CYIENT

SOC 2 Type II Report

Independent Service Auditor's Report on a Description of Cyient's Engineering Design & Spatial Data Services Relevant to **Security, Confidentiality, Availability** and the Suitability of the Design and Operating Effectiveness of Controls

November 01, 2020 to October 31, 2021

Table of Contents

Section I: Independent Service Auditor's Report

M. Kuppuswamy P S G & Co LLP
Chartered Accountants

G-2, Karthik Dev Apartments,
13-14 Sundararajan Street,
Abhiramapuram,
Chennai - 600 018
Phone : 044-24987268 & 24670086
email : audit@mkpsg.com
URL : www.mkpsg.com

Independent Service Auditor's Report

The Board of Directors
Cyient Limited
Plot No. 11, Software Units Layout,
Infocity, Madhapur,
Hyderabad – 500 081
Telangana, India

Scope

We have examined Cyient Limited's (Cyient) accompanying description of its services titled " Description of Engineering Design & Spatial Data Services " throughout the period November 01, 2020 to October 31, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 01, 2020 to October 31, 2021, to provide reasonable assurance that Cyient's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability (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).

Cyient uses subservice organizations for Managed Security Operations Centre and helpdesk ticketing services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cyient, to achieve Cyient's service commitments and system requirements based on the applicable trust services criteria. The description presents Cyient's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cyient's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Cyient, to achieve Cyient 's service commitments and system requirements based on the applicable trust services criteria. The description presents Cyient's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Cyient's controls. 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.

The information included in section 5, "Other Information Provided by Cyient," is presented by management of Cyient to provide additional information and is not a part of Cyient's description of its Engineering Design & Spatial Data Services made available to user entities during the period November 01, 2020 to October 31, 2021. Information about Cyient management's response to exceptions identified has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve Cyient's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service organization's responsibilities

In section II, Cyient has provided the assertion titled "Assertion of the Management of Cyient Limited," (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Cyient is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included procedures that we considered necessary in the circumstances.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on description criteria and the controls are suitably designed and operating effectively to meet the applicable trust services criteria throughout the period November 01, 2020 to October 31, 2021.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves

- Evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria and the controls were suitably designed and operating effectively, to meet the applicable trust services criteria throughout the period November 01, 2020 to October 31, 2021.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent or detect and correct, all errors or omissions in providing services. Also, the projection to the future of any evaluation of the fairness of the

presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls is subject to risks that the system may change or that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the description and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period November 01, 2020 to October 31, 2021.
b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 01, 2020 to October 31, 2021.
c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period November 01, 2020 to October 31, 2021.

Description of tests of controls

The specific controls we tested, the tests performed and the results of our tests are presented in section 4, "Independent Service Auditor's tests of controls and results of tests".

Restricted use

This report, including the description of tests of controls and results thereof in section IV are intended solely for the information and use of Cyient ; user entities of Cyient 's Engineering Design, Spatial Data & Software Services for the period November 01, 2020 to October 31, 2021; and prospective user entities, independent auditors, practitioners providing services to such user entities and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities or other parties
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

For M.Kuppuswamy PSG & Co LLP
Chartered Accountants

Panaiyur.S.Gopalakrishnan
CPA, CITP, CISA, CISSP, FCA, CEH, QSA
CPA License No. 22897
ICAI M.No. 021409
UDIN: **22021409ABEVZD8980**

Date: February 10, 2022
Place: Chennai, India

Section II: Management Assertion

Assertion by Management of Cyient Limited

We have prepared the accompanying description of Cyient Limited's (Cyient) accompanying description of services titled "Description of Cyient's Engineering Design & Spatial Data Services " throughout the period November 01, 2020 to October 31, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Engineering Design & Spatial Data Services that may be useful when assessing the risks arising from interactions with Cyient's system, particularly information about system controls that Cyient has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability (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*).

Cyient uses subservice organizations for Managed Security Operations Centre and helpdesk ticketing services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cyient, to achieve Cyient's service commitments and system requirements based on the applicable trust services criteria. The description presents Cyient's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cyient's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Cyient, to achieve Cyient's service commitments and system requirements based on the applicable trust services criteria. The description presents Cyient's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Cyient's controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents Cyient's Engineering Design & Spatial Data Services that was designed and implemented throughout the period November 01, 2020 to October 31, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period November 01, 2020 to October 31, 2021, to provide reasonable assurance that Cyient's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, ***and if the user entities applied the complementary controls assumed in the design of Cyient's controls throughout that period.***

c. the controls stated in the description operated effectively throughout the period November 01, 2020 to October 31, 2021, to provide reasonable assurance that Cyient's service commitments and system requirements were achieved based on the applicable trust services criteria, ***if complementary user entity controls assumed in the design of Cyient's controls operated effectively throughout that period.***

For Cyient Limited

Vijaya Kumar Adusumilli

Authorised Signatory

February 08, 2022

Section III: Description of Cyient's Engineering Design & Spatial Data Services

Description of CYIENT – Engineering Design & Spatial Data Services for the period November 01, 2020 to October 31, 2021

Background and Overview of Cyient

Cyient Limited (Formerly Infotech Enterprises Limited) established in 1991 in Hyderabad India, is a leading Engineering services company, spread globally across 48 locations with 30 global delivery centers. Cyient became a publicly traded organization in March 1997, with the company's equity shares listed in India, on the National Stock Exchange (NSE: CYIENT) and the Bombay Stock Exchange (BSE:532175)

Cyient aligns with industry best practices and internationally renowned standards and frameworks like Quality management system ISO 9001:2015, Information Security Management System 27001:2013, Aerospace (AS9100 Rev D), Medical Devices (ISO 13485:2016), IRIS (ISO/TS 22163:2017), Environmental Management System ISO 14001:2015, Occupational Health and Safety Management system OHSAS 18001 and CMMI Dev 1.3, Telecommunication system TL9000 R6.0 and information technology service management system ISO 20000.

The services 'Engineering Design & Spatial Data Services- Including Modelling, Analysis, Design, Product Development, Implementation, Conversion, Manufacturing Support and Maintenance' are carried out by the organization at the entity that is in scope

The Data center services that is within the scope of this examination are carried out at the other site of Cyient's where this primary Data Center situated 10 km far from the entity that is in scope.

Subservice Organizations

Cyient utilizes the following subservice providers for various functional activities and are not included within the scope of this examination.

Service Now – SAAS based application for end user requests handling through ticketing system
Tata Communications Limited (TCL)- Managed Security Operations Centre

Boundaries of the System

The specific geographic location and services included in the scope of this report includes the following:

Location-1: Plot No 11, Software Units layout, infocity, Madhapur, Hyderabad, India

Location- 2: Plot No-2, IT Park, ISB Road, Nanakramguda, Near Continental Hospital, Gachibowli, Hyderabad, Telangana 500032 limited to Data Center Operations

Any office location other than the above is not included in the scope of the current examination. The report excludes all processes and activities that are executed outside above locations.

Cyient has its offices/subsidiaries in other 45 geographical locations. These are not included in the scope of the report. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

Principal Service Commitments and System Requirements:

Cyient designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments that Cyient makes to user entities, the laws and regulations that govern the provision of products and services to its clients, and the financial, operational, and compliance requirements that Cyient has established for the services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

Cyient establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cyient'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. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

Control Environment

Cyient's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, guidelines, methods, and organizational structure.

The Chief Executive Officer (CEO), the Senior Management team and all employees are committed to establishing and operating an effective Information Security Management System (ISMS) aligned to ISO/IEC 27001:2013 in accordance with its strategic business objectives.

The Management at Cyient is committed to the Information Security Management System, and ensures that IT policies are communicated, understood, implemented and maintained at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Cyient requires Directors, Senior Management, Officers, and all employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Cyient promotes Values FIRST (Fairness, Integrity, Respect, Sincerity and Transparency) as its core ethical values of the company and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Cyient promotes an environment of open, transparent communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Board of Directors

Business activities at Cyient are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its Founder & Chairman Mr. B.V.R. Mohan Reddy and 'Krishna Bodanapu'

being the Managing Director & CEO, is in charge of the company's Global business operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

The Executive Management team at Cyient assesses risks prior to venturing into business ventures and relationships. The size of Cyient enables the executive management team to interact with operating management on a monthly basis through Operations Council (OC) meetings and Management Review Meetings (MRM).

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, threats to security are identified and the risk from these threats are formally assessed.

Cyient has placed into operation a core Enterprise Risk Management (ERM) and risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for client organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. Senior Management team are members of forums and core working groups in industry forums that discuss recent developments.

Information Security Policies

Cyient has developed an organization wide Cyient Information Security Policies.

Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet called as "Process Assets Library" (Cyient-PAL) or as relevant hard copy policies to new employees. Changes to the information security policies are reviewed by HEAD-IT and approved by CIO prior to implementation.

Information and Communication

Cyient has documented procedures covering significant functions and operations for each major work groups. Policies and procedures are reviewed and updated based upon changes and approval by management. Departmental managers monitor adherence to Cyient policies and procedures as part of their daily activities.

Cyient management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. For each service, there is a selected service manager who is the focal point for communication regarding the service activity. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Cyient's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with Cyient employees.

