KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park,
Pebble Beach, B Block, 1st and 2nd Floor,
Off Intermediate Ring Road,
Bengaluru 560 071 India
Tel: +91 80 6833 5000
Fax: +91 80 6833 6999

Capgemini Technology Services India Limited
Plot No. 14, Rajiv Gandhi Infotech Park,
Hinjawadi Phase-III, MIDC-SEZ,
Village Man, Taluka Mulshi,
Pune-411 057, Maharashtra, India

23 February 2024

Attention: Leena Sagar, Vice President, Head – Quality India

KPMG Assurance and Consulting Services LLP (herein after referred to as “KPMG”, “We”, “Our”) have completed SOC 3 examination for Capgemini Technology Services India Limited (herein after referred to as “Capgemini”, “service organization”, “you”) as outlined in our engagement letter. This report to you represents our final report for SOC 3 examination.

The data included in this report was obtained from you, on or before 22 February 2024. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 22 February 2024. The attached report is the electronic version of our signed deliverable, which has been issued to you in the hard copy format.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.

While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.

This report is intended solely for the information and use of the management of Capgemini , its user entities and the independent auditors of user entities (collectively referred to as authorized parties) and is not intended to be, and should not be, used by anyone other than these authorized parties. If this report is received by anyone other than authorized parties, the recipient is placed on notice that the attached SOC 3 report has been prepared solely for authorized parties for their internal use and this report and its contents shall not be shared with or disclosed to anyone by the recipient without the express written consent of Capgemini and KPMG. KPMG shall have no liability and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report. We have been engaged by Capgemini for the Services and to the fullest extent permitted by law, we will not accept responsibility or liability to any other party in respect of our Services or the report. We thus disclaim all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such other party arising out of or in connection with the report or any part thereof. By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Please contact us if you have any questions or comments. We look forward to providing services to your company.

M N Gururaja
Partner
KPMG Assurance and Consulting Services LLP

SYSTEM AND ORGANIZATION CONTROLS (SOC 3) REPORT

Report on description of System supporting the general operating environment provided by Capgemini Technology Services India Limited and on the suitability of design and operating effectiveness of controls relevant to the Security, Availability and Confidentiality Principles from the delivery centers located in India.

For the period 01 October 2022 to 30 September 2023

TABLE OF CONTENTS

Section 1

Independent Service Auditor's Assurance Report

KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park,
Pebble Beach, B Block, 1st and 2nd Floor,
Off Intermediate Ring Road,
Bengaluru 560 071 India
Tel: +91 80 6833 5000
Fax: +91 80 6833 6999

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

To
The Board of Directors,
Capgemini Technology Services India Limited

Scope

We have examined Capgemini Technology Services India Limited's ("Capgemini") accompanying management statement in section 2 titled "Statement by the Service Organization" that the controls within Capgemini' system for providing general operating environment to user entities ("System") were effective throughout the period 01 October 2022 through 30 September 2023, to provide reasonable assurance that Capgemini' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Capgemini' management is responsible for the management statement. Our responsibility is to express an opinion based on our engagement. Management's description of the aspects of the Capgemini' System covered by its statement is attached in. We did not perform any procedures regarding this description, and accordingly, we do not express an opinion on it.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Capgemini, to achieve Capgemini' service commitments and system requirements based on the applicable trust services criteria. The complementary user entity controls are described in the management statement and attachment. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Capgemini is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Capgemini' service commitments and system requirements were achieved. Capgemini has also provided the accompanying statement about the effectiveness of controls within the system. When preparing its statement, Capgemini is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's statement that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our assurance engagement was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board.) Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's statement is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve Capgemini' service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Capgemini' service commitments and system requirements based the applicable trust services criteria
- Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's statement that the controls within Capgemini' System were effective throughout the period 01 October 2022 through 30 September 2023, to provide reasonable assurance that Capgemini' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

KPMG Assurance and Consulting Services LLP

KPMG Assurance and Consulting Services LLP
22 February 2024

Section 2

Statement By The Service Organization

STATEMENT BY THE SERVICE ORGANIZATION

We are responsible for designing, implementing, operating, and maintaining effective controls within Capgemini Technology Services India Limited's (Capgemini') system throughout the period 01 October 2022 through 30 September 2023, to provide reasonable assurance that Capgemini' service commitments and system requirements relevant to security, availability, and confidentiality, were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our statement.

