entigrity

System and Organization Controls 2 (SOC 2) Type 1 Report

Description of *"Entigrity Pvt Ltd."*
relevant to Security, Availability, Privacy and Confidentiality
As of December 31, 2022

(SSAE 18 – SOC 2 Type I Report)

Table of Contents

Section I

Assertion of Entigrity's Management

entigrity

ASSERTION OF ENTIGRITY MANAGEMENT

We have prepared the accompanying description of ***Entigrity Pvt Ltd.*** system titled ***"Offshore Accounting Solution"*** (Description) As of December 31 , 2022 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 ***"Offshore Accounting Solution"*** that may be useful when assessing the risks arising from interactions with, particularly information about the system controls that ***Entigrity Pvt Ltd.*** 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, Availability, Privacy and Confidentiality* set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

The description includes only the controls of ***Entigrity Pvt Ltd.*** and excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organizations' controls contemplated in the design of ***Entigrity Pvt Ltd.*** controls are suitably designed and operating effectively, along with related controls at the ***Entigrity Pvt Ltd.*** The description does not extend to controls of the subservice organizations.

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

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

a. The description fairly presents the ***"Offshore Accounting Solution"*** throughout the period as of December 31, 2022 based on the following description criteria:

i. The description contains the following information:

1. The types of services provided:
2. The principal service commitments and system requirements:
3. The components of the system used to provide the services, which are as follows:
    a. Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
    b. Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

c. People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
d. Procedures. The automated and manual procedures in the operation of a system.
e. Data. The information used and supported by a system (Transaction streams, files, databases, tables, and output used or processed by the system).

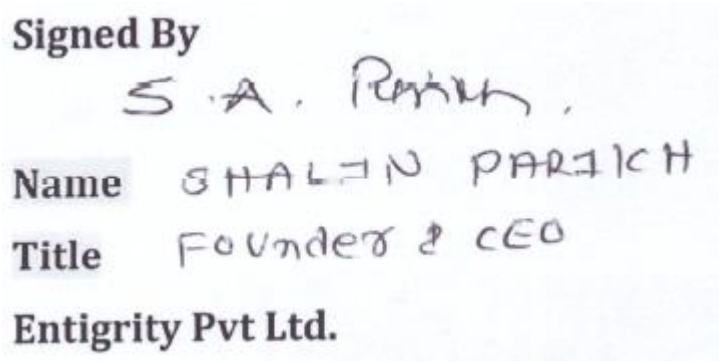
4. For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, as of the date of the description the following information:
    a. Nature of each incident
    b. Timing surrounding the incident
    c. Extent (or effect) of the incident and its disposition
5. The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.
6. If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)
7. If the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, the following:
    a. The nature of the service provided by the subservice organization
    b. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization
    c. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)
8. Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant.
9. There were no significant effects of COVID-19 epidemic spate on the ***Entigrity Pvt Ltd.***, its operations and the technologies used. In fact, there have not been any significant change in the business process execution as well. The technologies that were used before the pandemic period have been extended and applied to all the operating staff irrespective of the fact whether they work on the Client's environment using client's resources or ***Entigrity Pvt Ltd.'s*** systems and resources. With the advent in technology,

physical presence of operating staff has not been a cause for concern while performing the operations efficiently and effectively by allowing them to work remotely.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed as of December 31, 2022 to provide reasonable assurance that ***Entigrity Pvt Ltd.'s*** service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of December 31, 2022 and if the subservice organization and user entities applied the complementary controls assumed in the design of ***Entigrity Pvt Ltd.'s*** controls as of December 31, 2022.

c. ***Entigrity Pvt Ltd.*** controls stated in the description were operated effectively as of December 31, 2022to achieve ***Entigrity Pvt Ltd.'s*** service commitments and system requirements based on the applicable trust services criteria, if its controls operated effectively as of December 31, 2022 and if the subservice organization and user entities applied the complementary controls assumed in the design of ***Entigrity Pvt Ltd.'s*** controls as of December 31, 2022.