Electronic Mail (e-Mail)

Communication to Customer Organizations and project teams will be handled through e-Mail as the primary communication medium. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-Mail. e-Mail is also a means to draw attention of employees towards adherence to specific procedural requirements.

Monitoring

Monitoring is the critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Cyient management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Production systems and infrastructure are monitored through service level monitoring tools like 'Nagios', 'Manage Engine OpManager' which monitor compliance with service level commitments and agreements. Reports are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met. In addition, a self-assessment scan of vulnerabilities is performed using 'Tenable Nessus Professional'. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

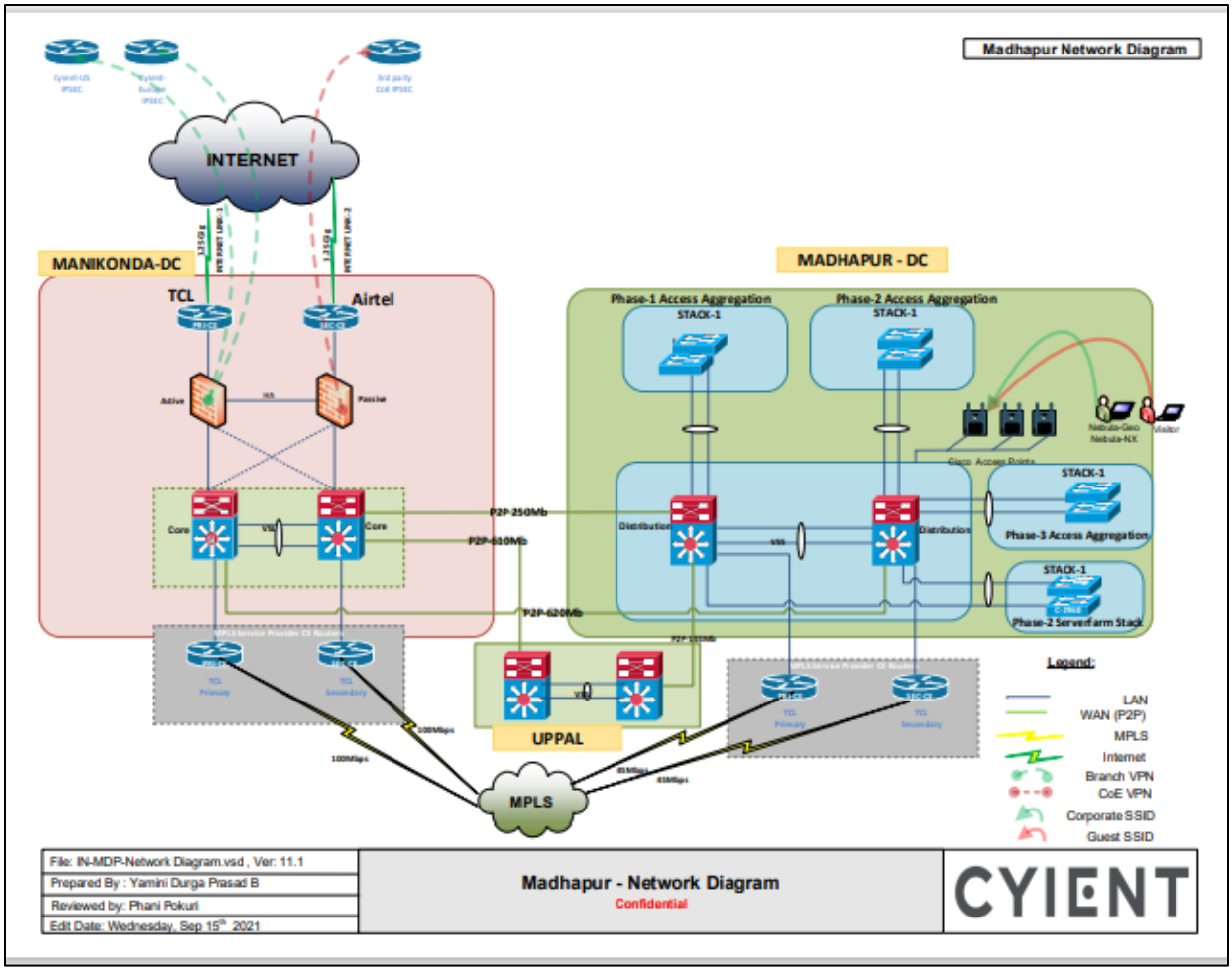
Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Cyient offices are equipped with the latest hardware, software and networking infrastructure. Offices are linked using high speed communication links, backed up by resilient 'networks and core infrastructure including network devices' to improve the SLA.



Network Connection to Client Sites

Cyient access the client network(s) via secured Point-to-Point VPN / Citrix Connections. Client application unique user login Id and password is shared with employees for accessing the client provided server/service. Clients are notified of any terminations or changes in project personnel for people who have been provided sign-on ids.

Physical Structure Overview

Cyient's power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises; UPS units and backup generators supply power to the center in the event of a power failure.

All components are covered by maintenance contracts and tested regularly. Generators are tested periodically.

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked, and AMC is entered on completion of Warranty. ERT team is formulated by identifying members from each floor. Yearly fire drills are conducted in coordination with Admin and HR personnel. The fire drill reports are collected, and analysis is made upon them.

Temperature and humidity monitoring devices are placed in critical information processing areas and the reading will be captured and processed by the respective area facility & administration teams for any actions.

Physical Access

Cyient has its global headquarters and delivery center at "Plot #11, Software units Layout, Infocity, Madhapur, Hyderabad". The Main building entrance is secured with a security personnel and CCTV surveillance. Physical and Environmental Security of Cyient is controlled and governed by Cyient ISMS Policy.

Entry to the Cyient offices/data processing areas is restricted to authorized personnel by a badge access control system. All employees are provided with badge access cards and these cards will also perform attendance recording. All visitors have to sign the visitors register and are given inactive visitor card.

Employees are granted access only to those areas which they require to access. Some members of the IT Support Team & Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to wear their access cards / employee identification cards at all times while within the facility.

CCTV's placed at each data processing area entrance is enhanced with Artificial Intelligence (AI) to capture any Piggybacking / Tailgating attempts and log the security events, send the respective alert to the respective employee manager.

CCTV is implemented to monitor the activities in server room and main entrance and other secure zones. Admin Team monitors the CCTV recordings. Logs are generated and communicated to the management periodically. Backup of recordings is stored for 45 days.

ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR group creates a ticket in helpdesk ticketing application requesting the IT team and Administration / Facilities team to issue an access card to the new employee. The IT / Administration team ensures that the access card/biometric controls configured with the appropriate access rights, and then issues the same to the employee.

On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked.

Access by visitors, contractors and/or third-party support service personnel's both entry and exit are monitored by security personnel. Photography, video, audio or other recording equipment, are not allowed inside secure premises, unless specifically authorized. Such accesses are recorded, authorized and monitored. Visitor, contract and/or third-party service personnel to sensitive areas such as data centers are strictly on "need to have" basis and subject to the principle of least privileges.

The Data Center

The Data Center monitoring and access is provisioned through CCTV and Biometric access systems. Cyient policies protect sensitive equipment such as servers, communication and power hubs and controls by locating them in secure and data centers and bonded areas that are not easily visible / accessible to public and apply appropriate controls to mitigate risks from physical and environmental threats and hazards and opportunities for misuse or unauthorized access. Only Authorized personnel are allowed to enter such

sensitive areas controlled with separate access cards and bio metric systems. Third parties are allowed access to the server room only under the supervision of Facility or IT team members

The badge access card along with biometric thumb print opens the door lock for entering into the Data Center. The Data Center is equipped with resilient systems that can support the availability and continuity of services at all layers viz power supply, ISP links, Cooling Systems and resilient core network infrastructure. All services being served through this data center are equipped with state-of-the-art load balancer technologies to avail high availability.

Firewalls

Palo Alto Firewall's are configured on the perimeter network to protect IT resources. Firewall and switch configuration standards are documented. Firewall and switch configurations are reviewed by management on a quarterly basis.

The ability to modify Palo Alto is limited to the Cyient IT Department. Specifically, IT Department is authorized to request changes from the provider. Internet Access to Cyient employees is limited through Palo Alto login and restricted to lower level employees. Sites are allowed based on the nature of the work and the allowed site categories for the employees. Only frequently used sites are open to the employees for production purpose. Management level employees are given restricted access through firewall configuration limiting not to browse any malicious site.

Visitors are limited to use the Internet through Cyient guest Wi-Fi upon specific request at the reception and a unique guest login. The Guest Wi-Fi is completely isolated from the rest of the Cyient network to maintain adequate security.

Network & endpoint protection and monitoring

Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any company address designation should be made through the company's approved perimeter security mechanisms. External connections to company servers are not permitted.

In order to stop any malware from affecting the security of the customer and organizational data, Cyient uses daily Symantec Endpoint Protection vulnerability scans along with UTM devices. IT team ensures that all the endpoints in organizations are scanned for any vulnerabilities, including public IPs and services hosted on Data Center, and that any malware is dealt with efficiently and in a timely manner.

Monitoring

Cyient has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

Capacity management controls are put in place to make certain Cyient 's resources are monitored, tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity related issues. Addition of new information systems and facilities, upgrades, new version and changes are subject to formal system analysis, testing and approval prior to acceptance.