The attached description in attachment A of the Capgemini system identifies those aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 01 October 2022 through 30 September 2023, to provide reasonable assurance that Capgemini' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality, (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Capgemini' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented as part of attachment A.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 01 October 2022 through 30 September 2023, to provide reasonable assurance that Capgemini' service commitments and system requirements were achieved based on the applicable trust services criteria.

ATTACHMENT A

CAPGEMINI’ DESCRIPTION OF THE BOUNDARIES OF ITS SYSTEM, PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

INTRODUCTION

SCOPE OF THE REPORT

The scope of this report includes the description of Capgemini Service Organization's system supporting general operating environment i.e., HR, ICRES, GROUPIT, ISMS, BCM, LnD, Procurement, Corporate & Legal provided to Customers (hereinafter referred as "User Entity" or "Customers") from its deliver centers at the following locations:

Center	Address
Bengaluru	• Bengaluru 6B, Pritech Park SEZ, Bldg 6B, Bellandur Village, Vatu Hobli, Outer Ring Road Bengaluru - 560037 • Bengaluru - Divyasree TechPark B5, A5 & B4, SEZ Divyasree Techno Park, IT/ITES SEZ SY No. 38(P) & 44/1, Kundalahalli, Whitefield, Bengaluru - 560037 • Bengaluru - Dartmoor Building, No. 158-162 (P) & 165-170 (P), EPIP Phase II, Whitefield, Bengaluru - 560066 • 155-156(P), EPIP Phase II, Whitefield, Bengaluru - 560066, Karnataka, India • 164-165 (P), EPIP Phase II, Whitefield, Bengaluru - 560066, Karnataka, India
Chennai	• Chennai MIPL, Capgemini Technology Services India Limited, Plot No.TP 4/1,4th Avenue, Techno Park, SEZ, Mahindra world city, Chengalpet, Tamil Nadu – 603004, India. • Chennai – PCT (Prestige Cybertech Park), Capgemini Technology Services India Limited, Prestige Cyber Tower,117, Rajiv Gandhi Salai, OMR, Karapakkam, Chennai, Tamil Nadu – 600097, India. • Sipcot IT Park, Plot No: H-6, Old Mahabalipuram Road, Siruseri, Chennai - 603103, Tamil Nadu, India.
Salem	• Capgemini Technology Services India Ltd., 41/52, PT Towers, Suramangalam Main Road, 3 Roads Salem - 636009, Tamil Nadu.
Trichy	• Capgemini Technology Services India Limited, VRN Center No 37, VRN Centre, Bishop Road, Puthur, Trichy – 620017 • Capgemini Technology Services India limited, Phase 2, 26/2 Muthiah Tower William Road, Cantonment, Trichy – 620001 Tamil Nadu, India
Mumbai	• Capgemini Knowledge Park - SEZ (M5), IT3/IT4, Off Thane Belapur Road, Airoli, Navi Mumbai – 400708. • Mumbai M4, Plant No. 5, (Godrej IT Park), Godrej & Boyce Mfg Co Ltd, Pirojsha Nagar, LBS Marg, Vikhroli (West) Mumbai - 400079 (Applicable from 1st April 2023 to 30th September 2023)
Pune	• Capgemini Technology Services INDIA Ltd, Campus, A-1 Technology Park, MIDC, Talwade, Pune - 411062 • Rajiv Gandhi Infotech Park, Plot No.14, Phase III MIDC SEZ, Village Man Taluka, Mulshi, Haveli, Hinjewadi, Pune – 411057 • Level 0, Tower III Cyber City, Magarpatta City Hadapsar, Pune - 411013, Maharashtra, India
Hyderabad	• Campus site, Hyderabad Gachibowli, Survey no: 115/32&35, Nanakram Guda, Gachibowli, Hyderabad, Telangana - 500032 • GAR Corporation Pvt. Ltd, LAXMI INFOBAHN, IT/ITES SEZ, Sy. No. 107, GAR SEZ, Kokapet Village, Gandipet Mandal, Ranga Reddy District, Hyderabad, Telangana – 500075
Kolkata	• Candor Hi-Tech-Structures Limited, SEZ – IT/ITES Tower A, B & C, 1st floor, Plot 1, 2 & 3, Block DH, New Town, Kolkata – 700156
Gandhinagar	• Capgemini Technology Services India Ltd., Aqualine Properties Pvt. Ltd. (IT/ITES), A-201 & 202, Bldg. #1, Mindspace SEZ Koba, Gandhinagar - 382009 Gujarat, India.
Gurugram	• Tower 6, IT/ITES SEZ, Candor Gurgaon One Realty Projects Pvt. Ltd., Village Tikri, Sector 48, Gurugram, Haryana 122018

