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,
Hinjewadi Phase-III, MIDC-SEZ,
Village Man, Taluka Mulshi,
Pune-411 057, Maharashtra, India

21 January 2026

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

KPMG Assurance and Consulting Services LLP (hereinafter referred to as "KPMG", "We", "Our") have completed SOC 3 examination for Capgemini Technology Services India Limited (hereinafter referred to as "Capgemini" or "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 20 January 2026. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 20 January 2026. 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.

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

Yours sincerely,

Anitha KS
Director
KPMG Assurance and Consulting Services LLP

SYSTEM AND ORGANIZATION CONTROLS (SOC 3) REPORT

Report on description of System supporting the general operating environment supporting the delivery of services 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 2024 to 30 September 2025

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 supporting the delivery of services to user entities ("System") were effective throughout the period 01 October 2024 through 30 September 2025, to provide reasonable assurance that Capgemini's 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's 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's 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's 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's 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's 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.

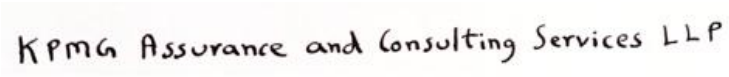
The firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality management including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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's System were effective throughout the period 01 October 2024 through 30 September 2025, to provide reasonable assurance that Capgemini's 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

20 January 2026

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 2024 through 30 September 2025, to provide reasonable assurance that Capgemini's 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 2024 through 30 September 2025, to provide reasonable assurance that Capgemini's 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's 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 2024 through 30 September 2025, to provide reasonable assurance that Capgemini's 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 providing general operating environment supporting the delivery of services i.e., HR, ICRES, GROUPIT, ISMS, BCM, LnD, Procurement, Corporate & Legal provided to Customers (hereinafter referred as "User Entity" or "Customers") from its delivery centers at the following locations:

Center	Address
Bengaluru	• Bengaluru 6B, Pritech Park SEZ, Bldg 6B, Bellandur Village, Vatu Hobli, Outer Ring Road Bengaluru – 560037, Karnataka, India • Bengaluru - Divyasree TechPark B5, A5 & B4, SEZ Divyasree Techno Park, IT/ITES SEZ SY No. 38(P) & 44/1, Kundalahalli, Whitefield, Bengaluru – 560037, Karnataka, India • Bengaluru - Dartmoor Building, No. 158-162 (P) & 165-170 (P), EPIP Phase II, Whitefield, Bengaluru – 560066, Karnataka, India • 155-156(P), EPIP Phase II, Whitefield, Bengaluru - 560066, Karnataka, India • 164-165 (P), EPIP Phase II, Whitefield, Bengaluru - 560066, Karnataka, India • Global Village IT SEZ, Lane - Pattanagere, Mylasandra Village, Off Mysore Road, RVCE Post, Bengaluru, 560059, India • Valdel,Vector Block, Prestige Technology Park III, Marathhalli, Sarajapur Outer Ring Road, Bengaluru, 560103 - 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. • ASV Chandilya Towers, No. 263/3B1A1, Door No: 5/397, Okkiam Thoraipakkam Village, Rajiv Gandhi Road (OMR) Chennai, Tamil Nadu – 600096, India.
Salem	• Capgemini Technology Services India Ltd., 41/52, PT Towers, Suramangalam Main Road,3 Roads Salem - 636009, Tamil Nadu, India.
Trichy	• Capgemini Technology Services India Limited, VRN Center No 37, VRN Centre, Bishop Road, Puthur, Trichy – 620017, Tamil Nadu, India. • 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, Maharashtra, India. • Mumbai M4, Plant No. 5, (Godrej IT Park), Godrej & Boyce Mfg Co Ltd, Pirojsha Nagar, LBS Marg, Vikhroli (West) Mumbai - 400079, Maharashtra, India.
Pune	• Capgemini Technology Services INDIA Ltd, Campus, A-1 Technology Park, MIDC, Talwade, Pune – 411062, Maharashtra, India. • Rajiv Gandhi Infotech Park, Plot No.14, Phase III MIDC SEZ, Village Man Taluka,

Center	Address
	Mulshi, Haveli, Hinjewadi, Pune – 411057, Maharashtra, India.
Hyderabad	• Campus site, Hyderabad Gachibowli, Survey no: 115/32&35, Nanakram Guda, Gachibowli, Hyderabad, Telangana – 500032, India. • GAR Corporation Pvt. Ltd, LAXMI INFOBAHN, IT/ITES SEZ, Sy. No. 107, GAR SEZ, Kokapet Village, Gandipet Mandal, Ranga Reddy District, Hyderabad, Telangana – 500075, India.
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, India.
Gandhinagar	• Capgemini Technology Services India Ltd., Fintech One,12th & 13th Floor Block No. 53, Road 5D and 52, Zone – 5, Village Ratanpur, Palaj, GIFT City, Gandhinagar – 382355, Gujarat, India
Gurugram	• Tower 6, IT/ITES SEZ, Candor Gurgaon One Realty Projects Pvt. Ltd., Village Tikri, Sector 48, Gurugram, Haryana – 122018, India. • Tower 5, IT/ITES SEZ, Candor Gurgaon One Realty Projects Pvt. Ltd., Village Tikri, Sector 48, Gurugram, Haryana 122018 • Tower 4, IT/ITES SEZ, Candor Gurgaon One Realty Projects Pvt. Ltd., Village Tikri, Sector 48, Gurugram, Haryana – 122018, India.
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
Coimbatore	• C Block, SF No 558/2, Udaiyampalayam Road, Hanudev Infopark Pvt Ltd, Nava India, Coimbatore – 641028, Tamil Nadu, 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 340,000 team members in more than 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.

SYSTEM OVERVIEW

COSO FRAMEWORK

The Committee of Sponsoring Organizations of the Treadway Commission ("COSO") was formed to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the Securities and Exchange Commission and other regulators, and for educational institutions. In 1992, it published Internal Control – Integrated Framework which presents a comprehensive model and objectives for corporate internal control.

COSO is the internal control integrated framework that has been adopted by Capgemini for use in design and analysis of its internal controls and for presentation in this report. While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time.

Figure 1: Components of Internal Control

Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. The components are:

- **Control Environment** – The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors.
- **Risk Assessment** – Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.
- **Control Activities** – Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as authorizations, verifications, reconciliations, and reviews of operating performance, security of assets and segregation of duties.
- **Information and Communication** – Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of

communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

- **Monitoring Activities** - Internal control systems need to be monitored through a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.

PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Capgemini designs its processes and procedures related to general operating environment supporting the delivery of services 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 ISO27001:2022 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.
- InTune 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, Coimbatore 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, Coimbatore 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).

The Local Area Network ("LAN") infrastructure is comprised of 100Mbps switched LAN comprising of Cisco Switches and Cisco Routers. The LAN is further divided into Virtual LANs ("VLANs). Client project networks are configured to operate in dedicated VLANs, where required by the client.

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, Coimbatore 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.

All the Client project users have access to the email server in CGSLAN, which is restricted through the Check Point firewall.

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 Corrections and Corrective Actions 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
- Customer 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

VISION

The business value of technology comes from and through people: Capgemini understands that business value cannot be achieved through technology alone. It starts with people: experts working together to get to the heart of your individual business objectives and develop the most adapted solutions to fit these requirements. We believe this human-centred approach to technology is what makes the difference for your business.