Patch Management

Corporate IT team will maintain contacts with software principles (Ex. Microsoft) and receive monthly security inputs on critical updates released. Patches are tested and confirmed by IT team before applying to the production environment. Before deployment of any patches they are tested and deployed by the corporate IT teams and business IT SPOC's. The patch management activity is done regularly or as and when any critical changes to the computing environment.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention

The cyber security team ensures that periodic checks to network device / servers operating systems are checked for stability and any vulnerability issues and inform to the respective IT operations team for taking necessary remediation. Required patches are installed to ensure efficient working of the servers, desktops and critical network devices to remediate the reported issues. Operating system patches are managed and applied as they become available.

As per the audit calendar, all the network settings are audited for any vulnerability by doing scans periodically. These scans are done by the system admin internally. McAfee endpoint protection is installed with the feature of scanning the device automatically and log reports are reviewed by the system admin.

End point security: Anti-virus and Data Leak protection

Anti-virus software has been installed on all desktops & laptops enabled with Threat protection & Adaptive Threat Prevention (ATP). e. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals. Anti-Virus software has end point DLP to protect and control the use of removable devices.

All inbound and outbound e-Mails are scanned for spam, phishing, viruses and are filtered by Cisco IronPort at gateway and further scanned automatically using TrendMicro Deep Discovery E-mail inspector (Advanced Threat Protection) for any advanced threats. Anti-malware and end-point Host Intrusion Protection System (HIPS) practices are in accordance with Cyient malware protection policy.

'Forcepoint DLP' an end-point protection has been installed on all the desktops & Laptops to prevent unauthorized data transfers outside the organization through various medium like web, e-mail, usb, CD/DVD, Bluetooth and any mobile apps.

People

Organizational Structure

The organizational structure of Cyient provides the overall framework for planning, directing, and controlling operations. It has segregate personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting Cyient clients.

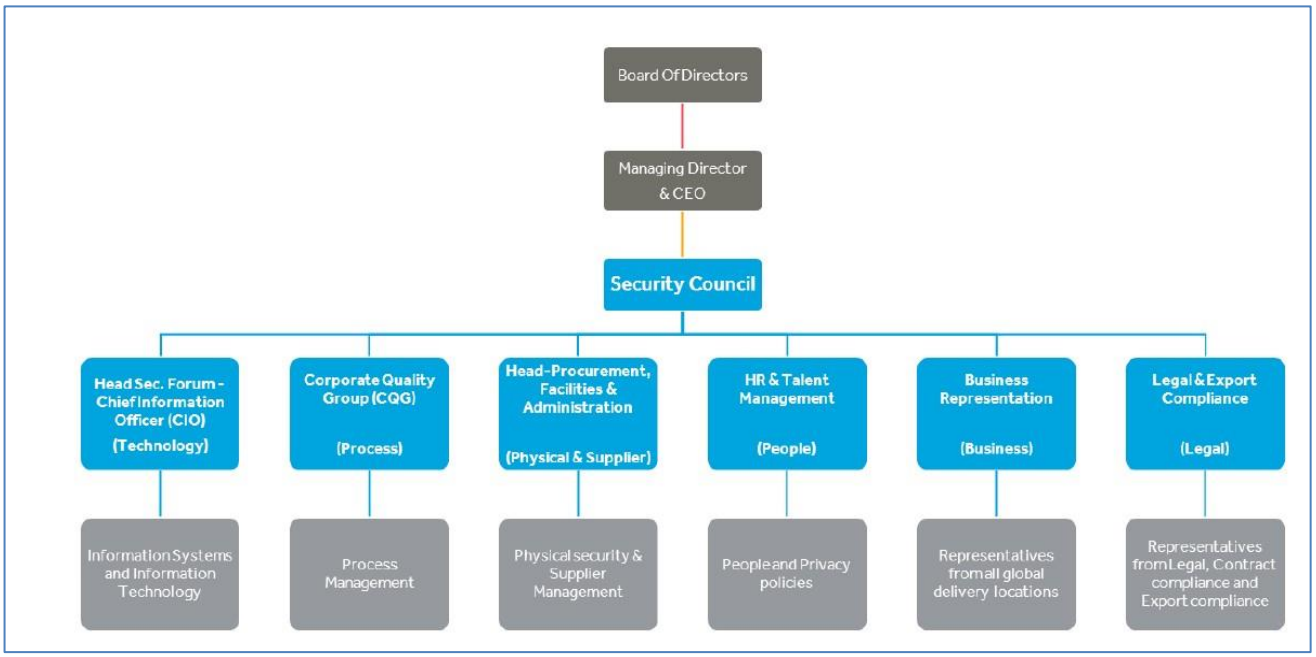
Mr. Krishna Bodanapu is responsible for oversight of global Cyient. The Cyient site is locally managed by the following individuals / teams:

- Operations / Legal Compliance
- Engineering
- Finance
- Marketing
- Sales
- Quality Assurance
- Product Delivery
- Information Technology
- Compliance and Audit
- Administration
- Human Resources
- Business Development

The management team meets periodically to review business unit plans and performances. Weekly, monthly meetings and calls with senior management, and department heads are held to review operational, security and business issues, and plans for the future.

Cyient's Information Security policies define and assign responsibilities/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives

Cyient Organization Chart



The Board of Directors ('the Board') is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance.

The MD & CEO lays down the security policy and objectives, and delegates' responsibilities for implementation of the information security system. He also formulates the Security Council, which is comprised of representatives from various functions and locations of the company. The group shall be reviewing the functioning of the information security systems and its effectiveness at least once in 6 months.

The Chief Information Officer (CIO), acting as the Chief Information Security Officer (CISO), is responsible for the preparation and maintenance of this CISM, enforcing policies and ensuring compliance, to assure protection of information assets. The CIO and GEO specific IT Directors will also maintain contacts with special interest groups such as CERT, SANS, NASSCOM, DSCI, CII and any local security bodies along with other technology partners in the industry.

Board of Directors

Board of directors shall review the overall security program, investments around information security to ensure controls in place and they are adequate to meet the statutory & regulatory requirements for protecting the interests of stake holders.

Managing Director & CEO

The MD&CEO gives overall strategic direction by approving and mandating the information security policy, manual and delegates operational responsibilities for physical and information security to the Security Council headed by the CIO.

The MD&CEO has charged the Security Council with the task of securing Cyient's information and information related assets.

Information security activities shall be coordinated throughout Cyient by the Security Council, to ensure consistent application of these security principles, axioms and policy statements.

Security Council

The Security Council comprised of representatives from all functional and delivery locations having responsibilities for Management oversight and direction for both physical and logical aspects of Information security, Coordinating and directing Cyient's entire security framework, including the information security controls at all Cyient locations

Commissioning or preparing information security policy statements, ensuring their compliance with the principles and axioms approved by the Executive Chairman and formally approving them for use throughout Cyient

Periodically reviewing the security policy statements to ensure the efficiency and effectiveness of the information security controls and recommending improvements wherever necessary Identifying significant trends and changes to Cyient's information security risks and, where appropriate, proposing changes to the controls framework and/or policies

Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes

Periodically reporting on the status of the security controls infrastructure to the Executive Chairman, and liaising as necessary with the Risk Management and Audit Committees etc., using metrics and other information supplied by the CIO, local security committees, the Information Security Manager, Internal Audit and others.

The Security Council delegates some of its responsibilities, however it remains accountable for the overall effectiveness of information security throughout Cyient.

Chief Information Officer (CIO)

The CIO is responsible for

Heading the Security Council

Taking the lead on information governance as a whole - for example by issuing the policy manual and by enforcing the overall strategic direction, support and review necessary to ensure that information assets are identified and suitably protected throughout Cyient.

Appointing the IT-Governance, Risk and Compliance team for information security implementation and compliance.

IT-Security Team

Implementation of the information security framework and controls

Defining technical and non-technical information security procedures, guidelines processes, methodologies and support for their implementation

Supporting information asset owners, project security coordinators and CDU heads in defining, implementation of controls, processes and supporting tools to comply with the policy manual to manage information security risks

Assisting and supporting information asset owners, project security coordinators in the investigation and remediation of information security incidents or other policy violations

Reviewing and monitoring compliance with the policy statements and contributing to internal audit and control self-assessment (CSA) processes

Collecting, analyzing and communicating information security metrics and information related incidents

Liaising as necessary with related internal functions such as IT operations, compliance and internal audit, as well as external functions when appropriate

Organizing a security awareness drive for personnel to enhance the security culture and develop a broad understanding of the information security requirements.

Verifying that suitable technical, physical and procedural controls are in place in accordance with the manual, and are properly applied and used by all associates. In particular, they shall take measures to ensure that Cyient Associates:

Providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within the respective areas.

Risk Owner

Risk owners are the highest level of authority, accountable to manage the risk and have the authority to approve the risk treatment plans and residual risks.

Information Asset Owners (IAOs)

IAOs are senior managers held accountable for the protection of Information Assets at their respective business areas. IAOs may delegate information security tasks to managers or other individuals, however, shall remain accountable for proper implementation of the controls on their respective assets.

IAO's are responsible for:

- Undertaking or commissioning information security risk assessments, to ensure that the information security requirements are properly defined and documented during the early stages of development.
- Appropriate classification and protection of the information assets.
- Specifying and funding suitable protective controls.
- Authorizing access to information assets in accordance with the classification and business needs
- Ensuring timely completion of regular system/data access reviews
- Monitoring compliance with protection requirements affecting their assets.

