Information Security Organization: Roles and Responsibilities

Version 4.0

16/04/2021

Document Ownership – Information Security Team

NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or disclosed to other Genpact employees without a need to know, or to any third party or made public without the prior express written permission of Genpact.

Version Control

Version No.	Version Date	Type of Changes	Owner/Author	Date of next Review
1.0		First Draft – Adopted from GE with some minor modifications	AR Vijay	
1.0	05/05/2006	Original release	AR Vijay	Need Based
1.1	04/01/2008	Reviewed and minor changes	AR Vijay	Need Based
1.2	08/04/2009	Reviewed	AR Vijay	Need Based
1.3	02/02/2010	Reviewed and Logo updated	AR Vijay	Need Based
1.4	04/16/2010	Added Global Client Security role	Satish Jagu	Need Based
1.5	6th Dec 2011	Reviewed No Changes	Avvari Uma Sekhar/ AR Vijay	Need Based
1.6	1st Dec 2012	Reviewed No Changes	Avvari Uma Sekhar/ AR Vijay	Need Based
1.7	16th Dec 2013	Reviewed No Changes	Avvari Uma Sekhar/ AR Vijay	Need Based
1.8	16th Dec 2014	Reviewed No Changes	Ankur Jain/ Ramachandra Hegde	Need Based
1.9	30th June 2015	Updated as per ISO 27001:2013	Ramachandra Hegde/ Sandeep Srivastava	Need Based
2.0	29th June 2016	Updated Organization Chart	Ramachandra Hegde/ Sandeep Srivastava	Need Based

Version Control table has been revised to ensure compliance to Genpact Version Control Guidelines.

Version No.	**Version Date**	**Type of Changes**	**Author**	**Approver**	**Date of next Review**
2.1	17th Aug 2017	Updated Organization Chart	Sandeep Srivastava	Srivastava Ramachandra Hegde	16th Aug 2018
2.2	22nd March 2018	Updated Organization Chart and responsibilities	Sandeep Srivastava	Ramachandra Hegde	21st March 2019
2.3	4th Jan 2019	Updated terminologies used	Sandeep Srivastava	Ramachandra Hegde	3rd Jan 2020
2.4	31st July 2019	Provided reference to Organization Chart, updated nomenclature & roles and responsibilities	Sandeep Srivastava	Ramachandra Hegde	30th July 2020

Version Control table has been revised to ensure compliance to Genpact Document Management Procedure.

Version No.	**Version Date**	**Type of Changes**	**Author**	**Approver**	**Date of next Review**
3.0	12/03/2020	Aligned to the new organization chart	Shailender	Kuhu Adhikary	11/03/2021
3.1	30/03/2020	1. Governance Structure modified 2. “Approver” details in version control updated 3. Path to access Roles and Responsibility added 4. Section 6.10 modified – From “All Employees” to “All Employees & Contractors”	Shailender	Lakshmanan Sriram	29/03/2021

4.0	16/04/2021	1. Governance Structure modified 2. Org Chart Modified 3. Path to access Roles and Responsibility document modified 4. Section 6 modified as per new cadence details and Governance structure	Shailender	Lakshmanan Sriram	15/04/2022

Contents

1 Introduction

This document defines roles and responsibilities for development, implementation, and maintenance of an Information Security Management System (hereinafter referred to as 'ISMS') at Genpact.

2 Objective

The purpose of this document is to define the roles and responsibilities of relevant stakeholders that are responsible for maintenance and governance of the ISMS framework of Genpact.

3 Applicability

Applicability of the Information Security Organization Responsibilities is for the entire organization.

4 Responsibility

The owner of the ISMS is the CISO. The CISO is authorized by the board of the company and is accountable for the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the Genpact ISMS. Genpact Chief Information Security Officer (CISO) shall act in accordance with defined procedures and is authorized to take decisions, considering all sources of information and resources that are available to Genpact.