Date: 10th January 2023

Section II

Independent Service Auditor's Report

entigrity

KRATIKAL
SECURE FOR SURE

Independent Service Auditor's Report

To
Shalin Parikh
Founder & CEO
Entigrity Pvt Ltd.

Scope

We have examined ***ENTIGRITY's*** accompanying description in ***Section III*** titled **" *Offshore Accounting Solution "*** as of December 31, 2022, (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 as of December 31, 2022, to provide reasonable assurance that ***ENTIGRITY's*** service commitments and system requirements were achieved based on the trust services criteria relevant to ***Security, Availability, and Confidentiality*** (applicable trust services criteria) set forth in **TSP Section 100, 2017** *Trust Services Criteria for Security, Availability, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ***ENTIGRITY***, to achieve ***ENTIGRITY's*** service commitments and system requirements based on the applicable trust services criteria. The description presents ***ENTIGRITY's*** controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ***ENTIGRITY's*** controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

The information included in ***Section V, "Other Information Provided by ENTIGRITY"*** that is not covered by this Auditor's Report, is presented by ***ENTIGRITY's*** management to provide additional information and is not a part of ***ENTIGRITY's*** description. Information about ***ENTIGRITY's*** management responses to exceptions identified in the report and glossary of terms has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve ***ENTIGRITY'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

ENTIGRITY is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ***ENTIGRITY's*** service commitments and system requirements were achieved. In ***Section II***, ***ENTIGRITY*** has provided its assertion titled ***"Assertion of ENTIGRITY Management"*** (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ***ENTIGRITY*** is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria if those controls operated effectively;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

The physical distancing and restriction on interstate movement due to COVID-19 epidemic has posed a real threat and challenge as the data collection, correspondence, interviewing the auditee, presentations etc., being done virtually. Lack of personal interaction with the attendee and not making physical visits to the premise could potentially limit the scope of audit. we were unable to determine whether changes in the system processes and resources might have been warranted in respect of effectiveness and efficiency of system of internal controls.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in ***Section IV***, ***"Trust Services Security Criteria, Related Controls, and Tests of Controls,"*** of this report in columns 2***, 3, and 4*** respectively.

Opinion

In our opinion, in all material respects,

a. the description presents ***ENTIGRITY's*** **"Content Management, Data Collection & Analytics and Machine Learning Services"** that was designed and implemented as of December 31, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of December 31, 2022, to provide reasonable assurance that ***ENTIGRITY'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 subservice organizations and user entities applied the complementary controls assumed in the design of ***ENTIGRITY's*** controls throughout that period.

c. the controls stated in the description operated effectively as of December 31, 2022, to provide reasonable assurance that ***ENTIGRITY's*** service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ***ENTIGRITY's*** controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in ***Section IV,*** is intended solely for the information and use of ***ENTIGRITY***, user entities of ***ENTIGRITY's*** **"Content Management, Data Collection & Analytics and Machine Learning Services"** during some or all of the period as of December 31, 2022 business partners of ***ENTIGRITY*** that were subject to risks arising from interactions with the ***ENTIGRITY's*** **" *Offshore Accounting Solution ***"**, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and

- The risks that may threaten the achievement of the service organization's service commitments and system requirements 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.

Section III

Description of the ENTIGRITY's

"Offshore Accounting Solution"

As of December 31, 2022

entigrity

A. Background and Overview of Services

Entigrity is a leading offshore staffing solutions provider to accounting and tax firms across North America and the UK. They help small and mid-sized accounting business firms hire qualified and experienced offshore staff at economical rates. They are the **preferred outsourcing partner for 30 out of the top 100 US Accounting firms**. With a workforce of **2,000+ accounting experts**, Entigrity have **served 600+ CPAs** and public accounting firms nationwide with an unmatchable client retention rate! Entigrity is headquartered in Sugar Land, TX, with offshore offices in India.

Entigrity is an ISO 27001:2013 certified organization for information security and ISO 9001:2013 certification for Quality Management. They comply and enforce best business practices in terms of Information Security and Quality Management. Their endeavour garners high brand trust and wins the confidence of every client They work with!