MISSION

With you we create and deliver business and technology solutions that fit your needs and drive the results you want: Capgemini enables you to transform your organization and improve performance. We aim to empower you to respond more quickly and intuitively to changing market dynamics. By bolstering your ability to harness the right technology, we help you become more agile and competitive.

Collaboration is central to the way we do business. Our experts join forces with your people to form a cohesive team. More than just a promise, our capacity to collaborate has become a key client expectation. We call this approach the Collaborative Business Experience. It shows in our every interaction and is our way of forging closer, more effective relationships.

'*People matter, results count.*'

VALUES

As the Group evolves, the seven values remain vital to Capgemini's development. Capgemini's decision-making and work at a company and individual level is guided by these principles. These seven values lie at the heart of everything that the Capgemini Group does. Values are important for respecting, defending, and upholding the Group as an ethical and responsible business and for protecting its reputation. The values are:

- **HONESTY** signifies loyalty, integrity, uprightness, a complete refusal to use any underhanded method to help win business or gain any kind of advantage. Neither growth nor profit nor independence have any real worth unless they are won through complete honesty and probity. And everyone in the Group knows that any lack of openness and integrity in our business dealings will be penalized at once.
- **BOLDNESS** which implies a flair for entrepreneurship and a desire to take considered risks and show commitment (naturally linked to a firm determination to uphold one's commitments). This is the very soul of competitiveness: firmness in making decisions or in forcing their implementation, an acceptance periodically to challenge one's orientations and the status quo.
- **TRUST** Meaning the willingness to empower both individuals and teams; to have decisions made as close as possible to the point where they will be put into practice. Trust also means giving priority, within the company, to real openness toward other people and the widest possible sharing of ideas and information.
- **FREEDOM** which means independence in thought, judgment and deeds, and entrepreneurial spirit, creativity. It also means tolerance, respect for others, for different cultures and customs: an essential quality in an international Group.
- **TEAM SPIRIT** meaning solidarity, friendship, fidelity, generosity, fairness in sharing the benefits of collective work; accepting responsibilities and an instinctive willingness to support common efforts when the storm is raging.
- **MODESTY** that is simplicity, the very opposite of affectation, pretension, pomposity, arrogance, and boastfulness. Simplicity is about being discreet, showing natural modesty, common sense, being attentive to others and taking the trouble to be understood by them. It is about being frank in work relationships, having a relaxed attitude, having a sense of humour.
- **FUN** Means feeling good about being part of the company or one's team, feeling proud of what one does, feeling a sense of accomplishment in the search for better quality and greater efficiency, feeling part of a challenging projects.

CORPORATE RESPONSIBILITY AND SUSTAINABILITY APPROACH

In today's unpredictable business environment, the need for responsible business practices is more critical than ever. We believe that corporate responsibility and sustainability deliver added value to our clients, employees, shareholders, business partners and the communities in which we live and operate.

Capgemini has achieved a position on the CDP (formerly Carbon Disclosure Project) 'A List'. The CDP Climate Performance Leadership Award Index recognizes our leading approach towards climate change mitigation. In doing so, Capgemini becomes

one of just ten French companies on the list. Capgemini has been identified as a leader by CDP for our significant contribution in driving environmental sustainability and climate change initiatives at a corporate level.

At Capgemini, the principles of corporate responsibility and sustainability go beyond legal compliance and philanthropy. They are embedded in our business, processes and ways of working. Our leadership in corporate responsibility and sustainable excellence is driven by a bold and influential approach that encompasses:

- **Values & Ethics**: **It's about who we are and the way we do business.** We embrace our core values of honesty, boldness, trust, freedom, solidarity, modesty and fun. Our rigorous Code of Business Ethics underpins our business practices, procurement behaviors and employee welfare policies.
- **Environmental Sustainability**: **We have a deep and measured understanding of our impact on the environment.** We are working to reduce our impact on the natural environment from energy, business travel and waste. We raise employee awareness on critical issues in sustainable development.
- **Community Engagement**: **We strive to have a positive impact on the communities in which we live and operate.** To do so, we work with local, national and international charities, NGOs and authorities on topics such as inclusivity and skills for the future. We support and encourage our employees to actively participate in community development.
- **People Culture**: **We aim to be the employer of choice for people who wish to flourish in a creative and diverse environment.** As a responsible and inclusive employer, we focus on the professional development and well-being of all our employees, with respect and value for their diversity. We ensure that our business practices and facilities empower delivery excellence.
- **Client Services**: **Our clients benefit from our deep understanding of sustainability and our world-class business transformation capabilities.** We incorporate customer dialogue and feedback to ensure long-lasting value and tangible results.

TRAINING

Particular attention is paid to the training of executives, account managers, and project leaders, as they play a key role in defining and implementing Capgemini's strategy. Capgemini's training policy uses a common global system called MyLearning, for which all Capgemini employees worldwide can register. This includes a catalogue of courses available either in the form of e-learning or as classroom teaching. The cornerstone of Capgemini's international training activities is its university at Les Fontaines (near Paris). The curriculum is focused on the most advanced skills development programs in order to impart training in new technologies and business practices.

New joiners undergo computer-based Cybersecurity training programs through MyLearning portal. Training records are maintained as an evidence of completion of training.

CODE OF BUSINESS ETHICS

Capgemini established an Ethics & Compliance Program in 2009. As a fundamental part of this program, Capgemini's values, rules and principles have been encapsulated in a formal Code of Business Ethics. The Code aims to explain the behavior that is expected from all of Capgemini employees, while at the same time relying on the employee's wisdom, judgment, and adherence to Group principles. The Code also requires leaders within the organization to have additional responsibilities with respect to Business Ethics.

Guided by the seven core values, the Code of Business Ethics comprises the following sections:

- **People**: To respect all health and safety applicable rules and contribute to a safe and inclusive work environment;
- **Business Integrity:** To act responsibly in the marketplace by complying with all applicable competition laws and regulations, complying with all applicable anti-bribery and anti- corruptions rules, by avoiding conflicts of interests and not to engage in insider trading, by providing accurate and correct business and financial information;
- **Business Relationships**: To build honest and clear relationships with clients, alliance or other business partners, and suppliers;
- **Group and Third-Party Assets**: Guarding intellectual property and confidential information, alongside the appropriate use of third-party assets and resources
- **Responsible Citizenship**: To support the communities and respect the environment in which Capgemini operates

To safeguard Capgemini's reputation and strengthen its competitive advantage, the Group launched an Ethics & Compliance Program to:

- Develop a sustainable ethical culture, which reinforces integrity and leads to ethical behavior
- Strengthen knowledge and awareness of international regulations and national laws and internal policies applicable in the

Group's companies
- Implement initiatives strengthening prevention and aiming at avoiding misconduct and breach in the field of ethics and compliance

Ethics do not allow for compromise since ethical behavior is, by definition, non-negotiable. Every single employee in the group, regardless of his or her position and level of seniority, should therefore, be aware of and comply with the Code of Business Ethics. New joiners are required to sign code of conduct and confidentiality/ non-disclosure agreement (NDA) which state their responsibilities towards maintaining confidentiality of Capgemini and its clients' information and also the legal implications of non- compliance. On an annual basis, employees are required to review the Code via on-line training. The goal of the online training is to help employees fully understand the Code and live its values and principles of action in their daily work. Completion of the training is tracked internally.