Center	Address
Noida	• Capgemini Technology Services India Limited, Noida Special Economic Zone (NSEZ) 139, 140, A Block Phase II, NOIDA - 201305, Uttar Pradesh, India • Capgemini Technology Services India Limited, Noida Special Economic Zone (NSEZ) 142 E&F, B Block Phase II, NOIDA - 201305, Uttar Pradesh, India • Capgemini Technology Services India Limited, Noida Special Economic Zone (NSEZ) 134, 135 A Block Phase II, NOIDA - 201305, Uttar Pradesh, India

Overview of Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini focuses on three 'playing fields' dedicated to the digitalization of key management areas at the core of businesses: Customer First, Intelligent Industry, and Enterprise Management. This is underpinned by two technological pillars essential to all forms of digital transformation – data and cloud, without losing sight of the fundamentals of cybersecurity and sustainable development. Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 325,000 team members in almost 50 countries.

Services Offered by Capgemini

Capgemini, one of the world's foremost providers of Consulting, Technology, Outsourcing and Other Managed Services, has a unique way of working with its clients called the Collaborative Business Experience. The Collaborative Business Experience is designed to help our clients achieve better, faster, more sustainable results through integrated access to the Capgemini network of leading technology partners and collaboration-focused methods and tools. Through commitment to mutual success and the achievement of tangible value, Capgemini helps businesses implement growth strategies, leverage technology, and thrive through the power of collaboration. For its clients, both local and international, Capgemini offers a complete range of services organized around four disciplines:

- **Consulting Services** *(Capgemini Consulting)*

The digital economy is triggering a new wave of transformation in the way leaders and organizations do business. However, this rapid adoption of new technologies demands significant cultural change and challenges traditional business models. Capgemini Consulting teams design winning strategies by harnessing the power of the new digital economy to deliver value and performance through mastery of digital advances, information insight and business transformation using expertise like Digital Transformation; Strategy and Transformation; Supply Chain Management Consulting; Finance Transformation; People and Performance; Marketing, Sales and Service; CIO Strategy & Transformation; Accelerated Solutions Environment; Big Data & Analytics Consulting

- **Application Services** *(Application Development and Maintenance -Next or ADM Next)*

Today's CIOs must contend with increasingly complex application landscapes while promoting continuous rationalization and cost-effectiveness. Capgemini's Next Generation Application Development and Maintenance proposition increases the effectiveness of business processes, provides superior Service Integration, enhances end-user experience, and enables business outcomes. This platform is a business value-oriented, industrialized approach for managing client applications that provides always-on business transactional capability while pervasively reducing costs by creating a business aware and future proof IT application landscape.