Department Information Security Off (DISO)

The Department Information Security Coordinator is the single point of contact between project teams, customer liaison, and IT teams, in implementation and adherence to controls by associates in their respective project(s).

The responsibilities of DISO included but not limited to are

- Documentation of security requirements for customer in IPMP
- Ensure agreed security controls are implemented and working effectively
- Conducting risk assessment as per risk management guideline
- Review of access rights in coordination with IT teams (Physical, USB/Cd/DVD, admin, Folder file permissions etc.),
- Conduct floor Awareness sessions, and reporting status to ISMS team
- Reporting security incidents and supporting Investigation,
- Coordinate with internal functional groups/customer for customer security assessments,
- Coordinate with ERT & BCP teams for DR drills.

All Associates

All Associates (i.e. employees on the payroll and others acting in a similar capacity, such as contractors, consultants, student placements etc.) are responsible for complying with the principles, axioms and policies in the information security policy manual where relevant to their jobs. They are responsible for maintaining the security of information and related assets entrusted to them. Upon hire, as a condition of employment, each associate undertakes to comply with Cyient's information security policies. Any associate failing to comply with the security policies would be subject to disciplinary action.

The Security Policy and Security Objectives of Cyient are available for all associates on the intranet

(Cyient PAL).

Commitment to competence

Cyient's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by current andanticipated needs of Business. Employees are evaluated on an Annual basis to document performance levels and to identify specific skill training needs

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within Cyient.

Human Resources Policies and Procedures

Cyient maintains clear Human Resources Policies and Procedures in the intranet "Process assets Library (PAL) site. The policies and procedures describe Cyient practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behaviour and competence which includes Non-disclosure Agreement (NDA) "Acceptable use of IT resources".

The Human Resources department review these policies and procedures along with relevant internal functional departments on periodic basis to ensure they are updated to reflect changes in the organization and the current operating environment. Employees are informed of these policies and procedures upon their hiring and sign an acknowledgement form confirming their receipt. Personnel policies and procedures are documented in the Cyient Human Resources Policy.

New Hire Procedures

New employees are required to read Cyient's' corporate policies and procedures and sign an acknowledgement form stating that they have read and understand them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective employees prior to employment through the independent third-party service providers. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

Training and Development

On an ongoing basis, Cyient examines its employee training and development needs from a business standpoint, both in terms of current needs either internal or customer driven. Cyient compares these needs to the current skills held by its employees. On an as-needed basis, Cyient may select certain employees to receive additional training to meet the current and anticipated needs of the organisation. Cyient also offers regular trainings prepared in-house to undertake trainings on a periodic basis on relevant topics. These trainings are attended by the selected technical employees of the specific department the training belongs to.

Performance Evaluation

Cyient has a performance review and evaluation program to recognize employees for performance and contributions. Cyient performance evaluation process is also used to help employees improve their performance and skill levels. Employees performance reviews, promotion and compensation adjustment are performed every 12 months. The performance evaluation is reviewed with the employee and signed by the employee and their manager. For specific cases, Interim performance reviews shall be carried out by the HR to meet the market benchmarking compensation levels.

New Employee Training

Digital awareness induction module is mandatory for any new joiner to complete within 15 days of the Joining. Failure in such mandated induction course completion will lead to in-accessibility to timesheet logging. HR coordinates to provide information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely attendance sheets and feedback forms from employees. Employees undergo security awareness training regularly.

Employee Terminations

Termination or change in employment is being processed as per Cyient HR related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment.

All employees, contractors and third-party personnel are required to return physical and digital Identification/access tokens provided to them by Cyient or its clients on their termination of employment or contract.

Access privileges are revoked upon termination of employment, contract or agreement. In case of change of employment /role, rights associated with the prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Ethical Practices

Cyient reinforces the importance of the integrity message and the tone starts at the top. Every employee, manager and director consistently maintain an ethical stance and support ethical behaviour. Employees at Cyient encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Code of Conduct and Disciplinary Action

Cyient has put forward Code of Conduct and Disciplinary Process in-order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. Cyient employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the Code is prosecuted as per defined process.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Help Desk

Cyient has put in place a helpdesk function that function within the IT Department and an integrated helpdesk to handle problems and support requirements of users. support users in case of incidents and manage them without disruption to Cyient ’s business and ensures that changes to any component of Cyient ’s information assets and infrastructure are controlled and managed in a structured manner.

All requests received at the Help Desk are classified as to their priority & criticality and resolved within the maximum resolution time as detailed in the Cyient helpdesk Change Management and Incident Response Procedure.

Change Management

Cyient has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal Change Management process.

Change Management covers any change to the Information assets and infrastructure of Cyient and include but not limited to addition/ modification in the application, application components, database structure, DBMS, system and network components, policies and procedures.

Every change to such base lined components is governed by the change control and management procedures as outlined in the Helpdesk, Change management and Incidence Response procedure. Cyient's change management process requires all security patches and system and software configuration changes to be tested before deployment into Staging or Production environments.

All changes are recorded, approved, implemented, tested and versioned before moving to production environment. The impact of implementing every significant change are analyzed and approved by the IT Head before such implementation. A sign-off shall be obtained from the personnel who had requested for the change after implementation of the change. The effectiveness of the Change Management process is reviewed on a quarterly basis by CIO.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. The help desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to security of Information assets including facilities and people are termed as an Incident.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analyses are approved by CTO.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new user account and the first-time password creation with mandated password change after first login will be sent to the respective manager. The allocation of workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty will be assigned by the respective manager in coordination with the IT team. The default access levels for different departments are defined and documented in IT policy manual. Any additional access is provided upon helpdesk ticket duly approved by the line manager and approved by VP Operations. Company has standard configuration that is implemented across Desktops & laptops individually based on the need of the business area.

Only the IT team has access to change user profile or give higher access. Other employees do not have local admin privileges on their desktops, only IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. This is documented in Access Control Matrix.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to IT team. Access to storage, backup data, systems, and media is limited to IT team through the use of physical and logical access controls.

Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated by an associated password. Use of encrypted VPN channels help to ensure that only valid users gain access to IT components. Remote access is not permitted to any employee.

Passwords are controlled through Password policy and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules.

Guest and anonymous login accounts are disabled are not allowed on any machines. Local administrator privilege is restricted to the IT Support Team and is not available to other users. However, where the project need the team members to have the local admin access, respective line manager will raise a request to senior management, which can approve or deny the request based on its merit.

Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved by Head of Information Security (ISMS).

Out Bound Communication

Cyient development applications are accessible only within the Cyient V-LAN Network. For uploading the files and communication to the client, external point-to-point VPN internet access is established. Internet usage is restricted and controlled through Palo Alto firewall. The IT Team periodically reviews and recommends changes to web and protocol filtering rules. Cyient Cyber security team review these rules and decide if any changes are to be made.

Confidentiality

Cyient classifies data as 'Highly Confidential', 'Confidential', 'Internal' and 'Public'. Access to data is restricted through password-controlled folders and any external data transfers are monitored using Forcepoint DLP¬

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Media Disposal process ensures that the disposal of unwanted media viz. HDD's, Tapes, print copies, CD's etc., are disposed timely to protect and maintain the secure disposal of the information and data.

Backup and Recovery of Data

Cyient has developed formal policies and procedures relating to back up and recovery. Backup policy is defined in the Backup and media handling policy. Suitable backups are taken and maintained (including storing of backups offsite) in relevant tape media or over remote storage through synchronisation (Storage replication).

Cyient has put in place backup processes that define the type of information to be backed up, backup cycles and the methods of performing backup. Monthly back-up copies are stored in a secure off-site location; the backup media are tested for restoration on a periodic basis to ensure the effectiveness and integrity of backup.

All backup copies are tested periodically to ensure that the data and information are securely retrievable in the event of an emergency without any loss of information. Users are made aware through adequate training their responsibilities for ensuring backup of required data and information.

Data Restoration Procedure

A well-established data restoration procedure is evident within the backup policy to ensure that the data in backup media is retrievable when in need.

Restoration is done in two cases – primary case is when a Cyient member makes a request to recover some data that they might have lost. The other case when a restoration test is done during our regular DR test. The relevant IT personnel (i.e., the backup administrator) ensures that the data is restored appropriately and inform back to the requester for verification and use.

Applicable Trust Services Criteria and related Controls

The security, availability and confidentiality trust services categories and Cyient related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

Cyient has determined that Processing Integrity and Privacy trust services Categories are not relevant to the system.

User- Entity Control Considerations

Services provided by Cyient to user entities and the controls of Cyient cover only a portion of the overall controls of each user entity. Cyient controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve objectives relating to the services outlined in this report to be achieved solely by Cyient. This section highlights those internal control responsibilities that Cyient believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

Contractual Arrangements

- User organizations are responsible for understanding and complying with their contractual obligations to Cyient such as providing input information, review and approval of processed output and releasing any instructions.

Other Controls

- User Organizations are responsible for ensuring end customer privacy.
- User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Cyient for processing.
- User Organizations are responsible for their network security policy and access management for their networks, application & data.
- User Organizations are responsible for working with Cyient to jointly establish service levels and revise the same based on changes in business conditions

Complementary Subservice Organization Controls

Cyient utilizes ServiceNow and Tata Communications Limited (TCL) to perform certain functions as described in the description above. Rather than duplicate the control tests, controls at ServiceNow and TCL are not included in the scope of this report. The affected criteria are included below along with the expected controls.