RAISING CONCERN PROCEDURE

The procedure for reporting concerns is mandated by Capgemini S.E. and implemented in each country in which the Group and all of its subsidiaries operate and is intended to operate in conjunction with the Code of Business Ethics. This procedure applies to all employees and is designed to be a readily available means for reporting concerns through internal channels. Furthermore, this procedure is designed to provide protections to all employees who report concerns in good faith, and to promote a workplace environment in which employees can raise concerns free from fear of retaliation.

The Raising Concern Procedure is intended for the reporting of concerns with regard to possible misconduct, fraud, wrongdoings, breaches of policies (including but not limited to the Code and the Blue Book), laws or regulations (including irregularities in accounting, auditing or banking matters, bribery, unfair competition or improper financial reporting related to the business of the Group and/or Company), or where the interests of the Group and/or Company or health and safety of any employee is at risk. The procedure provides a confidential mechanism for reporting and the matter is dealt with inside the Ethics function for each country. The procedure is posted on the internal intranet, and an annual reminder is sent out to employees.

For reports made under the Raising Concern Procedure, a preliminary assessment is conducted to determine the appropriate course of action. The Regional Ethics & Compliance Officer will either instruct the Internal Audit Department or other appropriate person to conduct an investigation. The Company, if possible, will acknowledge receipt of the reported concern to the reporting individual. During the investigation, the Company will always respect principles of fairness.

GROUP ANTI-CORRUPTION POLICY

Capgemini firmly believes that the Group's success is built upon honesty, the primary value of the Group—a longstanding commitment to act with high ethical standards and to conduct business legally and with integrity. The Code of Business Ethics reflects this commitment, stating principles and guidelines that define how the Group runs its business. This Anti-Corruption Policy focuses on one of the standards set out in the Code of Business Ethics, in the "Bribery and Corruption" section. Its purpose is to help Group company employees worldwide identify and avoid situations that could violate anti-corruption laws. It is written in a simple and practical manner, and it informs Group company employees of what they can and cannot do and where to find support. The Policy document explains what is considered as corrupt business practices and provides detailed practical guidance along with certain do's and don'ts. This Policy also extends to the Groups relationships with Third Parties and Suppliers.

Capgemini employees at all levels and at all locations are required to comply with the requirements of the Policy. The Policy document together with guidelines, training material and frequency asked questions (FAQs) are made available to all the employees through the Ethics and Compliance Hub on Talent.

CODE OF CONDUCT

All employees are issued the Capgemini employee handbook upon employment. The Capgemini Code of Conduct is detailed within the handbook. The Capgemini Code of Conduct is also available for review on the intranet; thus, making it readily available to all employees for review. Upon initial employment, all employees are issued the Acceptable Use of Information Technology and Telecommunications policy. All new employees are required to read the policy upon initial employment. Third party contracting agencies are required to sign master service agreements which address confidentiality and client information.

CLIENT DELIVERY ORGANIZATION

BUSINESS UNITS

Capgemini Group is composed of Strategic Business Units (SBU's) as follows:

- Americas and APAC SBU
- Europe SBU

- Global Financial Services SBU

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.

Business Units (BUs)

There are 15 Business Units, 8 within the Europe SBU (France, Germany, Italy, Netherlands, Scandinavia, Spain, UK, Europe Cluster), 3 within the Americas and APAC SBU (APAC, LatAm, North America), 4 within the Global FS SBU (APAC, Banking, Continental Europe, Insurance).

MARKET UNITS (MUS)

The Market Units orchestrate client relationships and sector perspective, working to profitably sell, deliver and grow the full Capgemini offering portfolio in these accounts. MUs common to many of our BUs are:

- Consumer Products, Retail & Distribution (CPRD)
- Energy, Utilities & Chemicals (EUC)
- Financial Services (FS)
- Manufacturing, Automotive & Life Sciences (MALS)
- Public Sector Services
- Telecom, Media & Technology (TMT)

Sogeti is a geographic Market Unit, within the Business Units, at the same level as sectorial Market Units. It aligns with the Group's unified Go-To-Market, while being coordinated at global level.

All the delivery projects in Capgemini India are executed from one of the above Business units. Business Unit leaders and Delivery Executives are assigned to each Business Unit. Primary responsibility of each Business unit is to deliver projects on time within budget with the required quality and achieve Client Satisfaction.

The Portfolio entities

The Global Business Lines (GBLs) and Application Business Lines have portfolio-related responsibilities such as managing the offering portfolio, taking care of pre-sales and solutioning, ensuring competitiveness and client focus on our delivery, and developing talents and managing people to ensure we are able to offer and develop the right skills and capabilities in established, high-growth, and emerging markets.

- **Global Business Lines (GBLs)**

  The Business Units work in close partnership with five Global Business Lines (GBLs) dedicated to developing and reinforcing our capabilities and expertise in domains that will be key growth drivers for Group in the years to come. 1- Business Services (BSv), 2- Cloud Infrastructure Services (CIS), 3- Insights & Data (I&D), 4- Capgemini Invent– bringing together Sogeti High-Tech and Product & Digital Engineering & Manufacturing Services to leverage the value of our expertise in Digital Engineering and help us accelerate in Digital Manufacturing. 5 – Capgemini Engineering.

- **Application Business Lines**

  The Application Business Lines support the Market Units with distinctive offerings, expertise and capabilities to increase our ability to win in the marketplace, and work to ensure client focus and competitiveness in our delivery. The Application Business Lines are as follows: Application Managed Services (AMS), Package-Based Services (PBS), Custom Software Development (CSD), Digital Customer Experience (DCX), Testing, Business & Technology Solutions (BTS), Practices specific to some SBUs/BU's.

ACIS now refers to as Americas, APAC, NCE & SCE SBU's, CIS (Cloud Infrastructure Services) GBL, I&D (Insights & Data) GBL, DCX, PBS, ER&D (Engineering, Research and Development), ADM GABL's & Sogeti BU's.

SUPPORT FUNCTIONS

India Corporate Real Estate Services ("ICRES") allocates work areas to the project teams as per contractual terms and conditions with the client organizations. It manages physical security of the premises, material movements in and out of office premises and is responsible for arranging and managing all transport facilities provided to the employees. It issues all access/identity cards that allow access to the main building premises to employees and authorized visitors.

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, Bengaluru, Hyderabad, Chennai, Salem, Trichy, Noida, Pune, Gandhinagar, Gurugram, Coimbatore 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.

Finance supports activities related to organizational accounting, reporting, employee time and expenses, invoicing, budget and forecasting and legal services.

Human Resources ("HR")
The HR group takes care of all activities related to recruitment, performance management, learning and development, payroll, and flexi-plan management (scheme under which employee can customize his/her compensation package) and international mobility.

Sales
This group is responsible for activities related to sales of services from Capgemini India. Sales handles development and maintenance of sales collateral, managing client visits, promoting Capgemini India capabilities within Capgemini groups worldwide and to external clients and prospects.

Procurement
India Procurement supports ~170,000 employees and ~13 locations- the largest across Capgemini globally. The procurement team supports business units and business functions to create 'Value for Money' proposition whilst ensuring the following benefits to the organization in particular.