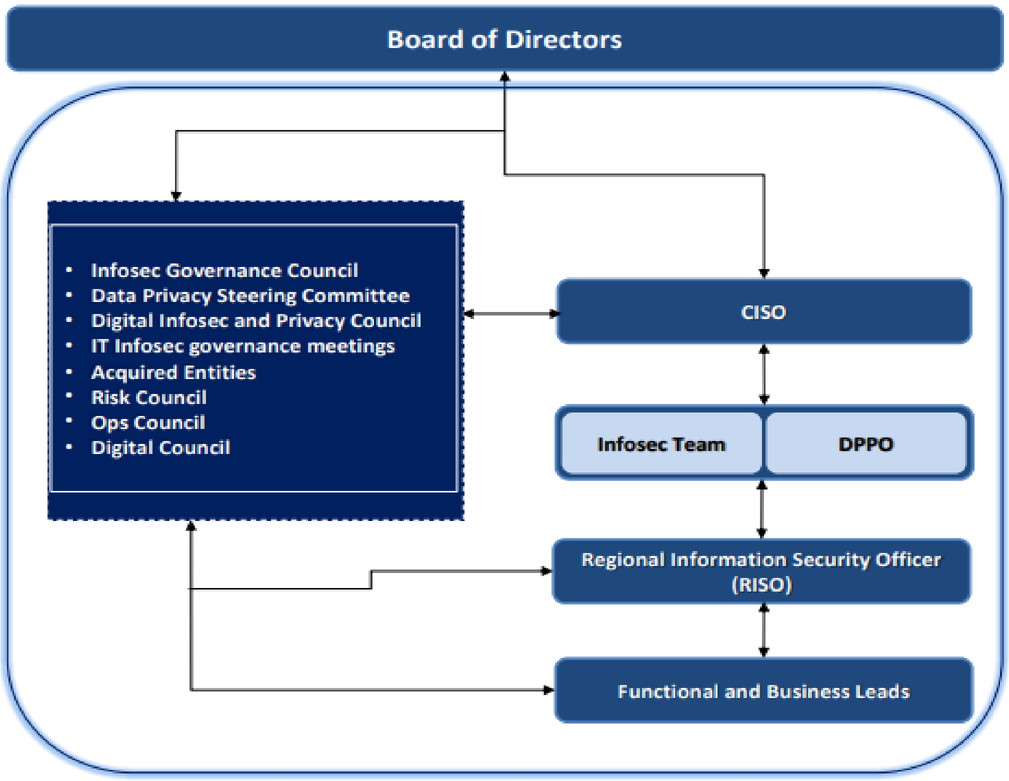
5 Information Security Management System Governance Structure

ISMS governance structure consists of

- Chief Information Security Officer (CISO)
- Information Security Team
- Data Protection & Privacy Office (DPPO)
- Regional Information Security Officers
- Functional and Business Leads

The governance structure receives inputs from:

- Board of Directors
- Infosec Governance Council
- Data Privacy Steering Committee
- Digital Infosec and Privacy Council
- IT Infosec governance meetings
- Acquired Entities
- Risk Council
- Ops Council
- Digital Council



Board of Directors

- Infosec Governance Council
- Data Privacy Steering Committee
- Digital Infosec and Privacy Council
- IT Infosec governance meetings
- Acquired Entities
- Risk Council
- Ops Council
- Digital Council