- **Other Managed Services (***Business Services***)**

Other Managed Services integrate, manage and / or develop either fully or partially, clients' IT Infrastructure systems (or that of a group of clients), transaction services and on demand services and/or business activities. Solutions include –

- ✓ Governance Risk and Compliance & Risk Analytics: To enhance clients' reputation, ensure compliance and deliver real business value.
- ✓ Business Process-as-a-Service (BPaaS): An "assemble-to-order" group of solutions that enables clients to grow their

business while reducing operational costs. Integrating services, processes, applications and infrastructure, BPaaS maximizes agility and responsiveness by leveraging a Cloud-based ecosystem of solutions and Capgemini's unique Global Enterprise Model© (GEM).

- ✓ Business Analytics: Harness the insights and data generated by customers, business operations and supply chain to drive business improvements.
- ✓ Customer Interaction Services: To enrich and enhance customers' experience with a powerful omnichannel solution.
- ✓ Optimize Operations: In today's digital revolution, renewed focus on business operations is essential for any organization wishing to strengthen competitiveness – core operations must be fast, streamlined and efficient. By developing the most appropriate cost, flexibility, quality and skills management environment, operations management can be optimized. Capgemini helps customers design, build and run business and IT operations that optimize total cost of service & create agility for a profitable growth through an integrated and industry-led approach.
- ✓ Optimize Supply Chain and Vendor Performance: Standardize, automate and integrate customers' systems and data to create a real-time operating and decision-making environment. Includes Contract Compliance & Optimization and Digital Supply Chain.
- ✓ Transformation of Finance Operations: Capgemini's Finance Powered by Intelligent Automation reimagines C2C, P2P and R2A, promising the very best-in-class finance operations for customers' business.
- ✓ Retain and Engage Employees: Enhance employee engagement and performance to raise the value of customers' HR function, enabling their business to achieve its objectives.

Clients are provided with a specifically designed combination of quality, cost and delivery options through a network of worldwide centers.

Capgemini has also developed alliances with the top global technology leaders, as well as local players, to form a unique ecosystem that better serves its clients.

Group is composed of Strategic Business Units (SBUs) as follows:

- Americas
- APAC
- Europe
- Northern Central Europe
- Southern Central Europe
- Financial Services

The SBUs are divided into Business Units (BUs), each of which encompasses a number of Market Units (MUs). The Business Units (BUs) and Market Units (MUs) are responsible for managing the P&L, managing the clients, and profitably selling, delivering, and growing the full Capgemini portfolio to all clients within their market - in full collaboration with the Global Business Lines.

PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Capgemini designs its processes and procedures related to general operating environment to meet its objectives. Those objectives are based on the service commitments agreed between Capgemini and user entities, and applicable laws and regulations that govern the provision of said services. Services provided by Capgemini to user entities are subject to Security, Confidentiality and Availability requirements.

Security, Availability and Confidentiality commitments to user entities are documented and communicated through a formal contract between Capgemini and user entities. These commitments are taken into account by Capgemini while establishing the operational and system requirements for user entities operations. These requirements are contained in information security policy and procedure documents. Capgemini has adopted ISO27001:2013 to establish a management framework for Information Security Management System.

Security commitments to user entities are documented and communicated in customer Master Service Agreements, as well as in the description of the service offering provided. Security commitments include, but are not limited to, the following:

- Access will be granted based on clearing the BGV mandated by client.
- Drive compliance with established policies through routine security evaluations and internal audits
- Ensure compliance to ISO 27001 and any other client specific information security requirements.
- Hardening guidelines are implemented in all the desktops and laptops. Those include but are not limited to restriction of removable media and administrative access to workstations. Local admin access is not enabled for all end users by default.
- Vulnerability assessments need to be performed on a periodic basis.
- Incident Management and Business Continuity Management.
- Reconciliation of physical access to ODC and hub room is performed on a periodic basis.
- Security commitments to client are documented and communicated in User Entities Master Service Agreement and include Capgemini's responsibility to obtain a SOC 2 Type 2 report annually.
- Physical Security elements around access to data centers, restricted areas and video surveillance for high security zones.
- Capgemini offers secure access email on mobile device.
- MDM (Mobile Device Management) is the baseline configuration as per the information security requirement.