Security:

1. Restrict access to data and systems applying the least-privileged principle through logical and physical access management processes. (CC 6)

2. Monitor key system components for security incidents to identify and respond to security threats timely through logical and manual security logging and monitoring processes. (CC 7.3)

3. Use of encryption technologies to protect user organization data both at rest and in transit. (CC 6.7)

4. Implement authorized and tested changes to system components through development and change management processes. (CC 8)

Availability:

5. Maintain and monitor an infrastructure that ensures user organization data are replicated and backed-up at multiple locations.(A1.2)

6. Maintain and monitor an infrastructure that ensures user organization capacity demands are met. (A1.1)

Confidentiality:

7. Maintain data classification standards and processes to identify confidential user organization data. (CC 6.1)

8. Restrict access to confidential data applying the least-privileged principle through logical and manual physical access management processes. (CC 6.1)

Section: IV: Independent Service Auditor's description of Tests of Controls and Results

Independent Service Auditor's description of Tests of Controls and Results

Overview

This report on the controls at Cyient (Service Organization) is intended to provide an opinion on the fairness of the presentation of the description of Cyient's system; the suitability of the design of the controls to achieve specified control objectives and the operating effectiveness of those controls in place at Cyient throughout the period from November 01, 2020 to October 31, 2021. Our examination of Cyient's controls was restricted to the control objectives and the related controls specified by Cyient in Section IV and was not extended to controls in place at user locations or other control procedures, which may be described in Section III but not listed in Section IV.

The examination was performed in accordance with AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE18), "Attestation Standards: Clarification and Recodification" read with AT-C 105, Concepts common to attestation engagements, AT-C 205, Examination engagements and the AICPA guide to Reporting on controls at a Service Organization relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®). It is the responsibility of User entities (User Organization) to evaluate this information in relation to the controls in place at each user location to assess the total control environment. If effective user controls are not in place, Cyient's controls may not compensate for such weaknesses.

This report on Controls at a Service Organization relevant to ***Security, Confidentiality, Availability*** and the suitability of the design and the operating effectiveness of those controls is intended to provide interested parties with information sufficient to understand the basic structure of controls within Cyient. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding the reviewed systems.

Evaluating the fairness of presentation of the description:

The criteria for evaluating the fairness of presentation of the description of the system of Cyient are as follows:

i. Information regarding the types of services provided
ii. Components of the system used to provide the services comprising of:
    a. Infrastructure
    b. Software
    c. People
    d. Procedures; and Data
iii. Boundaries of the system covered
iv. Capturing and addressing significant events and conditions by the system; and
v. Process used to prepare and deliver reports and other information to User entities (User Organization)

Test of operating effectiveness of controls:

Our tests of effectiveness of the controls included such tests as we considered necessary in the circumstances to evaluate the suitability of the design of the controls to achieve specified control objectives and the operating effectiveness of those controls achieved during the period from November 01, 2020 to October 31, 2021. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions and procedures throughout the period of November 01, 2020 to October 31, 2021, for the controls listed in Section IV, which are designed based on the ***Security, Confidentiality, Availability*** criteria are outlined in TSP Section 100 (2017), Trust Services Criteria. In selecting a particular test of the operational effectiveness of controls, the following were considered: (a) the nature of the items being tested, (b) the types and competency of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk and, (e) the expected efficiency and effectiveness of the test.

The types of tests performed with respect to the information addressed in Section IV and of the operating effectiveness of controls as detailed in Section IV are briefly described below:

Test	Description
Inspection	Inspected documents and reports indicating performance of the control activity.
Re-performance/Transaction	Testing Re-performed application of the control activity.
Observation	Observed application of specific control activities.
Corroborative Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.

Description of Tests Performed

The following information pertains to tests of operating effectiveness performed by Independent Auditors. Tests were performed only of those controls specifically identified. Testing of the operating effectiveness of identified controls was performed during the period from November 01, 2020 to October 31, 2021. The nature and extent of tests performed, along with the specific control objective they were designed to achieve, are identified in the table below.

Sampling

In accordance with AICPA authoritative literature, professional judgment is utilized to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a test. Samples were selected in such a way that they were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
CONTROL ENVIRONMENT		
CC1.1 The entity demonstrates a commitment to integrity and ethical values.		
• The Company has mission and vision statements. Additionally, the entity has developed a clearly articulated statement of values that is understood at all levels of the organization. • The Company has implemented a whistle blower program to identify financial irregularities, unethical practices and frauds. • The Company has approved code of business conduct that is applied across the entity. The Code of Conduct outlines strict disciplinary consequences for violation of code of conduct. • The code of conduct is published on the Cyient PAL portal for employees to review and accept.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • The Company has mission and vision statements. Additionally, the entity has developed a clearly articulated statement of values that is understood at all levels of the organization. • The Company has implemented a whistle blower program to identify financial irregularities, unethical practices and frauds. • The Company has approved code of business conduct that is applied across the entity. The Code of Conduct outlines strict disciplinary consequences for violation of code of conduct. • The code of conduct is published on the Cyient PAL portal for employees to review and accept. **Inspection:** Inspected the following and determined that the defined controls are in place: • Cyient Vision/Mission statements published and circulated amongst the employees • Whistle Blower policy • Disciplinary action policy	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	Observation: Observed the internal portal for a select sample of employees and determined that code of conduct is reviewed and accepted.	
CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control		
• Security Council Meetings headed by CIO are held every 3 months to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives. • The Company has an Enterprise Risk Committee that reports to the Board of Directors.	**Inquiry:** • Inquired with the Senior Manager- Corporate Quality and ascertained that Security Council Meetings headed by CIO are held every 3 months to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives. **Inspection:** Inspected the following and determined that the defined controls are in place: • Select sample of Security Council meetings minutes • Governance and Business Alignment structure	No exceptions noted
CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
• Organization chart is documented that depicts authority, reporting lines and responsibilities for management of the organization's information systems. These charts are communicated to employees through intranet and are updated as needed. • Company has defined and documented Information security related policies and procedures shared internally via CYIENT PAL(Document repository).	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Organization chart is defined and communicated via Cyient portal. • CYIENT PAL portal hosts information security and other employee policy documentation • Information Security Policies are reviewed and approved by the Management at least annually.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Information Security Policies are reviewed and approved by the Management at least annually. • Allocation of information security responsibility is documented in information security manual available at CYIENT PAL (Document repository).	• Allocation of information security responsibility is documented in information security manual available at CYIENT PAL • Authority limits, delegation of powers and other responsibilities are in place for significant roles. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Cyient Organization chart • Review history of policy documentation • Information Security Manual **Observation:** Observed the Cyient Pal portal and noted that the company has defined and documented Information security related policies and procedures shared internally via CYIENT PAL.	
CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
• The company has documented Policies and procedures pertaining to management of human resources. • Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process. • New employees sign offer letter as their agreement and acceptance of broad terms of	**Inquiry:** Inquired with the HR Manager and ascertained that: • The company has documented Policies and procedures pertaining to management of human resources. • Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
employment including a brief description of position and other terms. • Talent acquisition team initiates the background check process with an external vendor prior to onboarding. • Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position. • The induction training given by HR includes information security training. In this training the HR, physical access and security polices are explained. • An awareness refresher training is provided to all employees on at least annual basis. These are rolled out as digital E Learning. • All new employees have to read and sign the Confidentiality Agreement/NDA upon joining. • As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of the Acceptable Information Use Policy (AUP).	• New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms. • Talent acquisition team initiates the background check process with an external vendor prior to onboarding. • Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position • An awareness refresher training is provided to all employees on at least annual basis. These are rolled out as digital E Learning. • All new employees have to read and sign the Confidentiality Agreement/NDA upon joining. • As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of the Acceptable Information Use Policy (AUP). **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Job descriptions for a select sample of roles	

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Cyber Security Awareness Program completion status for a select sample of employees. • Offer letter, NDA, background check reports, acceptable use policy acknowledgement and induction training attendance for a select sample of new joiners • Employee Code of conduct **Observation:** Observed the Cyient PAL portal and noted that policy and procedure documents are maintained and updated.	
CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
• Roles and responsibilities are defined and documented at CYIENT PAL (Document repository). • Job descriptions are reviewed by entity management on a periodic basis. • Performance appraisals are performed at least annually.	**Inquiry:** Inquired with the HR Manager and ascertained that: • Roles and responsibilities are defined and documented at CYIENT PAL(Document repository). • Job descriptions are reviewed by entity management on a periodic basis. • Performance appraisals are conducted on an annual basis. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Roles and responsibilities as part of the Information Security Manual • Select sample of job descriptions • Performance appraisal completion from Cyient portal for a select sample of employees.	No exceptions noted
COMMUNICATION AND INFORMATION		