A.2. Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope
The scope of this report is limited to Offshore Accounting Solution activities **Products** • N/A **Services** • Tax • Accounting • Auditing • Non-accounting

Office Location	**Address**
Ahmedabad, India	SAKAR-1, 9TH-11TH FLOOR, ASHRAM ROAD, ELLISBRIDGE, AHMEDABAD, GJ 380009
Ahmedabad, India	ENTIGRITY HOUSE, 18, PATEL SOCIETY, OFF C.G. ROAD, AHMEDABAD, GJ 380009
Vadodara, India	701, K.P PLATINA, ABOVE TANISHQ SHOWROOM, NEXT TO VIDHYUT BHAVAN, RACECOURSE ROAD, VADODARA, GJ 390007
Mumbai, India	FL-3, B WING, SHAH INDUSTRIAL ESTATE, ANDHERI (EAST), MUMBAI, MH 400072
Kochi, India	3rd floor, Modayil Centre Point,
Indore, India	301, Bansi Trade Centre, Mahatma Gandhi Rd

Jaipur, India	Plot No. 59 Nemi Nagar Vistar, Vaishali Nagar
Gandhinagar, India	Brigade International Financial Center, Gift City
Rajkot, India	4th Floor, Bhabha Bizz Hub
Texas, US	1600 HIGHWAY 6 SOUTH, SUITE 250, SUGAR LAND, TX, 77478 USA
Florida, US	1467 SILVER LEAF DR, LAKELAND FL 33813
Mississauga, Canada	1311 FREEPORT DR,MISSISSAUGA, ON, L5C 1S5
LONDON, UK	KEMP HOURSE, 160 CITY ROAD, LONDON EC1V 2NX

The report excludes all processes and activities that are executed outside above locations. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

A.3. Control Environment

ENTIGRITY PVT LTD '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, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at ENTIGRITY PVT LTD 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.

A.4. Integrity and Ethical Values

ENTIGRITY PVT LTD requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations. ENTIGRITY PVT LTD promotes an environment of open 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.

A.4.1. Board of Directors

Business activities at ENTIGRITY PVT LTD are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its founder as the Chairman & CEO is in charge of the company's Global operations playing a key role in strategy and client management.

A.5.Management's Philosophy and Operating Style

The Executive Management team at ENTIGRITY PVT LTD assesses risks prior to venturing into business ventures and relationships. The size of ENTIGRITY PVT LTD enables the executive management team to interact with operating management on a daily basis.

B. 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 is formally assessed.

ENTIGRITY PVT LTD has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User 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

ENTIGRITY PVT LTD has developed an organization-wide ENTIGRITY PVT LTD Information Security Policies.

Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet or as hard copy policies to new employees. Changes to the Information Security Policies are reviewed by and approved by prior to implementation.

C. Monitoring

Monitoring is a 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. ENTIGRITY PVT LTD management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities. ENTIGRITY's is maintaining register for all the assets & Infrastructure, critical resources are being monitored for confidentiality, integrity, availability and risk assessment is periodically reviewed and is monitored.

D. Information and Communication

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

ENTIGRITY PVT LTD 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 ENTIGRITY PVT LTD's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with ENTIGRITY PVT LTD employees.

D.1. Electronic Mail (e-Mail)

Communication to Customer Organizations and project teams through e-Mail. 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.