- Increase spend visibility and spend under management.
- Find more savings, with better category management.
- Efficient sourcing strategies and price discovery.
- Better credit terms and payment strategies.
- Improve supplier performance through collaboration, assessment of the supply base, supplier groups, spend thresholds as well as supplier profile and risk.
- Drive compliance and follow policy guidelines.
- Control of maverick spending, better transaction management, and lean spend operations.

India Procurement is transforming into a broader ambition towards Total Cost of Ownership (TCO) reduction through categories management - namely Indirects, IT & Telco and external resource, to help us take thorough 'make or buy' decisions. As part of the new Capgemini supply chain model, the scope of Procurement is no longer limited to sourcing (suppliers, contracts, and costs) only, but will be going forward also be critical in securing the supply (quantity and quality) to address both internal and client needs.

QUALITY MANAGEMENT SYSTEM

Capgemini has many Global functions to enable delivery of its services and organizing the support activities. Group Delivery is enabling the business to follow process-based delivery. Similarly, Business Risk management, Group IT, Corporate Real Estate Services (CRES), Group HR and other functions are having a process-based work culture. Group Quality under the Group Delivery function is responsible for setting up the Quality Management System (QMS) and the SBU & Delivery center level Quality teams/Process/ Compliance teams are responsible for implementation of the process/standards and controls. The SBU & Delivery center level QA teams are responsible for checking the compliance and making relevant changes in the process through Group Quality. Every SBU function is having multiple Quality Standard certifications to handle the type of services and client expectations. Most commonly covered Certifications are ISO 9001, ISO 20000, AS 9100, ISO 27001 and CMMI Institute's Capability Maturity Model Integrated for Services constellation (CMMI-SVC 3.0). In addition, these units have lean and Six Sigma practices with strong analytic culture.

The Risks are evaluated at Business level and Delivery level as indicated in Group Blue Book. The Quality Analyst checks the delivery risks in their regular interaction.

Capgemini's Unified Quality Management for Excellence (UniQue), a part of Capgemini's Deliver Framework provides comprehensive coverage across multiple project types (Development, Maintenance, Testing, Production Support and Infrastructure Management) and lifecycles. It is an end-to-end framework for managing the complete organizational processes beginning from relationship management, Governance, Accelerated Development Centres, Program and Project Management, Sales, Development, Lifecycles, Support and Continuous Improvement Processes.

Refer to the exhibit below for an illustration of the key areas addressed by the **Integrated Quality Management System.**

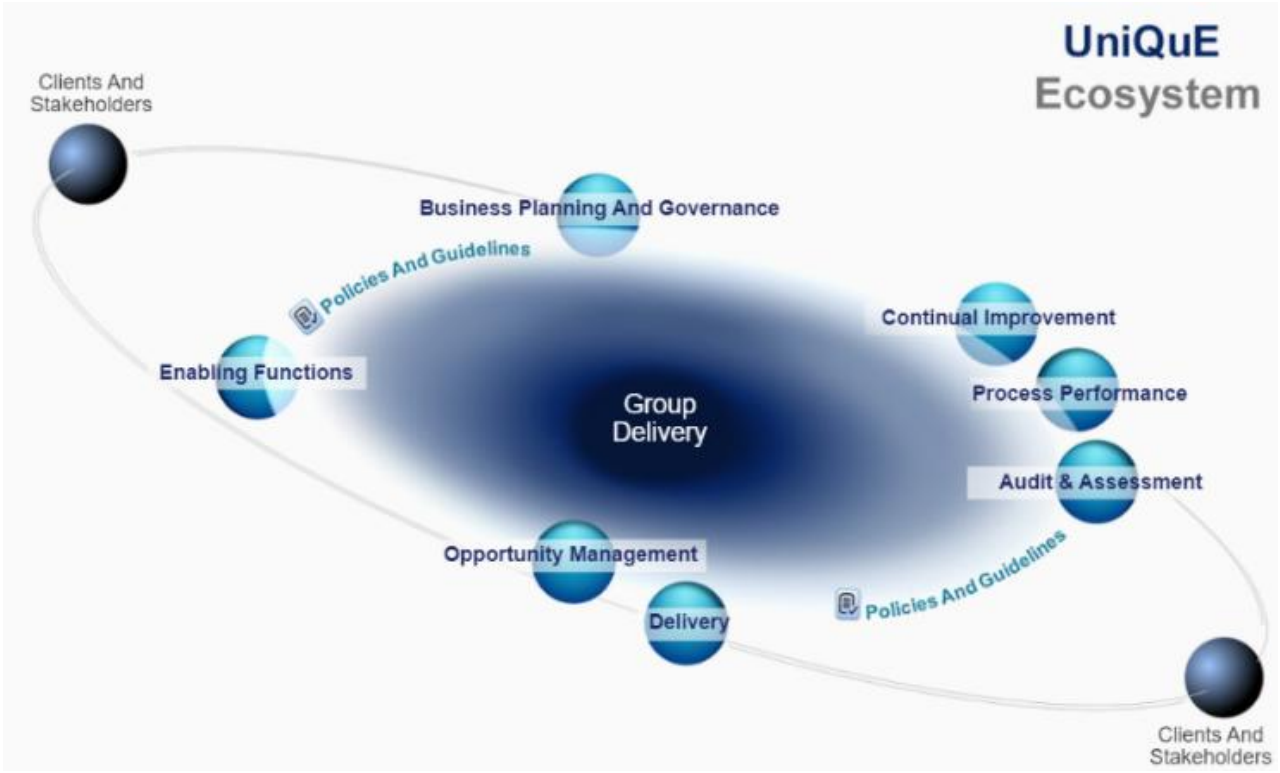


Figure 2: Integrated Quality Management System

QUALITY POLICY

Capgemini' s Quality Policy is *"Capgemini is committed to satisfy customer expectations by delivering solutions and services through state-of-the-art processes and continual improvement frameworks in line with contractual, statutory and regulatory requirements."*

The key objectives of CAPGEMINI's Quality Policy are to:

- Deliver engagement/projects on time as agreed with the client.
- Establish engagement/project management procedures that create transparency and eliminate surprises.
- Establish continuous improvement in processes based on SEI's Capability Maturity Model Integrated CMMI Services V3.0 ML5, ISO 9001, SSAE18/ISAE3402, ISO 20000, ISO 27001 and PCI DSS Standards.
- Attain superior customer satisfaction as defined by the Clients.