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
• Internal audits are performed, results are communicated and corrective actions monitored. • Timely reporting is carried out internally by all major departments.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Internal audits are performed, results are communicated and corrective actions monitored. • Timely reporting is carried out internally by all major departments. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • select sample of process wise internal audit reports, Non-conformity and corrective action reports • Select sample of monthly report- control tower for tracking deliverables, resource efficiency and other metrics-maintained project wise	No exceptions noted
CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
• Employees/associates can express their concern/issues/grievances through MYCYIENT portal and feedback through annual ASAT survey • An organizational wide incident management process is in place enabled through MYCYIENT portal. IT specific incidents are captured through GHD(Global help desk) and information security incidents through security incident management portal.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Employees/associates can express their concern/issues/grievances through MYCYIENT portal and feedback through annual ASAT survey • An organizational wide incident management process is in place enabled through MYCYIENT portal.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• An awareness refresher training is provided to all employees on at least annual basis covering security objectives. These are rolled out as Information Security Awareness Program. Users are informed of the process for reporting complaints and security breaches during induction Security Training. • Security policies are published and disseminated to employees via Cyient PAL intranet	• An awareness refresher training is provided to all employees on at least annual basis covering security objectives. These are rolled out as Information Security Awareness Program. Users are informed of the process for reporting complaints and security breaches during induction Security Training. • Security policies are published and disseminated to employees via Cyient PAL intranet **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Select sample of incident tickets from MYCYIENT portal and IT incidents tickets from GHD helpdesk • Cyber Security Awareness Program completion status for a select sample of employees. • Select sample of emails sensitizing employees about phishing, work from home best practices, cyber security awareness and privacy best practices. **Observation:** Observed the MyCyient portal and noted that employees can report concern/issues/grievances through their respective dashboards. Also noted that ASAT feedback is collected from employees for various initiatives within the organization.	

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	Observed the CYIENT PAL portal and noted that policy documents are stored in the centralized repository.	
CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
• Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / SOW. • Customer specific SLA commitments are monitored on a periodic basis. These are shared with customers based on the customer requirements. • Customers provide their issues, complaints or feedback through email to Business Heads. • A client escalation matrix is in place to ensure that communication channels for external users are available on a timely basis. • Changes to systems, network, working arrangements, employees are communicated to clients, if it impacts their operations • Customer can provide their issues, complaints or feedback through email to Business Heads, customers feedback is collected annually through survey (CSAT)	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / SOW. • Customer specific SLA commitments are monitored on a periodic basis. These are shared with customers based on the customer requirements. • Customers provide their issues, complaints or feedback through email to Business Heads. • A client escalation matrix is in place to ensure that communication channels for external users are available on a timely basis. • Changes to systems, network, working arrangements, employees are communicated to clients, if it impacts their operations • Incidents impacting external users are communicated to them through emails along with root cause analysis, if required. **Observation:** • Observed a select sample of MSAs entered into with customers and noted that Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / SOW.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Observed the CSAT surveys collected from customer and noted that feedback mechanism is in place. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Select sample of monthly report- control tower for tracking deliverables, resource efficiency and other metrics-maintained project wise • client escalation matrix • Integrated Project Management Plan for the project in scope specifying the methodology of execution, responsibilities of Cyient and the customer. • Select sample of emails notifying customers of changes to workforce members for creation/modification of access	
RISK ASSESSMENT		
CC 3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
• Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework. • Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework. • Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	Inspection: • Inspected the Information Security Operational Risk Management Procedure and determined that the defined controls are in place.	
CC 3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
• Policies and procedures related to risk management are developed, implemented, and communicated to personnel. • A risk assessment is performed atleast on an annual basis. • As part of this process, threats to security are identified and the risk from these threats is formally assessed. • Risk treatment plans are in place to respond to risks.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Policies and procedures related to risk management are developed, implemented, and communicated to personnel. • A risk assessment is performed atleast on an annual basis. • As part of this process, threats to security are identified and the risk from these threats is formally assessed. • Risk Mitigation Plans and action trackers are in place to respond to risks. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Information Security Operational Risk Management Procedure • Risk Management Plan done process wise • Risk treatment plan	No exceptions noted
CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.		

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Company has defined a formal risk management process for evaluating risks based on identified vulnerabilities, threats, asset value and mitigating controls. • A risk assessment is performed atleast on an annual basis.	I**nspection:** • Inspected a select sample of process wise Risk Assessment reports and determined that Company has defined a formal risk management process for evaluating risks based on identified vulnerabilities, threats, asset value and mitigating controls. **Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that risk management policy documents the process for risk evaluation.	No exceptions noted
CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.		
• The Risk and Compliance team evaluates the design of controls and mitigation strategies in meeting identified risks and recommends changes in the control environment. • Whenever new products or services are added or its business model changes, a risk assessment is carried out for the new service. • Emerging technology and system changes are considered when performing risk assessment	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Cyient has a risk identification process which considers changes to the regulatory, economic, and physical environment in which the entity operates. **Inspection:** Inspected a select sample of process wise risk assessment reports, Information Security Operational Risk Management Procedure and determined that the defined control is in place.	No exceptions noted
MONITORING ACTIVITIES		
CC 4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• The internal audit function conducts process wise reviews on a periodic basis and findings are remediated on a timely basis. • Internal audit team is staffed with competent professionals with technical expertise and relevant certifications.	**Inspection:** Inspected the following documents and determined that the defined controls are in place: • Internal audit reports for a select sample of projects • Corrective action taken on Internal audit findings **Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • The internal audit function conducts process wise reviews on a periodical basis. • Results and recommendations for improvement are reported to management. • Internal audit team is staffed with competent professionals with technical expertise and relevant certifications.	No exceptions noted
CC 4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
• The internal audit function conducts process wise reviews on a periodic basis. Results and recommendations for improvement are reported to management via security council meetings. • All internal audit issues are tracked until closure to ensure that these are closed.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • The internal audit function conducts process wise reviews on a periodic basis. Results and recommendations for improvement are reported to management. • All internal audit issues are tracked until closure to ensure that these are closed.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	Inspection: Inspected the following documents and determined that the defined controls are in place: • Internal audit reports for a select sample of projects along with corrective action plan on the findings • Select sample of Security Council meeting minutes	
CONTROL ACTIVITIES		
CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
• Compliance team sensitizes security best practices to all employees through emails • The internal audit function conducts process wise reviews on a periodic basis. Results and recommendations for improvement are reported to management. Audit has a rotation plan so that all areas are covered. • Segregation of duties is in place for critical functions and departments	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Compliance team sensitizes security best practices to all employees through emails • The internal audit function conducts process wise reviews on a periodic basis. Results and recommendations for improvement are reported to management. Audit has a rotation plan so that all areas are covered. • Segregation of duties is in place for critical functions and departments as documented in the organization chart **Inspection:** Inspected the following documents and determined that the defined controls are in place:	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Select sample of emails sensitizing employees about phishing, work from home best practices, cyber security awareness and privacy best practices. • Internal audit reports for a select sample of projects along with corrective action plan on the findings • Master Organization chart of Cyient	
CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		
• During the risk assessment and management process, Compliance along with Project personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. • Compliance team evaluates the effectiveness of Risk Mitigation strategies during the meetings and recommends changes based on its evaluation. • Risk Assessment is reviewed and approved by respective department head	**Inspection:** • Inspected a select sample of risk management plan conducted process wise and determined that during the risk assessment and management process, Compliance along with Project personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. • Inspected the version history of the risk management plan and determined that it is reviewed and approved by the department head. **Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Compliance team evaluates the effectiveness of Risk Mitigation strategies during the meetings and recommends changes based on its evaluation.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Risk Assessment is reviewed and approved by respective department head	
CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
• All policies are updated/reviewed at least every year to ensure that these are current and in line with the current business. • The compliance department assesses adequacy and relevance of policy and procedures.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • All policies are reviewed at least every year to ensure that these are current and in line with the current business. • The compliance department assesses adequacy and relevance of policy and procedures. **Inspection:** Inspected the version history of the policy documentation and determined that annual review process is in place.	Exception noted In some instances, MKPSG could not verify if the policy documents were periodically reviewed in the absence of relevant information in the policy document version history.
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
• Company has a documented procedure for logical access controls • Access is granted on least privileges basis by default and any additional access needs to be approved • Company has established hardening standards, production infrastructure that include requirements for implementation of security groups, access control, configuration settings, and standardized policies.	**Inquiry:** Inquired with the CISO and ascertained that: • Company has documented procedure for logical access controls • Access is granted on least privileges basis by default and any additional access needs to be approved • Company has established hardening standards for infrastructure that include requirements for implementation of security groups, access	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Network diagrams are documented covering Cyient infrastructure • Infrastructure components and software are configured to use the Windows security using group policies & Active Directory. • Password policy and complexity requirements are enabled in the Active Directory. Minimum length, password history, password age, account lockout attempts and duration are set, • Remote working is enabled via VPN • The IT department maintains an up-to-date listing of all software. • All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed. • Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Management. Privileged access is authorised by COO and reviewed by IT on a periodic basis. • All confidential data is classified as per the data classification policy • All information assets are identified in an asset inventory.	control, configuration settings, and standardized policies. • Network diagrams are documented covering Cyient infrastructure • Infrastructure components and software are configured to use the Windows security using group policies & Active Directory. • Remote working is enabled via VPN and Akamai cloud • The IT department maintains an up-to-date listing of all software. • All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed. • Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Management. • All confidential data is classified as per the data classification policy as part of Cyient Information Security Manual **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Access Control Policy and Procedure, Cyient Information Security Manual • Patch Management group policy, vendor document on firewall security guidelines • Network diagram of Cyient Head office and Manikonda Data Center	