CISO

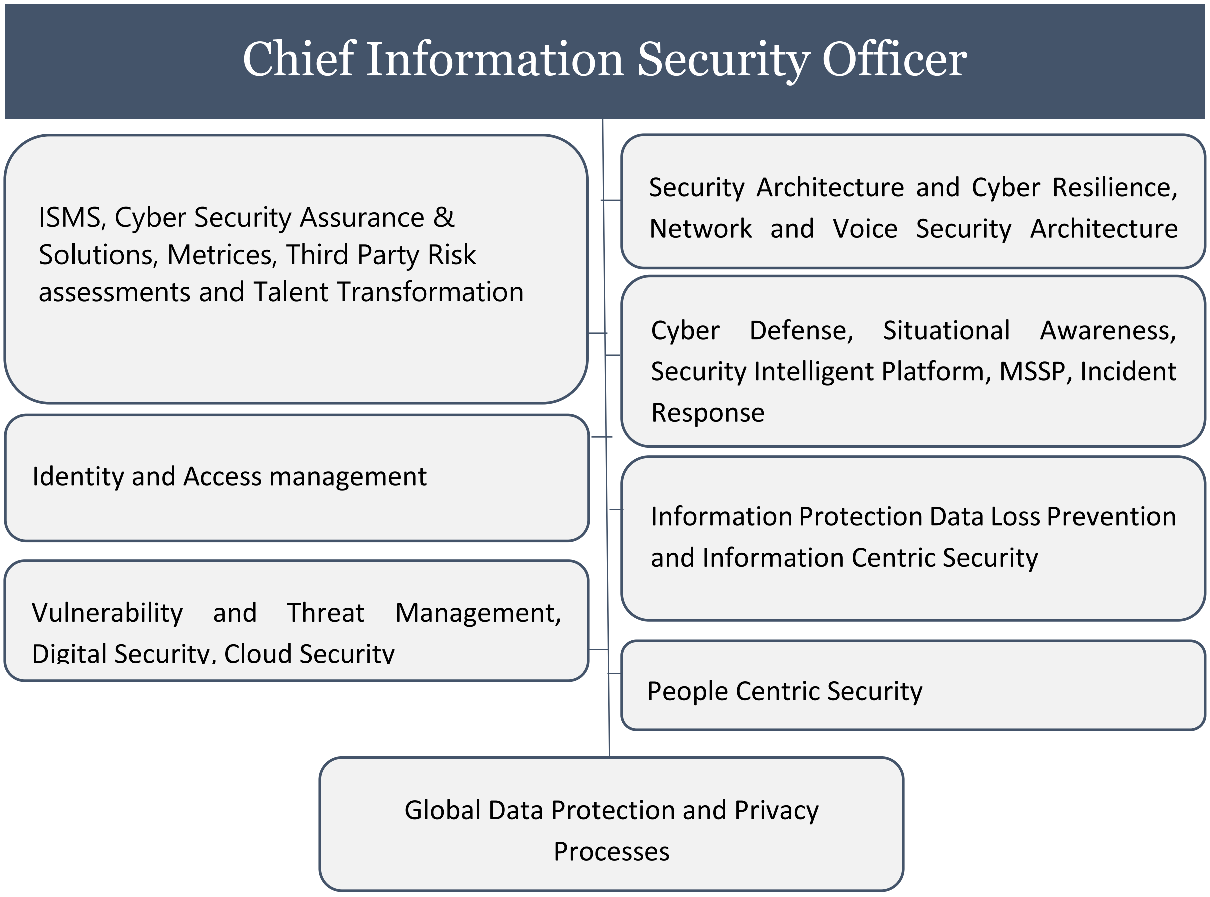
Infosec Team

DPPO

Regional Information Security Officer (RISO)

Functional and Business Leads

The Information Security functions is led by the Chief Information Security Officer (CISO) in conjunction with the functions mentioned below:



Chief Information Security Officer

ISMS, Cyber Security Assurance & Solutions, Metrices, Third Party Risk assessments and Talent Transformation

Security Architecture and Cyber Resilience, Network and Voice Security Architecture

Cyber Defense, Situational Awareness, Security Intelligent Platform, MSSP, Incident Response

Identity and Access management

Information Protection Data Loss Prevention and Information Centric Security

Vulnerability and Threat Management, Digital Security, Cloud Security

People Centric Security

Global Data Protection and Privacy Processes

The high-level Organization Chart of the Information Security Team and Data Protection and Privacy Office (DPPO) can be accessed at following location: Information Security Organization Chart.

Role and Responsibility details are made accessible to the relevant stakeholders at the below mentioned location:

GSocial->All Tools->I-> Infosec Policy and Procedure

6 Roles and Organizational Representatives

Function Name	Key activities of the function	Frequency of assembly
Board of Directors	The Board provides strategic direction to the Company and oversight of management in the performance of the Company's business activities. They also ensure that there is a clear direction and visible management support to manage information security within the organization.	Quarterly
Infosec Governance Council	Provide outline of Infosec strategy Awareness of program status, key metrics, benchmarks, challenges, key incidents Decisions and approval around strategy, policy changes, program direction	Monthly
Data Privacy Steering Committee	Update on privacy program status, legislative changes Review of key metrics, benchmarks, incidents Decisions on key areas on program initiatives	Quarterly
Digital Infosec and Privacy Council	Update on privacy program status, legislative changes Review of key metrics, benchmarks, incidents Decisions on key areas on program initiatives Focus is purely on Digital projects/ products/ processes &	Monthly

	performance/ initiatives – and associated vulnerabilities, exceptions, privacy by design and related decisions. These could be client facing (CORA/ RPA etc.) or internal G facing projects (e.g., Amber/ ICON/ Genome etc.)	
IT Infosec Governance meetings	Review of key Information technology metrics, challenges, key incidents with IT leadership Decisions on key areas on IT-initiatives	Monthly
Acquired Entities	Review security and privacy posture, key metrics, incidents, and risks Discuss ongoing business engagements, client implementations and delivery from InfoSec standpoint Determine current integration progress in line with Genpact Toolset and hosting environment	Monthly
Risk Council	The Enterprise Risk Council (also commonly referred to as Risk Council) is responsible for approval of policy, risk appetite, governance, prioritization, and mitigation of key risks Review and approve risk management related guidelines and policy Ensure that risk management system is established, implemented, and maintained in accordance with the defined framework Review and approve the organization's risk profile periodically	Quarterly