The following certifications have been obtained by Capgemini India, with reference to quality and information security standards:

Item #	Certification	Certification Date (MM/DD/YY)	Service Provider Comments
1.	ISO 9001:2015	01/Nov/2019 to 31/Oct/2028	• Scope of the certificate includes Provision of information technology solutions including application development and maintenance, application management, 'data, AI & analytics' platforms and services, testing services, infrastructure services, 'digital engineering and manufacturing' services, consulting services and business process outsourcing services. || Countries: Argentina, Australia, Austria, Brazil, Belgium, China Colombia, Czech Republic, Denmark, Egypt, France, Finland, Germany, Hungary, India, Japan Luxembourg, Mexico, Morocco, Netherlands, New Zealand, Norway, Philippines, Poland, Romania, Sweden, Tunisia, Ukraine, United Kingdom, USA and Vietnam || Certifying Body: DNV
		02/Jul/2023 to 01/Jul/2026	• Scope of the certificate includes provision of Cloud Infrastructure Services at Capgemini Australia, Belgium,

			Canada, Finland, France, Germany, India, Italy, Poland, Romania, Spain, Sweden, Switzerland, Netherlands, United Kingdom and United States of America || Certifying Body: BSI
2	ISO 20000-1:2018	02/Jul/2023 to 01/Jul/2026	• Scope of the certificate includes provision of Cloud Infrastructure Services at Capgemini Australia, Belgium, Canada, Finland, France, Germany, India, Italy, Poland, Romania, Spain, Sweden, Switzerland, Netherlands, United Kingdom and United States of America || Certifying Body: BSI
		22/Oct/2024 to 19/Dec/2027	• Scope of the certificate includes The Information Technology Service Management System that covers the provision of Application Management and Infrastructure Management services by Capgemini Technology Services Limited to its customers covering locations from India at Mumbai, Bangalore, Kolkata, Hyderabad, Gurugram, Pune and Chennai. This is in accordance with Capgemini India's latest version of Service Catalogue for Application Management services || Country: India || Certifying Body: BSI
3	ISO 27001:2022	15/Oct/2024 to 14/Oct/2027	• Scope of the certificate includes Information security management system for delivery of business process outsourcing services in accordance with statement of applicability version 9.0 update 1 dated 22nd March 2024 || Countries: China, India, Poland, Brazil, Guatemala, Philippines, Egypt, Mexico, Romania, Netherlands and France
		04/May/2023 to 03/May/2026	• Scope of the certificate includes The provision of IT and Engineering services including Applications Managed Services, Consulting, Technology and Outsourcing Services and governed by Group Cybersecurity and Group IT, covering those services provided by Capgemini's Cloud Infrastructure Services (CIS), Engineering (ER&D), Financial Services (FS), Insights and Data (I&D), Invent and Sogeti Global Business Lines (GBLs) and Strategic Business Units (SBUs) in Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Colombia, Czech Republic, Denmark, Egypt, Finland, France, Germany, Hong Kong, Hungary, Ireland, India, Italy, Japan, Luxembourg, Malaysia, Mexico, Morocco, New Zealand, Norway, Philippines, Poland, Portugal, Romania, Singapore, Spain, Sweden, Switzerland, Netherlands, United Kingdom, USA and Vietnam. This is in accordance with Statement of Applicability version 3.2 dated 2 October 2024. || Certifying Body: BSI
4	ISO 27701:2019	15/Oct/2024 to 14/Oct/2027	• Scope of the certificate includes Privacy Information management system for delivery of business process outsourcing services with the role as 'PII Processor' in accordance with statement of applicability version 9.0 update 1 dated 22nd March 2024. || Countries: India, Brazil, Poland, Philippines, Guatemala, China, France, Netherlands, Egypt, Mexico, Romania || Certifying Body: DNV
5	CMMI Services V3.0 (CMMI-SVC) without SAM - ML5	31/Jul/2024 to 31/Jul/2027	• Scope of the certificate includes Application Development and Maintenance (ADM) Engagements in steady state. || Certifying Body: QAI /CMMI Institute
6	CMMI Dev ML5 V3.0	19/Nov/2024 to 19/Nov/2027	• Scope of the certificate includes FS SBU – Agile Development Full Lifecycle (FLC) projects managed under the framework of QMS. || Country: India || SBU: Global FS || Certifying Body: QAI /CMMI Institute
7	ISO 22301:2019	24/Sep/2022 to 23/Sep/2028	• Scope of the certificate includes Management of Business Continuity to Financial Services accounts pertaining to Banking, Capital Markets and Insurance and all Support functions

			(ICRES, Group IT, HR) || Country: India || SBU: FS SBU || Certifying Body: BSI
		15/Oct/2024 to 14/Oct/2027	• Scope of the certificate includes Delivery of business process outsourcing services. || Country: China, India, Poland, Brazil, Guatemala, Philippines, Egypt, Mexico, Romania, France, Netherlands || Certifying Body: DNV
		13/Oct/2023 to 12/Oct/2026	• Scope of the certificate includes the management of Business Continuity applies to Consulting, Technology and Outsourcing services of its business units namely 'Northern and Central Europe' (NCE), 'Southern and Central Europe' (SCE), Americas SBU India' (NA), 'APAC SBU', 'Capgemini Engineering', 'Capgemini Invent', 'Insights and Data' (I&D), 'Cloud Infrastructure Services (CIS) India', 'DCX India', 'Global Packaged Based Solutions' (PBS), 'Cloud and Custom Apps (C&CA)', Global ADM Practice (GADM); Sogeti; and all supporting functions i.e. Group IT, Human Resources (HR), Facilities (ICRES), Quality and Finance operating from India. || Country: India || Certifying Body: BSI
8	PCI DSS V4.0	13/Feb/2025 to 12/Feb/2026	• Scope of the certificate includes Financial Services Strategic Business Unit. Development, testing and support for applications supporting cardholder data of their customers. || Country: India || Certifying Body: BSI

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"). This framework has been developed as part of the International Organization for Standardization ISO 27001 certification, which covers the following:

- Acceptable IT Usage Policy
- Access Control Policy
- Backup and Restore Policy
- ISMS Policy Manual
- ISMS Scope Document
- ISMS Policy Framework
- Risk Assessment Methodology
- Password Policy

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

Capgemini has a documented Information Security Policy and Procedure that is approved by Management. This is made available to employees through the Capgemini Intranet Site. New joiners agree to abide by these policies and procedures by signing the offer letter. Changes to policies and procedures are made as needed and are communicated to relevant employees.

Capgemini policies and instructions on compliance are communicated to all employees regularly through standard communication methods.

CONTINUITY FOCUS

Capgemini India has set up a BCM committee at the Group and India level with the top management directly involved in setting up the directives. Capgemini implements BCM at the account and center level as well. Capgemini has set up an intranet portal with comprehensive information on Government Advisories, Internal protocols, Travel and meetings, client communication, Office protocols.

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.

Capgemini as well as all subsidiaries and any companies at least 50% owned, either directly or indirectly, are insured for possible financial losses resulting from general or professional liability claims arising in the course of their business. The coverage has been taken out with several different insurance companies as part of a worldwide program. The terms and conditions of the program, including coverage ceilings, are reviewed and adjusted periodically in order to take into account any changes in Capgemini' s revenues, businesses, and risks. Due to the wide geographical dispersion of its operations, insurance coverage for property damage and business interruption is managed at the local level, according to the value of the property, the nature of operations in each business site and the risks involved.

CAPGEMINI SBU - 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.

Following are the important processes in Risk Management Process

- **Initiate Risk Management** - The purpose of this activity is to consolidate all significant risks related to this project into a risk list and if required, establish a tailored set of procedures for risk management, specific for the project.
- **Assess Risk** - The objective of this activity is to identify and record risks to the project, to assess their potential impact, to define the risk containment and review the impact on business risk.
- **Monitor Risks** - Risks are tracked on a weekly basis. Risks are reported in weekly status report along with the risk containment plan.
- **Complete Risk Management** - Some of the risks that have been identified and managed in the course of the project might still be a threat to the project success at the time when the involvement of Capgemini in the project is ending. In this case, Capgemini transfers all pertinent risk information to the party that is carrying on the work be it the client, a Capgemini SBU operations team, or a third party.

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.