E. Components of the System

E.1. Infrastructure

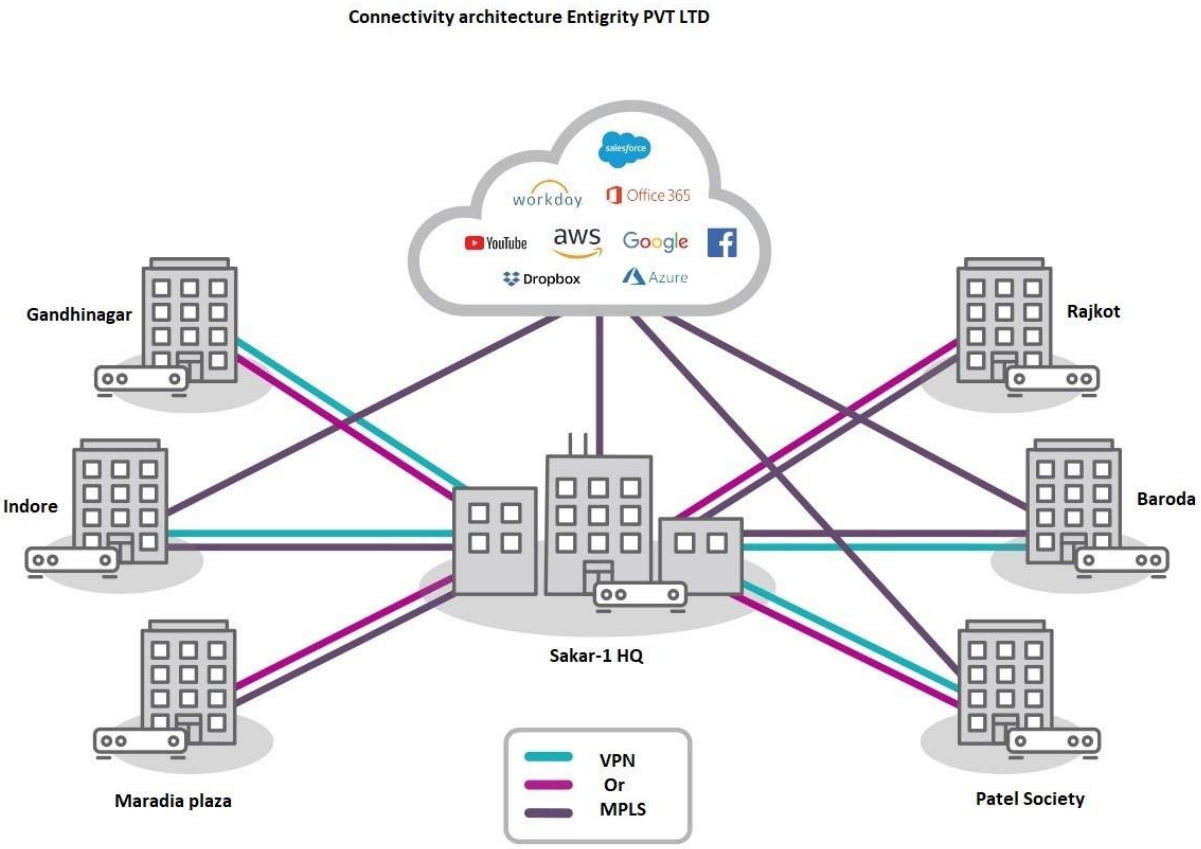
The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

E.1.1. Network Segmentation Overview

ENTIGRITY PVT LTD offices are equipped with the latest hardware, software and networking infrastructure. Offices are linked using high speed communication links, backed up by redundant networks.

E.1.2. NETWORK DIAGRAMS

NETWORK DIAGRAM



E.1.3. Physical Control Access

Entigrity Pvt Ltd has implemented the Biometric fingerprint and entrance and to the restroom. Identix biometric device is used for access control. Every access and denial is monitored in the system. Access adding and removing by the request of management and done by HR team.

E.1.4. Access to the Server Room

Entigrity Pvt Ltd have an access restricted server. Firewall, core switch, patch panel is in room. All the products related to Entigrity Pvt Ltd are separated and locked in Room. Access to the server is for System admin of Entigrity Pvt Ltd and the security employed in the premises.

E.1.5. Electric Backup

At Entigrity we have we use a stabilizer for controlling power fluctuation.

E.1.6. Fire Safety

- keeping their workplace tidy and having a good standard of housekeeping
- regularly removing combustible waste, including accumulations of dust
- keeping ignition sources away from combustible material or flammable liquids and gases
- keeping use of flammable liquids to a minimum and closing containers when not in use.

For Fire Safety We have installed a Fire Extinguisher Type which is Water Basis (Solid Red) and CO2 extinguisher.

Fire Drills

They do Fire drill twice in a year.

F. Software

F.1. Firewalls

Entigrity is currently using SonicWALL Nsa 4700

F.2. Security 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 is not permitted.