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Password policy configuration in the Active Directory • IT asset inventory **Observation:** • Observed the Global protect VPN configuration and noted that secure remote access channel is configured. • Observed the Active directory groups and noted that Administrator groups with privileged access are defined and monitored	
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
• On the day of joining, HR triggers an email from Workday application which sends a mail to global helpdesk providing the details of the new joiners. The helpdesk then provides necessary access as per request. • Employee user accounts are removed from various applications and network systems as of the last date of employment based on access revocation request sent by the concerned department to the global helpdesk team. • Client is informed about the new joiners to the team by the respective managers for granting necessary access	**Inspection:** Inspected the following documents and determined that the defined controls are in place: • Helpdesk tickets raised by internal departments pertaining to access creation for new joiners. • Helpdesk tickets pertaining to access revocation for a select sample of exited employees from the active directory. • Select sample of emails informing clients to grant access for new joiners. • Select sample of emails informing clients to revoke access when employees leave the organization. **Inquiry:** Inquired with the CISO and ascertained that: • On the day of joining, HR triggers an email from Workday application which sends a mail to	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Access on client systems is removed by sending an email to the client manager informing them about the exiting employee.	global helpdesk providing the details of the new joiners. The helpdesk then provides necessary access as per request. • Employee user accounts are removed from various applications and network systems as of the last date of employment based on access revocation request sent by the concerned department to the global helpdesk team. • Access on client systems is requested/removed by sending an email to the client manager informing them about the changes to the team.	
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
• A role based security process is setup in Active directory with groups and roles based on job requirements. • Centralized AD manager tool is used for management of access permissions.	**Observation:** • Observed the assignment of groups in the Active Directory and noted that role-based security process is setup in Active directory with groups and roles based on job requirements. • Observed the AD manager tool used for access creation, revocation and management of permissions and noted that a centralized process is in place.	No exceptions noted
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
• Physical access to office premises is monitored through CCTV installed at key points within the premises.	**Inquiry:** Inquired with the Manager- Facilities & Admin and ascertained that:	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• There is a security desk at the office entry manned by a security guard • Visitor register is maintained to log entry and exit details. • Visitor badges are for identification purposes only and do not permit access to the facility. • All visitors must be escorted by a Company employee when visiting office facilities. • ID cards that include an employee picture must be worn at all times when accessing or leaving the facility. • Physical access is setup by the Admin Dept for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas. • Physical access to sensitive areas / server rooms is granted only to privileged users by helpdesk Team. • A periodic review of physical access logs is carried out by the Admin team. • Upon the last day of employment, HR Team sends exit email requesting for deactivation of physical access for terminated employees. Physical access is deactivated by the Admin Team. • Employees are required to return their ID cards on the last day, and all ID badges are disabled.	• Access cards are issued to new employees based on an access card requisition initiated by the Human Resource (HR) group. **Observation:** Observed during the virtual tour of the facility and noted that: • Physical access to office premises is monitored through CCTV installed at key points within the premises. • There is a security desk at the office entry manned by a security guard • Visitor register is maintained to log entry and exit details. • Visitor badges are for identification purposes only and do not permit access to the facility. • All visitors are escorted by a Company employee when visiting office facilities. • ID cards that include an employee picture is worn at all times when accessing or leaving the facility. • Physical access is setup by the Admin Dept through a tool for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas. • Physical access to sensitive areas / server rooms is granted only to privileged users / IT Team. Access to such restricted zone is given against written request by the Managers. • Employees are required to return their ID cards on the last day, and all ID badges are disabled.	

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• The sharing of access badges and tailgating are prohibited by policy. • Access to server rooms are restricted and log of visitors is maintained	• Access to server rooms are restricted and log of visitors is maintained. **Inspection:** • Inspected the badge access deactivation for a select sample of exited employees from the pro watch portal and determined that badge access revocation process is in place. • Inspected the physical access log review emails for a select sample of months and determined that access validation process is in place. • Inspected the Physical Security and Access control policy and determined that sharing of access badges and tailgating are prohibited by policy. • Inspected the server room access logs and determined that visitor log is maintained and monitored.	
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
• Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment. **Inspection:** Inspected the the Cyient Information Security Manual and determined that procedures are defined and documented.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
• External points of connectivity at office network are protected by firewall. • The firewall provides unified threat management (UTM) services such as intrusion protection, web filtering and inbound and out bound traffic filtering. • Incoming connections are accepted from only whitelisted IPs in the firewall. • Company has implemented content filtering system through firewall that blocks access to certain sites such as personal emails, storage etc. • Access to modify firewall rules is restricted by management • Logical access to Company systems is restricted through active directory based domain policies. • Administrative access to the firewall is only enabled through secure connections like https/SSH. • Logs of firewall device are forwarded to SIEM for monitoring suspicious events.	**Inspection:** Inspected the following documents and determined that the defined controls are in place: • Cyient Network diagram for Head office and Manikonda Data center **Observation:** Logged into the Palo Alto firewall and noted the following configurations: • The firewall provides unified threat management (UTM) services such as intrusion protection, web filtering and inbound and out bound traffic filtering. • Rules are configured to restrict inbound and outbound traffic and implicit deny is configured • Company has implemented content filtering system through firewall that blocks access to certain sites such as personal emails, storage etc. • Access to modify firewall rules is restricted by management. • Observed the administrators accessing the company systems using domain credentials and noted that access is controlled only through official IDs. • Observed the management interface settings in the firewall and noted that only secure connections like https/SSH are enabled.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Observed the log configuration in the firewall and noted that forwarding of logs to SIEM is enabled. **Inquiry:** Inquired with the CISO and ascertained that: • External points of connectivity at office network are protected by firewall. • Logical access to Company systems is restricted through active directory based domain policies.	
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
• Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. • VPN connection to the corporate network is encrypted. Also multifactor authentication is enabled while logging into the VPN. • Use of removable media is prohibited by policy except when authorized by management • Deep discovery email inspector is used for quarantining and restricting ransomware, phishing, and other suspicious emails. • Policies are configured in the email gateway for quarantining emails matching criteria	**Inquiry:** Inquired with the CISO and ascertained that: • Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. • VPN connections to both the corporate and cloud networks are encrypted. • Users access Client system only after logging into company network followed by connecting into client network using encrypted channels such as VPN. • Use of removable media is prohibited by policy except when authorized by management **Inspection:** • Inspected the Cyient Information Security Manual and determined that entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
pertaining to anti-spam, malware protection, content filters and phishing protection.	• Inspected the Global protect VPN configuration, encryption settings, multifactor authentication settings and determined that secure remote connectivity is in place for employees. **Observation:** • Observed the removable media restriction configuration in Anti virus and noted that prohibition is enforced. • Observed the dashboard of the deep discovery email inspector, quarantine information and noted that suspicious emails are filtered as per advanced threat indicators. • Observed the policy configuration in the email gateway and noted that policies pertaining to anti-spam, malware protection, content filters and phishing protection are in place.	
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
• Antivirus software is installed on workstations, laptops, and servers. Periodic scans are configured and scheduled to take place. • Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines. • Use of removable media is prohibited by policy except when authorized by management • Deep discovery email inspector is used for quarantining and restricting ransomware, phishing, and other suspicious emails.	**Inquiry:** Inquired with the CISO and ascertained that: • Antivirus software is installed on workstations, laptops, and servers. Periodic scans are configured and scheduled to take place. • Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines. **Observation:** • Logged into the Mcafee ePolicy Orchestrator Anti-virus console version 5.9.1 with the help of the administrator and noted that periodic scans	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Policies are configured in the email gateway for quarantining emails matching criteria pertaining to anti-spam, malware protection, content filters and phishing protection.	are configured. Also noted that periodic updates are be auto installed in the server and connected systems receive updates on a regular basis. • Observed the Cyient USB block rule in Mcafee DLP policy settings and noted that use of removeable media is prohibited. • Observed the dashboard of the deep discovery email inspector, quarantine information and noted that suspicious emails are filtered as per advanced threat indicators. • Observed the policy configuration in the email gateway and noted that policies pertaining to anti-spam, malware protection, content filters and phishing protection are in place.	
SYSTEM OPERATIONS		
CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
• Management has defined configuration standards and hardening standards. • Cyient utilizes a third party service provider for managed Security Operations Center (SOC) and threat monitoring • Periodic Vulnerability assessments are performed by competent Cyient internal staff project wise. Vulnerability assessments are done by the internal cyber security team on regular intervals.	**Inquiry:** Inquired with the CISO and ascertained that: • Management has defined configuration standards and hardening standards. • Cyient utilizes a third-party service provider for managed Security Operations Center and threat monitoring • Vulnerability Assessments are performed on a periodic basis **Inspection:**	No Exception noted.