	Provide a sign off on the current & planned approach to manage key business risks. Approve the risk mitigation plan and strategy ensuing it's in line with the company's risk appetite. Periodically report on business risks to the Board	
Ops Council	Drive awareness and generate support for cyber / privacy decisions having operational impact. Ensure Infosec team is aware of key operational decisions	Monthly
Digital Council	Key updates from Digital Security and Privacy Steering Committee will be presented to Digital council for specific decision making and general awareness. Maturity projections/ investments or strategic project decisions etc. Infosec Digital leader to participate in awareness of status of digital security and privacy controls and key risk issues	Monthly

6.1 Chief Information Security Officer

The CISO shall be responsible for driving implementation of the ISMS in Genpact. The CISO is accountable for the overall management of Information Security in Genpact. CISO shall also be responsible for the on-ground implementation and maintenance of Information Security across the organization.

6.1.1 Role Competency

Below are the requirements for the role of CISO:

Role –Chief Information Security Officer

S. No.	Competency Parameter	Competency Details
1.	Professional and Behavioral	a. Qualified Information Security and Privacy leader with proven credentials in managing security and privacy of products, & services b. Thought leader that continually augments the maturity of the Information Security posture c. Enable secure business decisions d. Should be able to work in a complex and dynamic business environment e. Should promote teamwork, quality, efficiency and employee development

6.1.2 Responsibilities of CISO

Following are the responsibilities of the CISO for ISMS establishment, implementation, operation, monitoring, maintenance, and improvement phases at Genpact:

- Owns the overall framework, policy, and procedures for Information Security
- Establish and monitor due processes for identifying, documenting, and managing risks
- Communicate essential messages related to Information Security and Privacy to stakeholders (internal and external);
- Provide approvals on Information Security and Privacy Framework and Policy
- Communicates to the organization the importance of meeting Information Security and Privacy objectives and adherence to the Information Security and Privacy Policy
- Informs the senior management for any ISMS related issues at different Enterprise Risk Council and Privacy Steering Committee meetings on Quarterly basis
- Regularly update relevant management forums on compliance status, issues and plans for key Information Security related compliance programs such as PCI DSS, ISO 27001

6.2 Information Security Team

The Information Security Team shall be responsible to establish, implement and operate ISMS in accordance with

- ISO 27001, PCI-DSS and other applicable frameworks, standards, and applicable regulatory requirements on a need basis.

6.2.1 Role Competency

Below are the competency requirements for the role of Information Security Team members:

Role – Information Security Team Member		
S. No.	Competency Parameter	Competency Details

1.	Professional and Behavioral	a. Role Relevant understanding of information security to build organizational continuity, capability, and knowledge of globally accepted information security management standards (e.g., ISO 27001:2013, NIST, HITRUST) b. Continuous development and upskilling the team on the most current security trends and technologies c. Sound understanding of the organization d. Certification in Information Security (e.g., ISO 27001:2013 Lead Implementer, ISO 27001:2013 Lead Auditor, CPISI, CISSP, CISA, CISM) e. Appropriate professional work experience f. Should possess good analytical abilities to identify, analyze and address Information Security and Privacy risks

6.2.2 Responsibilities of Information Security Team

- Shall be responsible for development, implementation, monitoring and improvement of ISMS arrangements
- Ensure active participation of employees towards ISMS awareness programs and initiatives
- Participate in initiatives with respect to information security as directed by the CISO
- Own and Manage Security Certifications such as but not limited to ISO27001 and PCI DSS
- Facilitate the risk assessment process for all teams in scope across all locations
- Proactively identify and report security incidents and weaknesses
- Members of the Information Security may be additionally tasked with security and privacy tasks in-line with the requirements in the region. They may be required to assist with any of the Infosec functions

6.3 Data Protection and Privacy Office (DPPO)

6.3.1 Role of DPPO

The Data Protection and Privacy Office comprises of the CISO, Data Privacy Team and is supported by the other Information Security team members. The DPPO drives the implementation of data privacy and protection processes within Genpact.