SYSTEM CHARACTERIZATION

The boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization [or accreditation] boundaries, and provides information [e.g., hardware, software, system connectivity, and responsible division or support personnel] essential to defining the risk.

LIKELIHOOD DETERMINATION

Based on the Risk and the frequency at which it can be realized the Likelihood is determined. Any limitation in the system can create a chance for increased likelihood.

IMPACT ANALYSIS

The adverse impact of a security event will be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality.

RISK DETERMINATION

The determination of risk exposure can be expressed as a function of:

- The likelihood of a given risk getting realized.

- The magnitude of the impact the risk to which it can create challenges/adverse results.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix is developed. Probability and value are assigned for each impact level.

CONTROL RECOMMENDATION

Controls that could mitigate the identified risks, as appropriate to the organization's operations, are identified. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.

RISK MITIGATION

Risk mitigation can be achieved through any of the following risk mitigation options:

- *Risk Assumption* - To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- *Risk Limitation* - To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability [e.g., use of supporting, preventive, detective controls].
- *Risk Planning* - To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- *Risk Transference* - To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Senior management knowing the potential risks, has authority to implement new controls or improve existing ones in spite of the value of total risk. Senior Management decided on implementing new controls or improvement in existing processes and determines the following:

- Residual risk value in terms of new controls,
- Implication of implementing new controls, and
- Owner who will implement new controls.

ORGANIZATIONAL STRUCTURE

Figure 3: India Organization Structure

Roles and responsibilities including formal job descriptions are maintained to delineate employee skill requirement, responsibilities and reporting structure.

CAPGEMINI GROUP EXECUTIVE COMMITTEE

The Group Executive Committee is comprised of 25 members, including the nine members of the Group Executive Board. The Group Executive Board is in charge of ensuring the collective management of the Group at an operational level.

The Group Executive Committee helps define Capgemini's main strategies. It sets the strategic priorities and the resulting action plans. It ensures that these plans are effectively implemented at the operational level.

Group Delivery

Group delivery function is further subdivided into Group Delivery Risk, Group Quality, Resource Supply chain and Group Delivery HR. These functions are connected to the Business Units and Global business lines to enable standard delivery practices and compliance.

Group IT

Group IT is under Group CIO. The functions Global infrastructure, Global Applications, IT Security, Business partners and Office of CIO and Enterprise architecture operates. They support all the Business Units and Global Business line to operate successfully with required secure infrastructure.

Group Cybersecurity

Group Chief Cybersecurity officer leads the function. They are connected with Business Units and Global Business lines chief Information Security Officers (CISO).

INDIA OPERATIONS

India Operations are led by the Chief Executive Officer (CEO) and supported by Chief Operating Officers (COO). The function like CRES, HR, Quality/Compliance, Business Risk management, Marketing Communication, India offshore leaders of BU and others are operating in this umbrella.

BOARD OF DIRECTORS

The Board of Directors of Capgemini represents all shareholders collectively. It acts at all times in the interests of the Group, and determines overall strategies and oversees their implementation. All major strategic decisions and decisions material to the financial position or the commitments of the Group must receive prior approval from the Board of Directors.

The Board of Directors has set up several specialized committees (the "Committees") which derive from it and which act under its authority. They are responsible for examining or preparing matters falling within their terms of reference, making proposals and formulating opinions to the Board of Directors concerning decisions to be made by the Board of Directors.

The Audit Committee whose charter is to follow-up questions concerning the preparation and control of accounting and financial information and to assess the appropriateness of Group accounting standards and the consistency of the accounting principles and methods used in the preparation of the consolidated and statutory financial statements. It checks the efficiency of internal control and risk management procedures and ensures the quality process to prepare published information. The Committee evaluates the various engagements conducted by the statutory auditors and gives an opinion as to whether they should be reappointed.

The Ethics & Governance Committee first mission is to ascertain the conformity and results of actions implemented to ensure the promotion and respect of the seven core Values, notably the strict application of the Group's ethical principles, the practices related to the management of staff, the compliance of commercial partnerships and alliances with the values of Honesty and Freedom of judgment, enabling the guarantee of the Group's full independence, and the application of prudential rules regarding relations with shareholders and financial markets, and information supplied to them.

It is also tasked more generally with overseeing the application of best corporate governance practice within Cap Gemini S.A. and its main subsidiaries.

The Board of Directors (Board) has ultimate responsibility for overseeing the business policies of Capgemini. The Board meets at least once per quarter to discuss matters of Capgemini operations and to review financial results. Some of the items reviewed at the Board meetings include:

- Monitoring of various customer contracts and contribution margins;
- Annual business plan;
- Annual working capital requirements /declaration or distribution of dividend;
- Financial results;
- Appointment of key personnel, bankers or auditors; and

- Statutory compliance.
- The various policies of the organization are a reflection of the importance the Board gives to business and ethical values and commitment to competence.

ORGANIZATION STRUCTURE – MANAGING PROJECT

The Capgemini team supporting client projects in the service units specified by the Capgemini India is split between three different entities - Capgemini global offices: Capgemini India project team and the Client. The Capgemini global team provides front-end support and maintains communication and relationship with the client. The Capgemini India team provides back-end support and is responsible for maintenance, design, development, and testing services.

- **The Capgemini Global Office team** is responsible for contractual commitments for client service delivery. They hold the overall responsibility for delivery and are also responsible for the project management of the team, both Capgemini Global Office and delivery centers in India. The project management team at India is responsible for project management and delivery at the India centers and for liaison with Capgemini Global Office teams.
- **Project Management Office ("PMO")** consists of engagement managers, project managers and account coordinators from the on-site team and Capgemini India. The PMO is responsible for managing inter-group issues (and their escalations), scope changes, risks and management communications.
- **Development Team** – The Back Office (Capgemini India) development team assists the on-site team in defining the details of the application design, developing the application according to the high/low level design documents, conducting unit test, peer review and fixing trouble tickets raised by internal/client testers before or after the application is moved into production. It also ensures conformance to Group Unique (QMS) standards.
- **Testing Team** – Testing team prepares test cases, test data, conducts testing, reports defects and coordinates with the application development team to help ensure that all defects reported are closed and re-tested before releasing the code.

CAPACITY MANAGEMENT

Capacity Management's function is to provide a single point of ownership and management for all capacity and performance related issues encompassing IT services and resources. The goal of the Capacity Management process is to ensure that cost-justifiable IT capacity across all areas of IT is available and corresponds to both the current and future agreed needs of the business, in a timely manner'. Monitoring tools are utilized to examine system/ network capacity and availability at any given point of time. Incidents are raised if defined capacity and availability thresholds are exceeded and are classified as per the priority for resolution by the concerned teams. Major objectives are:

- Provide expert support to the business and IT on capacity and performance related matters including assistance with the diagnosis and resolution of performance and capacity related incidents and problems.
- Management of the performance and capacity of IT services and resources to ensure that all measured performance targets are met or exceeded.
- Assess the impact of all changes to the current and future capacity and consider the impact to all services and resources.
- Ensure that cost-justifiable proactive measures to improve the performance of services are implemented.

INFORMATION AND COMMUNICATION

CAPGEMINI

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.