In order to stop any malware from affecting the security of the customer and organizational data, <ENTIGRITY PVT LTD> 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.

In order to stop any malware from affecting the security of the customer and organizational data, Entigrity uses daily Webroot Endpoint Protection vulnerability scans along with UTM devices. The 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.

ENTIGRITY PVT LTD 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 ENTIGRITY PVT LTD '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.

F.1.3 Patch Management

Entigrity security team ensures that all patches to network device/servers operating systems are checked for stability & any availability issues & tested before applying to the production environment. Before deployment of any patches they are tested and deployed. The patch management activity is done regularly or as and when any

critical event occurs and required updates or patch are installed to ensure efficient working of the servers, desktops and critical network devices. Operating system patches are managed and applied as they become available.

G. Vulnerability Scans & Intrusion Detection/Intrusion Prevention

Entigrity is currently using Seqrite Cloud Vulnerability on a weekly basis
Entigrity has an Advanced Av Protection system that includes a Vulnerability scan weekly and intrusion detection or prevention on daily basis.

H. People

The organizational structure of ENTIGRITY PVT LTD 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 ENTIGRITY PVT LTD clients.

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.

ENTIGRITY PVT LTD'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.

Roles and Responsibilities

1. Recruit candidates

From time to time we hire staff as per the requirement of the company which is in terms of semi-skilled and skilled staff.

2. Hire the right employees

For Hiring right candidate, we have a process where we hunt data from different platforms like Linkedin and other recruitment platform.

3. Process payroll

We Process our payroll every first week of the month. We collected all attendance data from our biometric by end of the month and on that basis we process payroll.

4. Conduct disciplinary actions

We have in-house policy such us No mobile phone on the floor/ No Food item on the floor/ Attire Policy etc..

5. Update policies

Policies are always updated as per the business requirement and staff benefits.

6. Maintain employee records

We have in-house software to maintain record of our staff and their work.

7. Conduct benefit analysis

Improving quality in service emphasizes the need to understand customer or client needs, measure achievements in terms of those needs, and use measurements to adjust processes so that the needs are better met and we give benefits accordingly.

H.1. Commitment to competence

ENTIGRITY PVT LTD'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 and anticipated needs of Business. Employees are evaluated on an Annual basis to document performance levels and to identify specific skill training needs.

H.2. Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within ENTIGRITY PVT LTD.

H.3. New Hire Procedures

HR needs to understand the organization's needs and make sure those needs are met when recruiting for new positions. It's not as simple as just throwing an ad up on Indeed: you'll need to analyze the market, consult stakeholders, and manage budgets.

Then, once the role is advertised, more research needs to be done to make sure that the right candidates are being attracted and presented. Recruiting is a massive—and costly—undertaking; the right candidate can revitalize an entire organization, but the wrong candidate can upend operations

H.4. Training and Development

We provide training on Information system and its security.

H.5. Performance Evaluation

Stagnation is bad for business, and it's smart to keep your best employees with the company. HR can provide career paths to help guide each employee to a long future within the company. HR can then check in periodically to further guide employees on their career paths

H.6. New Employee Training

Entigrity provide two inductions: Date of joining induction and then refresher's Induction.

H.7. Employee Terminations

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

H.8. 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 higher level in IT and Operation team.

I. Outbound Communication

ENTIGRITY development Applications are accessible in ENTIGRITY Network. For uploading the files and communication to the client, external internet access is required. Internet usage is restricted with firewall. The IT Team periodically reviews and recommends changes to web and protocol filtering rules.

J. Backup and Recovery of Data

ENTIGRITY 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.
ENTIGRITY 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.

The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the "Data Archival and Retention Policy"
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.

K. Data Restoration Procedure

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

L. Other Information Provided by ENTIGRITY

The information provided in this section is provided for informational purposes only by ENTIGRITY. Independent Auditor has performed no audit procedures in this section.