6.3.2 Responsibilities of DPPO

The DPPO is responsible for the overall management of following in context of data protection and privacy:

- Privacy Policies, Procedures and Guidelines
- Privacy Related Processes
- Enabling technology identification and adoption
- Training
- Program Updates to Privacy Steering Committee
- Systems Design Considerations
- Data Subject Rights

- Mergers and Acquisitions, and Divestiture
- Vendor Certification and Oversight
- New Business Developments
- Contractual Aspects
- Data and Information Management
- Customer Assurance
- Research and Benchmarking

6.4 Regional Information Security Officers (RISO)

6.4.1 Roles of RISO

CISO representative for the service delivery regions and is appointed by the Global Cyber Security Assurance Leader

6.4.2 Responsibilities of RISO

- Key enabler of the businesses in the region from an Information Security and Privacy perspective
- Drive and assist the Information Security and Privacy programs for the regions
- Coordinate, assist and lead global Information Security requirements and regional Privacy requirements
- Ensure alignment of regional Information Security and Privacy requirements with that of global
- Represent InfoSec and Privacy during customer assessment and similar activities
- Help identify and manage Infosec and Privacy risks as per global processes
- Support required certifications such as for ISO 27001 or PCI
- Publish or help publish the key metrics as explicitly required by Clients and regional senior management
- Look for continual improvement in the region and in the global context
- Research and share perspectives on regulations and changes in business or industry environment in the region
- Advise local business on right security and privacy processes
- Help create and spread security culture amongst all functions

6.5 Functional and Business Teams (SPOC)

To adequately provide Information Security to business, the Chief Information Security Officer & Information Security Team are expected to interface with following functions and teams:

- Enterprise Risk Management
- Legal
- HR & Training
- Infrastructure & Logistics
- Business Continuity Management
- Information Technology
- Vendor Governance & Sourcing
- Business and Corporate Finance
- Business Verticals

6.5.1 Responsibilities of SPOC

- Ensure satisfactory implementation of Information Security and Privacy Policy and related policies, procedures, standards, and guidelines of Genpact

- Instill security awareness among all employees, business partners and personnel affiliated with third parties who are associated with their team
- Act as single point of contact for Information Security related initiatives within their team
- Maintain relevant documents adhering to Genpact policies, procedures, standards, and guidelines for their teams on a regular basis
- Conduct risk assessment for their respective team
- Act as asset owner of information assets and ensure compliance with data classification requirements for the information assets of their respective team
- Participate and provide support in internal and external audits
- Be responsible for taking corrective actions for the team's audit findings

6.6 Third Parties

Genpact has dependency on third parties for various services. Third parties should participate and assist Genpact in undertaking the necessary precautionary/ preventive as well as reactive steps towards security breaches. Thus, the Information Security function as appropriate may need to interface with the following external (non-Genpact) organizations and departments:

- Local and National Law Enforcement (via Legal)
- External Auditors
- Government Regulators (via Legal)
- Customers
- Suppliers
- Trade Organizations
- Security Interest Groups

6.6.1 Responsibilities

- Ensure communication as per escalation matrix
- Ensure that Non-Disclosure Agreements are signed timely
- Strictly maintain the confidentiality of all Genpact and its clients' information
- Shall be aware of Genpact Information Security and Privacy Policy and related policies and comply to same as applicable
- Ensure active participation in ISMS initiatives such as training and awareness, internal audits and reviews scheduled by Genpact

6.7 All Employees & Contractors

Employees and contractors play a critical role in the ISMS at Genpact. They should follow and comply with the requirements of ISMS.

6.7.1 Responsibilities

- Ensure they are aware of Genpact Information Security Policy and related policies, procedures, standards, and guidelines and adhere to them
- Ensure that they adhere to client security requirements
- Ensure that they actively participate in ISMS activities
- Ensure all the actions are taken towards safety of personnel
- Ensure instant communication and reporting about security incidents to ensure timely and effective response to emergencies
- Strictly maintain the confidentiality of Genpact and its clients' data including Personally Identifiable Information (PII)
- Follow guidelines and instructions given by Infosec functions for the maintenance of ISMS

7 Annexure

7.1 Document Reference List

Please refer to the ISMS Master List of Documents.

7.2 Abbreviations and Definitions

Please refer this Link.