DESCRIPTION OF INFORMATION SYSTEMS

LAN AND WAN ARCHITECTURE

All In-scope sites (Mumbai, Bengaluru, Hyderabad, Pune, Chennai, Salem, Trichy, Noida, Gurugram, Gandhinagar, Coimbatore 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 centres. Other shared servers like the email server and domain server are hosted within the data centre. Our facilities are connected by fibre optic cable. Data centres at each location also host critical communication devices like routers and the call manager 'VoIP '(Voice over IP).

The Local Area Network ("LAN") infrastructure is comprised of 100Mbps switched LAN comprising of Cisco Switches and Cisco Routers. The LAN is further divided into Virtual LANs ("VLANs). Client project networks are configured to operate in dedicated VLANs, where required by the client.

Based on client requirements, client project networks are separated from the Capgemini India corporate network, in Mumbai, Bengaluru, Hyderabad, Pune, Chennai, Salem, Trichy, Noida, Gurugram, Gandhinagar, Coimbatore and Kolkata Centres, 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 proxy configuration and content filtering. The proxy filters content and blocks access to non-business categories.

All the Client project users have access to the email server in CGSLAN, which is restricted through the Check Point firewall.

PROCESS OVERVIEW

RECRUITMENT AND RESOURCE MANAGEMENT

The recruitment and resource management process are documented as part of the Capgemini India Human Resources procedures. The key processes involved in recruitment and resource management are described below:

Recruitment

- Recruitment for all positions is initiated based on a Service Order (SO) appropriately filled in by the recruiting project manager/engagement manager and approved by the respective Practice Leader and HR.
- The sourcing process is handled by the HR department, which first advertises the open position internally inviting deserving candidates and referrals. Subsequently, the requirement positions are advertised to external agencies and newspapers.
- Basic educational qualifications and academic performance standards have been defined to qualify for an interview. The candidate must be willing to work on such shift timing, which allows work time overlap with teams in other geographies.
- Profiling tests are performed to understand the behavioral pattern of the candidate.
- All hiring decisions are subject to requisite approvals.
- The joining formalities include submission of various testimonials, performing applicable reference checks and obtaining a background check report if it is mandated by the client to work on specific projects.

There exists a defined and documented selection criterion for hiring the new employees. The lateral candidates are evaluated for fitment to the positions by the Technical (as applicable) and HR team member during the interview process. The campus hires are evaluated for fitment to the positions by the technical team member only at the time of interview process.

Formal background checks (BGV) are performed for the Capgemini new joiners and the background verification reports are maintained. The following aspects are verified during the background check:

- Educational qualification check - highest degree obtained; and
- Work experience – previous two employments or 5 years' prior work experience (whichever is higher).

For applicable cases, client given background verification criteria is adopted and additional background checks are conducted. For unsatisfactory results from background checks, appropriate actions are taken. Background verification is not performed for those employees who were rebadged on account of an acquisition. Background verification is not performed for contract employees.

Resource Management

- The project team lead is responsible for providing Assignment Review (AR) to each project team member and inputs to the local counselor and/or project team leader.
- The offshore project/team leaders are responsible to obtain feedback from the Capgemini global office team. Additional inputs or special mention beyond the typical feedback are provided at the discretion of the Capgemini global office project team.
- The incentive/bonus program is common at the corporate level (Capgemini India) and is decided on the basis of overall performance ratings of the member.

LOGICAL ACCESS TO NETWORK

Domain access for new joiners is enabled after the onboarding flag is checked in the HR system. There exists an approved Work Order (WO) for new domain accounts created for subcontractors. Domain access is created in advance for Grade E and above employees. Domain access for leavers is revoked by Group IT team within two business days from last working day. The authority to create and manage employee records in the HR System is segregated from the authority to create and administer accounts on the corporate domain. The monthly review of current Capgemini domain administrators is performed by the appropriate functional manager or delegate. The password parameters for corporate network are configured in line with the documented and approved password policy.

PHYSICAL AND ENVIRONMENTAL SECURITY

Access to the premises is authorized either by usage of appropriate access cards or by controls maintained by the reception desk. There are 24x7 security guards at the main entrance to the buildings to monitor the movement of people and equipment into and out of the premises. The employees are required to wear access cards at all times when inside the facilities, which carry the photographs of the employees. Employees who report for work without their access cards are required to enter their details in an interim/ temporary access card register before they are issued a visitor pass /temporary access card for the day. Logging

of entry/exit in the register maintained by the security guards is mandatory for access during non-working hours and on holidays. All visitors to the premises are required to record details in the visitor register / Visitor Management System (VMS) present atthe main entrance and are accompanied by Capgemini employees throughout their time in the premises. Employees and Contractors that do not have access rights to data centres/ server rooms are escorted by Security Personnel/IT team member. Entry/exit of such associates is logged in the visitor register maintained by ICRES in the data centres/ server rooms.

Access to server rooms/data centers is further secured by access card privilege combined with biometrics access restrictions to authorized Group IT personnel only. Group IT personnel must accompany all other employees, subcontractors, vendors and service providers and the entry/exit should be logged in the register maintained by the Group IT.

Physical access for the new joiners to the facilities is granted based on requests sent by HR team. Physical access to the facilities and client dedicated ODCs is controlled through proximity-based access control system. Physical access to the server rooms/data centres is controlled through two factor authentication mechanism. Physical access to client dedicated ODC requires approval from authorized individual from the project or allocation email by staffing team to ICRES team. Physical access to the data centre/ server room is granted by ICRES team only on approval from the authorized personnel from IT team.

Access to restricted project work areas is controlled by access cards configured with specific access privileges for the authorized project team members only. Access into such areas is not allowed to non-project personnel unless formally approved by the respective project manager. Real time monitoring is enabled on data centers/server rooms. Access to the data centers/ server rooms is monitored and the notification is sent to managers for unsuccessful access attempts. Entry/Exit points to ODC and data centres/ server rooms are under video monitoring surveillance as per client requirements/ Capgemini policy as applicable.

The following server rooms are covered with adequate controls mentioned in this report:

City	Site Name
Bengaluru	EPIP & DTP
Mumbai	IT3/IT4 B3 & IT3/IT4 B5
Gurugram	Candor Tower 5

The ICRES team deactivates the access card of resigned employees within two business days from the last working day. When an employee is off boarded from a client dedicated ODC or data center/ server room, ICRES team revokes the physical access to the respective ODC, or data center/ server room based on the e-mail request/last working date.

Server rooms/data centers are installed with fire and smoke detectors and fire extinguishers. Fire alarms are tested, and fire suppression systems are reviewed periodically, and corrective actions are taken, if required. Server rooms/data centers are provided with uninterrupted power supply systems (UPS) and backup power generators. UPS and generators are maintained periodically. Temperature inside the server rooms/data centres is controlled and monitored to protect the equipment against extreme temperature and humidity. Temperature control equipment are maintained periodically. Air conditioners are installed in the server room/data center to maintain the temperature. The temperature in the server room/data center is monitored manually on an hourly basis and any deviation from the defined temperature range is notified to the administration. The devices installed to protect against environmental hazards are periodically inspected. Servers in the server rooms/data centers are stored on raised floor.