Availability commitments include, but are not limited to, the following:

- Environment threats are identified, and necessary precautions are taken. Environment thresholds are monitored.
- Backup and restoration tests are conducted for IT infrastructure used for services provided to User Entities
- Business continuity and disaster recovery plans have been developed, updated, and tested annually.

Confidentiality commitments include, but are not limited to, the following:

- Information security policy detailing classification of data based on its criticality and sensitivity is in place.
- Non-Disclosure Agreements are in place and necessary protections are in place for confidential information.
- Retention and disposal of confidential information based on the requirements agreed in the MSA between Capgemini and the user entities.

Capgemini establishes operational requirements that support the achievement of the service commitments, relevant laws and regulations, and other systems requirements. Such requirements are communicated in Capgemini's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

COMPONENTS OF THE SYSTEM

INFRASTRUCTURE

Group IT is responsible for maintaining the IT infrastructure of the organization. The Group IT team manages the entire network and telecommunication infrastructure at Mumbai, Pune, Bengaluru, Hyderabad, Chennai, Noida, Salem, Trichy, Gandhinagar, Gurugram and Kolkata. It also assists project and pursuit teams in defining and implementing network requirements. The Group IT leader is responsible to ensure IT support functions such as helpdesk, network provisioning and server administration are provided as per the SLAs or within the agreed timelines as applicable

LAN AND WAN ARCHITECTURE

All In-scope sites (Mumbai, Pune, Bengaluru, Hyderabad, Chennai, Noida, Salem, Trichy, Gandhinagar, Gurugram and Kolkata) are connected to the Capgemini global WAN backbone. This global backbone connects all the Capgemini regions to one another via an MPLS fully redundant network provided by Orange Business Services (service provider, out of scope of this report). The sites are connected to each other on 45mbps link and configured with OSPF protocol to achieve redundancy in case of link failure.

Firewall appliances and Internet proxy servers are hosted in data centers. Other shared servers like the email server and domain server are hosted within the data center. Our facilities are connected by fiber optic cable. Data centers at each location also host critical communication devices like routers and the call manager 'VoIP '(Voice over IP).

Based on client requirements, client project networks are separated from the Capgemini India corporate network, in Mumbai, Bangalore, Hyderabad, Pune, Chennai, Noida, Salem, Trichy, Gandhinagar, Gurugram and Kolkata Centers, either physically or logically.

The company's network infrastructure (CGSLAN) provides access to the Internet and related services to selected users. The Internet access is controlled through a Bluecoat proxy and Check Point (CP) firewall. The access to the Internet sites is restricted by using URL filtering software (Infoblox Software).

Two types of Internet access are available in Capgemini India, one link is dedicated to Projects specific IPSec traffic and the other link is used for browsing which is controlled through NGFW. The NGFW filters content and blocks access to non-business categories.

SOFTWARE

Capgemini also utilizes various software utilities, which include, but are not limited to those outlined below:

- The tool ScienceLogic is used to monitor systems, Network activity and Server availability.
- Crowdstrike is utilized for anti-virus protection to protect against infection by computer viruses, malicious code, etc.
- C*Cure , Solus and Prowatch system used to manage the physical access control system for overall Capgemini.
- Veritas NetBackup Exec is used to manage the data backup scheduling and monitoring.

PEOPLE

- **Executive Management**: Responsible for overall strategic direction and committed to provide adequate support and resources to establish, implement, operate, monitor, review, maintain and improve security & confidentiality principles and also overseeing of company-wide activities, and attainment of business objectives.

- **Operations Management and Staff**: Responsible for monitoring the controls implemented to determine whether the delegated security responsibilities have been discharged effectively. They also manage the Customer data for individual projects, new project initiation, user account authorization, client renewals and day to day customer support

- **Technology Services Group**: Responsible for implementation of all technical controls identified, managed, monitored, and supported within the information systems and responsible for the day-to-day maintenance of system integrity, security and availability of data. It is also responsible to keep the IT infrastructure functional at all times by implementing necessary controls.

