal Data Inventory of Corporate functions in the role of Data controller	

3.5 Audits

Following are the responsibilities of Audit Team

Ensure Yearly Planning for the Internal and External Audits

- Ensure Bi- Annual Internal audits and Yearly External Audits for Quality Management System, Information Security Management System,

- Privacy Information Management System and Service Management
- System across Trianz for India, US- Virginia and US- California Locations
- Ensure End to End Internal Audit Planning, Implementation, Selection of
  Auditors, Training, Audit findings Closure etc
- Ensure Internal and External Audits for Products
- Ensure SOC audits for Projects and Functions across Trianz

3.6 Business Continuity

Establish Business Resilience and Crisis Management structure across all location levels to facilitate local resumption of activities and deployment of supporting or recovery resources.

Design and establish a BCM framework for the company including its subsidiary operations and operating units to guide their business continuity efforts.

Conduct Business impact analysis, BCP risk assessments for any Trianz offices and critical functions and develop the continuity plans.

Regularly the test the business continuity plans for the key engagements and IT systems and report to the management.

Review the business continuity plans periodically and update the plans accordingly in case of any changes.

Develops and provide staff training on BCM via awareness sessions, eLearning and mailers.

Collaborates with delivery and corporate functions to develop and implement best practices to protect and restore data and systems in the event of natural disasters and security/privacy incidents.

4. Outputs

Identifying and Mapping of Information Security and Data Privacy Assurance Council roles & responsibilities

5. Process Assets

Document Name
ISMS Policy and Procedures PIMS Policy and Procedures

6. Measurement

None

7. Standards Addressed

ISO 27001 :2022	
Control	**Description**
A 6.1.1	Management commitment to information security
A 6.1.2	Information security coordination
A 6.1.3	Allocation of information security responsibilities

.

8. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Controls	5.2 Information security roles and responsibilities Control Information security roles and responsibilities shall be defined and allocated according to the organization needs.	ISDP Assurance Roles and Responsibilities.

Document Control

Owne	CISO	Release ID:	ISDPRR_PROC_0170

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	14Jul2022	Vijaya Rajeswari	Balu N & Karthik	Siva N	For Review	• Initial Version
1.0	14Jul2022	Vijaya Rajeswari	Balu N & Karthik	Siva N	For Approval	• Approved and Baselined
1.1	24-April-2023	Krutideepta, Rama Madhavan	Karthik N	Srikanth M	For Review	Reviewed with no changes. Migrated to new template
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
2.1	15-Feb-2024	Shalini	Vijaya	Srikanth	For Review	Mapped with new ISO 5.2 control

3.0	23-Feb-2024	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
3.1	8-May-2025	Vijaya	Balu			1.Migrated to new template and Yearly Review
4.0	14-May-25	Vijaya	Balu	Srikanth	For Approval	Approved and Baselined

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com