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Centralized patch management of Servers and systems is in place as per Cyient patch management policy.	Inspected the following documents and determined that the defined controls are in place: • Patch Management policy as configured in the group policy • Alert monitoring dashboard from SOC provider-TCL, incident tickets raised and closure • Select sample of monthly patch update emails circulated internally and corresponding change tickets for initiating the patch updates Inspected the Internal Vulnerability assessment report performed using Nessus tool for the project in scope and determined that no high/critical findings were reported.	
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
• Cyient utilizes a third party service provider for managed Security Operations Center (SOC) and threat monitoring • Vulnerability monitoring scans are performed on a periodic basis. Management takes appropriate action based on the results of the scans.	**Inquiry:** Inquired with the CISO and ascertained that the defined controls are in place: • Cyient utilizes a third party service provider for managed Security Operations Center (SOC) and threat monitoring • Vulnerability monitoring scans are performed on a periodic basis. Management takes appropriate action based on the results of the scans. **Inspection:** Inspected the alert monitoring dashboard from SOC provider-TCL, incident tickets raised and resolved	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	and determined that event logs from systems and servers are monitored. Inspected the Internal Vulnerability assessment report performed using Nessus tool for the project in scope and determined that no high/critical findings were reported.	
CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		

• An incident management process is defined and documented for evaluating reported events.
 	
• Incidents are reported to the Global Helpdesk team (GHD) and resolved
 	
• Reported incidents are logged as tickets and include the following details:
  ○ Severity, date and Time of incident
  ○ Details
  ○ Status
  ○ Root Cause
	Inquiry:
	Inquired with the Senior Manager- Corporate Quality and ascertained that:
	• An incident management process is defined and documented for evaluating reported events.
	• Incidents are reported to the Global Helpdesk team (GHD) and resolved
	• Reported incidents are logged as tickets and include the following details:
	  ○ Severity, date and Time of incident
	  ○ Details
	  ○ Status
	  ○ Root Cause (High severity incidents only)
	
	Inspection:
	Inspected the following documents and determined that the defined controls are in place:
	• Incident Management Procedure
		No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Select sample of incident tickets from GHD helpdesk along with resolution details	
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
• All security incidents are reviewed and monitored by the Security Council Meetings. Corrective and preventive actions are completed for incidents. • All incidents are evaluated, and necessary action taken to close the threat / vulnerability. • Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives. • Reported incidents are logged as tickets and include the following details: o Severity, date and Time of incident o Details o Status o Root Cause (High severity incidents only)	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that the below defined controls are in place: • All security incidents are reviewed and monitored by the Security Council Meetings. Corrective and preventive actions are completed for incidents. • All incidents are evaluated, and necessary action taken to close the threat / vulnerability. • Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives. • Reported incidents are logged as tickets and include the following details: o Severity, date and Time of incident o Details o Status o Root Cause (High severity incidents only) o Lessons learnt, Impact and Improvement opportunities **Inspection:** Inspected the following documents and determined that the defined controls are in place:	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Select sample of incident tickets from GHD helpdesk along with resolution details and corrective action taken • Incident Management Procedure • Security council meeting minutes analyzing the incident types	
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
• All incidents are evaluated and necessary action taken to close the threat / vulnerability • Root cause analysis is performed for major incidents. • Lessons learnt are analyzed, and the incident response plan and recovery procedures are improved.	**Inspection:** Inspected the following documents and determined that the defined controls are in place: • Select sample of incident tickets from GHD helpdesk along with resolution details and corrective action taken • Incident Management Procedure • Security council meeting minutes analyzing the incident types **Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that the below defined controls are in place: • All incidents are evaluated and necessary action taken to close the threat / vulnerability • Root cause analysis is performed for major incidents. • Lessons learnt are analyzed, and the incident response plan and recovery procedures are improved.	No exceptions noted
CHANGE MANAGEMENT		

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
• Entity has defined its change management and approval processes in its IT Change Management policy and procedure. • All change requests are submitted with implementation and rollback plans. • All change requests are logged and change request ticket created. • Major changes are tracked separately as major infra changes and approved by CAB. • Minor change requests are logged in Service Now and approved by the appropriate authority • For high severity incidents, change requests are created. • A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • Entity has defined its change management and approval processes in its IT Change Management policy and procedure. • All change requests are submitted with implementation and rollback plans. • All change requests are logged and change request ticket created. • Minor change requests are logged in Service Now and approved by the appropriate authority • For high severity incidents, change requests are created. • A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • IT Change Management policy and procedure • Select sample of change tickets from Service now with implementation and roll back plan details	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	• Select sample of Emergency change requests and related approvals	
RISK MITIGATION		
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
• A Policy on Business Continuity and Disaster Recovery planning is defined and documented. It includes mitigation activities like planning, communication and recovery efforts, alternate location of work. • Business continuity and disaster recovery plans are tested annually.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • A Policy on Business Continuity and Disaster Recovery planning is defined and documented. It includes mitigation activities like planning, communication and recovery efforts, alternate location of work. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • IT Business Continuity and Disaster Recovery Plan • ISP failover, firewall failover mockdrill reports for Manikonda data center • Firedrill reports pertaining to Madhapur and Manikonda locations	No exceptions noted
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.		
• New Third Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process. • Company obtains and reviews compliance reports and certificates such as ISO 27001, SOC1	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: • New Third Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring. • A formal contract is executed between Company and third Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties. • All customer & vendor contracts have terms related to confidentiality. • Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process. • Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	• Company obtains and reviews compliance reports and certificates such as ISO 27001, SOC1 or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring. • A formal contract is executed between Company and third Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties. • All customer & vendor contracts have terms related to confidentiality. **Inspection:** Inspected the following documents and determined that the defined controls are in place: • Third party service provider security evaluation process • SOC 2 reports of TCL and Service Now • Select sample of contracts/MSA with third party service providers	
ADDITIONAL CRITERIA- AVAILABILITY		
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
• The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements	**Inquiry:** Inquired with the CISO and ascertained that: • Processing capacity is monitored on an ongoing basis using various tools	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Processing capacity is monitored on an ongoing basis. • Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	• Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy. • Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. **Observation:** Observed a select sample of system/host availability reports and noted that processing capacity is monitored on an ongoing basis. **Inspection:** Inspected the ISP failover, firewall failover mock-drill reports for the Manikonda data center and determined that redundancy check is done periodically.	
A 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
• Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. • Devices are checked on a periodic basis and checklists are prepared. • Fire drill is conducted annually.	**Observation:** Observed through a virtual tour of the facilities at Madhapur and Manikonda and noted that: • Following environmental protections have been installed including the following in critical areas: · o Air conditioners o UPS in the event of power failure o Redundant exit points o Smoke detectors o Fire Extinguishers o Diesel generators	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
• Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. • DG set of sufficient capacity is provided to provide power during outage. • Company has multiple ISPs in place to provide redundancy in case of link failure • IT Engineer monitors the temperature in server room on a daily basis and take corrective actions in case of discrepancy • Vendor AMC specifications are documented and followed up for service requirements. • Facilities and admin personnel monitor the status of environmental protections on a regular basis.	• Observed the Server rooms and noted that IT Engineer monitors the temperature in server room on a daily basis and take corrective actions in case of discrepancy **Inspection:** • Inspected the Network diagram of Cyient Madhapur and Manikonda DC and determined that Company has multiple ISPs in place to provide redundancy in case of link failure. • Inspected the preventive maintenance reports for Air conditioners, Diesel Generators, UPS, fire alarms and determined that environmental protections receive maintenance on at least an annual basis. • Inspected the fire drill reports conducted in Madhapur, Manikonda locations, ISP failover, firewall failover mock-drill reports for the Manikonda data center and determined that the Business continuity and disaster recovery plans, are tested periodically. Also testing results and change recommendations are reported to the concerned teams. • Inspected the vendor AMC details maintained for Madhapur and Manikonda facilities and determined that vendor AMC specifications are documented and followed up for service requirements. **Inquiry:** Inquired with the Manager- Facilities and ascertained that Operations personnel monitor the	

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	status of environmental protections during each shift.	
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives. The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
• Business continuity and disaster recovery plans, are tested annually. • Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented.	**Inspection:** Inspected the fire drill reports conducted in Madhapur, Manikonda locations, ISP failover, firewall failover mock-drill reports for the Manikonda data center and determined that the Business continuity and disaster recovery plans, are tested periodically. Also testing results and change recommendations are reported to the concerned teams. • IT Business Continuity and Disaster Recovery Plan **Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that Business continuity plan testing is performed on a periodic basis.	No exceptions noted
ADDITIONAL CRITERIA- CONFIDENTIALITY		
C 1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
• The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that the entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	No exceptions noted

Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Result
	Inspection: Inspected the Cyient Information Security Manual and determined that the defined control is in place.	
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
• The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	**Inquiry:** Inquired with the Senior Manager- Corporate Quality and ascertained that: The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed. **Inspection:** Inspected the Cyient Information Security Manual and determined that the defined control is in place.	No exceptions noted

Section V – Other Information Provided by the Management of Cyient

The information included in Section V of this report is presented by Cyient to provide additional information to user entities and is not part of Cyient's description of the system. The information included here in Section V has not been subjected to the procedures applied in the examination of the description of the system related to description of the system, and, accordingly, M Kuppuswamy PSG & Co LLP expresses no opinion on it.

Management's responses to exceptions noted:

The table below contains Management's response to the exceptions noted in Section IV - Information Provided by Independent Service Auditor.

Item	Control Activity	Exception noted	Management Response
CC 5.3	All policies are updated/reviewed at least every year to ensure that these are current and in line with the current business.	In some instances, MKPSG could not verify if the policy documents were periodically reviewed in the absence of relevant information in the policy document version history.	Cyient has reviewed policy documentation and will take steps to document the same.

*****End of the Report*****