- **Compliance Team**: Responsible for interacting directly with the Management Team on matters pertaining to the Compliance Program. The program consists of risk assessment, information security awareness training, communications, policy development, controls implementations, business continuity, security incident management and any new compliance initiatives with new standards as per Management directives.
- **Information Security Forum**: Responsible for the review of Information Security Management Systems and approving the information security policy, checking the effectiveness of security implementation of controls, analyzing cost effectiveness of security implementation, approval of security initiatives, initiating changes in policy to new business and technology requirements, engaging on Corrective and Preventive Action (CAPA) for first- and second-party audits.
- **Service Delivery Team:** Responsible for rendering client services which include claims processing (KFI, Audit and Revaluation).

DATA

Information assets, whether in electronic or in printed form, are classified based on criticality to determine information handling and protection procedures. Classification systems are consistent with the business requirements and consider the value and sensitivity, in terms of confidentiality, integrity and availability, of the information for the organization. Information assets are classified in the following categories:

- Public
- Company Confidential
- Company Restricted
- Company Sensitive

Rules for Data Classification have been defined as follows:

- Information stored in several media formats (either hard copy or electronic) have the same level of classification.
- The Information Classification Policy will be reviewed by the CISO (Chief Information Security Officer) at least once every year to update their classification and for considering exclusion/inclusion of items.

PROCEDURES

Capgemini has several policies and procedures that govern the day-to-day operations and management of IT Infrastructure, Human Resources, Facility Administration and all business operations, including physical and logical access and the proper handling of changes and incidents within the environment. These policies are available on the intranet.

Capgemini has developed formal policies and procedures across various business domains. Standard operating procedures are documented and implemented based on these policy guidelines. Policies and procedures implemented by Capgemini include:

- Recruitment and On-Boarding
- Compensation
- Exit Clearance
- Disciplinary Policy & Guidelines
- Employee Benefit
- Information Security Acceptable Usage
- Information Security
- Infrastructure Management
- Work Environment
- Change Management
- Security Incident Management
- Backup procedure
- Media Handling & Disposal
- Log Review
- IT Monitoring
- Privilege Access Management

CONTROL ENVIRONMENT

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

The main objective of ISMS is to protect information assets from unauthorized access, usage and to ensure confidentiality, integrity and availability of our information resources and services. Capgemini India has developed security policy based on Information Security Management System ("ISMS").

The ISMS policy is periodically reviewed and updated in consultation with the senior management. The ISMS principle is followed in formulating, implementing, monitoring and reviewing the policies periodically to suit the business objectives of the organization.
The primary responsibility of the Information security team is as below:

- Drive compliance with established policies through routine security evaluations and internal audits.
- Ensure compliance to ISO 27001 and any other client specific information security requirements.
- Monitor the technical aspect of security of Capgemini India through security operation center.
- Incident Management and Business Continuity Management

RISK ASSESSMENT

On an annual basis, Capgemini identifies the risks associated with their outsourcing services. Risks are mapped to internal controls to determine whether risks have been appropriately mitigated. Management accountability is assigned for each risk and control identified. Through the Account Management channel, Capgemini communicates with its key client contacts to better understand the client's risk and jointly plan to mitigate the risks.

RISK MANAGEMENT PROCESS

The risk management process is defined by way of a Risk Management Plan document prepared for each project. Capgemini has devised a formal process to identify and control risks associated with the delivery of Information Systems Projects ordered by clients, from pre-sale to acceptance and payment by the client of the last invoice for the project. Risk Management begins in the sales cycle at the time of proposing a client solution and ends when Capgemini has successfully completed the implementation and received final sign-off.