NETWORK SECURITY

Layered network architecture is achieved with network segmentation using External, Internal DMZ and VLAN. Access controls lists are enabled on inter-VLAN traffic. The infrastructure is protected with the help of Firewalls and Intrusion detection and prevention system. Network Intrusion Prevention System is configured on the network to detect unauthorized activity and prevent virus/worm or intrusion attacks. The updates of Intrusion Prevention System (IPS) signatures are performed when signatures are released by the vendor. Data is encrypted before transmission over public networks. Communications over public networks are controlled through a firewall. Next generation, perimeter firewall configuration and rule sets are reviewed Monthly by the Network team. Access to change the firewall rule sets is restricted to authorized personnel. Customer communications over public networks are encrypted. Based on the or the communication from the project team, client specific projects networks are physically/logically separated from each other and from the Capgemini India internal network by Group IT. Network usage is also monitored for abnormal network traffic behaviour to check virus/worm propagation. Critical assets are configured into Security Information and Event Management (SIEM) tool to protect against cyber threats. Group IT team performs vulnerability assessment monthly. Penetration Testing is conducted on an annual basis. A report is created identifying issues and exposures found during testing. Issues and exposures found are reviewed and tracked.

DESKTOP SECURITY

Active Directory and single sign on authentication are used and local security policies are enforced through GPO. Security patches are applied through Microsoft Intune. Workstations and servers have anti-virus software installed.

Password-protected screen saver is enabled.

CROWD STRIKE

CrowdStrike is a next generation anti-virus powered by machine learning to ensure breaches are stopped before they occur. CrowdStrike antivirus/ antimalware, threat response, anomaly detection capabilities provide comprehensive endpoint monitoring and protection. CrowdStrike has no signatures and has a lightweight sensor with minimal footprint (0-2% CPU, 40MB Client).

Servers and workstations are installed with EDR and periodically updated. EDR is configured to block malicious software being run on the end user workstations, based on the hash configuration. Antivirus Endpoint Protection is configured to disable removable media on workstations.

MOBILE DEVICES

Capgemini offers secure access email on mobile device, as part of our Bring Your Own Device (BYOD) policy using InTune MDM.

Utmost care is taken to ensure that these devices do not pose a security risk when connecting to the Capgemini corporate network or accessing corporate data. Privileged company information and applications needs to be protected.

Emails can be accessed on mobile devices as per Capgemini's Bring Your Own Device (BYOD) policy using InTune MDM.

MICROSOFT INTUNE

Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints. It has below mentioned key features and benefits.

1. Intune simplifies app management with a built-in app experience, including app deployment, updates, and removal.
2. Intune automates policy deployment for apps, security, device configuration, compliance, conditional access.
3. Intune integrates with mobile threat defense services, including Microsoft Defender for Endpoint and third-party partner services.

For end users accessing Capgemini data/network using mobile device, password parameters on the mobile device are enforced via MDM. These password parameters are defined in Enterprise Mobility Management Policy for Mobile Device.

Configuration to remotely delete company specific data from end user mobile device is enabled on MDM platforms.

End user access to Capgemini data on mobile device through MDM (VMWare Workspace one) is integrated to Capgemini active directory.

ZSCALER CONTEXTUAL ACCESS

Group IT and Group Cybersecurity have jointly implemented Contextual Access, which strengthens online protection and connects users to Capgemini applications in a simpler and more secure way. Contextual Access is enabled by the Zscaler Client Connector, which has been automatically installed on Capgemini Intune-enrolled laptops.

The Zscaler solution, as implemented within the Contextual Access project, contains three main components:

Zscaler Client Connector (ZCC) is the Zscaler agent/app that is installed through Intune on all Capgemini-managed devices. Once enabled, ZCC connects the device to the control plane and ensures that all access requests are handled according to the security policies defined on the control plane.

Zscaler Internet Access (ZIA) secures access to Internet resources (websites), Internet-based applications (SaaS), and, potentially, customer-provided resources that need to be accessed to manage that particular customer. Access to internet-based applications is secured by setting dedicated access policies for the applications and access to the normal internet is based on the Capgemini Internet Access policy.

Zscaler Private Access (ZPA) secures access to Capgemini's private applications. These are hosted in our own datacenters or in our private instances in the public cloud.

ZPA eliminates the need for users to be 'on the network' and does not require the applications to be published on the internet and therefore removes the risks.

This means that all access will first be verified and monitored so that we can proactively identify and respond to potential threats. This will allow us to simplify network connectivity and ensure all access to network resources is controlled and secure.

INFORMATION SECURITY INCIDENT RESPONSE

Capgemini has a documented Information Security Policy and Procedure that is approved by Management. This is made available to employees through the Capgemini Intranet Site. New joiners agree to abide by these policies and procedures by signing the offer letter. Changes to policies and procedures are made as needed and are communicated to relevant employees.

All the IT and non-IT security incidents which directly or indirectly breach the information security policy are managed by Information Security Incident Management Procedure. This process specifies procedures for notification, escalation, resolution, and documentation.

The Security Operation Centre pro-actively monitors internal and external environment to fine-tune security controls in accordance to evolving threats. The users are required to report any incidents to ISMS Team either by email or by informing to ISMS Team member. The team is responsible for coordinating the investigation, closure of findings and corrective action.

DATA SECURITY

Security controls are placed in operation to ensure safeguarding of data in its complete lifecycle (i.e., "data at rest", "data in transit" and "data in disposal").

- Access to the Capgemini's internal network resources is provided on need-to-know basis and after appropriate approvals.
- In case of access to clients' network resources –
- Individual project teams in Capgemini India are responsible only for requesting the accesses to clients' network resources.
- Accesses are either granted by Client or Capgemini Onshore Team.
- Accesses are requested through methods and practices suggested by each individual client.
- Hard disk encryption for all workstations is mandatory.
- Standard hardened OS image is used on all workstations.
- Real-time monitoring of security events through security operation center.
- Data is backed up on daily, weekly and monthly basis based on contractual needs.

SECURITY AWARENESS

Employee security awareness sessions are conducted on regular basis. All employees are required to attend mandatory training on information security through group security module and also specific trainings are conducted to employees. These awareness programs explain the need for information security and provide the user community with adequate security training.

DATA BACKUP MANAGEMENT

There exists an approved backup policy. The backup policy defines the schedule for performing data backup and restoration. Servers (which are managed by Group IT) are configured in the backup tool for periodic backup. Backup failures are logged, monitored, and resolved. Restoration testing of backup is performed on a periodic basis. Discrepancies identified if any, are resolved.

INCIDENT MANAGEMENT

There exists an approved incident management policy. The incident management policy defines the incident resolution procedures and escalation matrix. Infrastructure related security incidents are logged, prioritized, and assigned to appropriate team / person. Incidents are analyzed and resolved. Escalation procedures are documented and followed. Resolutions are documented. SLA compliance as agreed upon with the business was monitored monthly. Critical incidents and incidents remaining unresolved for a long time are reviewed periodically. Critical assets are configured into Security Information and Event Management (SIEM) tool to protect against cyber threats. (This is not applicable to access switches).

CHANGE MANAGEMENT

A formal change management process exists and is approved by management. For Global Infra Support changes, impact assessment documents are prepared and approved by appropriate personnel Changes to production environment are implemented only after receiving approval from the appropriate personnel in accordance with the procedures outlined in the change management policy and process documents. Access privilege to make changes to production environment is restricted to authorized personnel. Post Implementation Review is performed for unsuccessful normal changes with high and medium risk and all unsuccessful emergency changes. The emergency changes are processed in alignment to the defined Change Management process. Formal approval is obtained either prior to or subsequent to migration to production.

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 corrections and corrective 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.