Risks related to the services provided to the client are regularly monitored by Capgemini senior management through M-Reviews. In addition to this Capgemini performs Risk Assessments on an annual basis to identify the risks related to information assets and services provided. Risks are mapped to internal controls to determine whether risks are appropriately mitigated.

INFORMATION AND COMMUNICATION

All Capgemini centres are part of a global service network and are consequently part of a global information and communication network. Formal corporate communications begin at the office of the Chief Executive Officer with regular company-wide communications and formal regional communications that are customized for each geographic/operational location and business unit. The communication framework provides for two-way communication that includes distribution of the corporate and operational unit organization structure, to allow ad hoc upward communication as well as periodic employee feedback surveys.

The relationship of risk assessment, delivery team operation and information and communication are established prior to the establishment of any new contract through team-based solution design and mandatory pre-contracting solution, risk, and contract economic reviews. The pre-sales communication structures are carried forward after contracting in transition and full delivery phases of contract services. Routine communications of risks, operational performance, economic performance, and client satisfaction provide the fundamental information and communication structures and linkage of centre performance and operational and executive management of Capgemini.

MONITORING ACTIVITIES

Operations and controls are monitored for each client at the account management, quality assurance and centre management levels.

Account Management – Upon completion of the contract, service level and quality monitoring processes are established to monitor and manage service level and quality performance defined. The account management team also establishes with the client both the OTACE client satisfaction criteria (or Equivalent) and frequency, generally quarterly, of measurement.

Quality/Compliance Team– For all contracts that meet certain size and complexity criteria, a quality assurance reviewer, independent from the delivery team and independent of the delivery center, performs a periodic audit of all aspects of delivery included in the contract.

Center Management – Management of the Delivery Center routinely monitor reporting of service level and quality measurements, quality assurance review reports, and client satisfaction results.

CAPGEMINI INDIA - INTERNAL REVIEW AND REPORTING MECHANISMS

INTERNAL AUDIT

Internal audits provide an independent evaluation of the extent to which projects and functions are complying with established procedures and to identify improvement opportunities in UNIQUE. Client satisfaction is used as a primary measure of system output, and the internal process audit is used as a primary tool for evaluating ongoing system compliance.

Internal Audit executes audits of projects along with quality groups and support functions (Group IT, Procurement, ICRES, Human Resources and Learning & Development). The Audit team plans for these audits with coverage of each project / support function on periodic basis. The results of each audit are documented in the audit report and sent to the auditees. Post-receipt of confirmation on the findings from the auditees, the audit report is published to the project's Senior Management. The audit report identifies all findings (observations and non-conformances) that require corrective and preventive actions. In addition to these, the audit reports also identify the leading practices from projects that can be implemented across the organization. The auditee implements corrective action plans for all observations and non-conformances identified during the audit and reports the results to the audit team.

During scheduled audits, the results of corrective actions taken in response to non-conformances identified in the previous audit are reviewed, to determine if they were effective. The Audit team does Non-Compliance ("NC") analysis on a periodic basis on the audit findings to address issues on recurrence during process implementation by identifying corresponding process improvements. NC analysis and corresponding steps are also discussed with Senior Management.

COMPLEMENTARY USER ENTITY CONTROLS

In the design of its controls, Capgemini has envisaged certain controls to be exercised by the user entities (complementary user entity controls.The responsibility for design, implementation and operating effectiveness of these controls rests with the user entities. This information has been provided to user entities and to their auditors to be taken into consideration when making assessments of control risk for user entities. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The list of complementary user entity controls presented below do not represent a comprehensive set of all the controls that should be employed by user entities.

- User entity is responsible for managing logical access of Capgemini's personnel to their network, applications and tools;
- User entity is responsible for communicating the needs and requirements for additional background verification and the timelines for completion.
- User entity is responsible for communicating the needs and requirements for video monitoring surveillance and video record retention for ODC and data centers/ server rooms.
- User entity is responsible for providing the network requirements for the restricted project areas.
- User entity is responsible for specifying requirements for physical and/or logical separation.