L.1. Disaster and Recovery Services

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks as opposed to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions. As a result, a service organization should not include in its description of controls any specific control procedures that address disaster recovery planning. Therefore, ENTIGRITY's disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls, ENTIGRITY has implemented to safeguard against an interruption of service, ENTIGRITY has developed a number of procedures that provide for the continuity of operations in the event of an extended interruption of service at its data centre. In the event of an extended interruption of service, ENTIGRITY will utilize backup site maintained.
The disaster recovery plan defines the roles and responsibilities and identifies the critical IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis.

Disaster recovery process is configured for internet services. Primary and backup line are there and the same is taken care by automatic switch over process. If the primary is down and for primary and backup line both are offline having another line which will serve the purpose for internet services and for production Servers as of now, we have not configured any.

Section IV

Description of Criteria, ENTIGRITY's

"Offshore Accounting Solution"

As of December 31, 2022

A. Testing Performed and Results of Entity-Level Controls

In planning the nature, timing and extent of testing of the system controls based on the Trust Services Criteria, Kratikal Tech considered the aspects of ENTIGRITY's control environment and tested those that were considered necessary.

In addition to the tests of operating effectiveness of specific controls described below including the Trust Services Criteria, the procedures included tests of the following components of the internal control environment of ENTIGRITY:

- Communication and Information
- Risk Assessment
- Monitoring Activities
- Control Activities
- Logical and Physical Access Controls
- System Operations
- Change Management
- Risk Mitigation

Tests of the control environment included the following procedures, to the extent Kratikal Tech considered necessary:

a) A review of ENTIGRITY organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals and personnel controls;
b) Discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and
c) Observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of the testing of system controls based on Trust Services Criteria and controls relevant to the achievement of the control objectives.

B. Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), Kratikal Tech performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

- inspect the source of the IPE,
- inspect the query, script, or parameters used to generate the IPE,
- mapping data between the IPE and the source, and/or
- inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls and system controls based on Trust Services Criteria requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), Kratikal Tech inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the source data or inputs.

C. Trust Services Criteria and Related Controls for Systems and Applications

The applicable Trust Services criteria and the controls to meet the criteria have been specified by, and are the responsibility of ENTIGRITY. The "Tests Performed Kratikal Tech" and the "Results of Tests" are the responsibility of the service auditor.

D. Information System Control Environment

The following controls apply to the services listed in the System Description.

D.1. ENTIGRITY Controls Mapped to the Security, Availability, Confidentiality Criteria

- Security Principle: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.
- Availability Principle: The system is available for operation and use to meet the entity's commitments and system requirements.
- Confidentiality Principle: Information designated as confidential is protected to meet the entity's commitments and system requirements.

E. Tests of Operating Effectiveness

Kratikal Tech's tests of the operating effectiveness of the controls specified by ENTIGRITY included such tests as has been considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified control objectives until the period December 31, 2022
. In selecting particular tests of the operating effectiveness of controls we considered:

1) the nature of the controls being tested;
2) the types and completeness of available evidential matter;
3) the nature of the control objectives to be achieved;
4) the assessed level of control risk;
5) the expected efficiency and effectiveness of the test; and,
6) the testing of other controls relevant to the stated control objectives.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities or their auditors for the system controls based on Trust Services Criteria specified to achieve the stated objective are presented in this section under the column heading "Results of Testing".

Exceptions, if any, identified herein are not necessarily considered significant deficiencies or material weaknesses in the system of ENTIGRITY, as this determination can only be made after consideration of controls in place at user entities.

F. Types of Tests Performed

F.1. Description of testing procedures performed

Kratikal Tech performed a variety of tests relating to the controls listed in this section until the period December 31, 2022 and were applied to those controls relating to control objectives specified by ENTIGRITY.

In addition to the tests listed below, ascertained through multiple inquiries with management and the process owner / control owner that each Trust Service Criteria listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
	Inquired of competent personnel seeking relevant information or representation to obtain knowledge and additional information regarding the policy or procedure; and also corroborating evidence of the policy or procedure.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, a) the Examination / Inspection of source documentation and authorizations to verify transactions processed; b) Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures, approvals, exceptions etc.; c) Examination / Inspection of systems documentation, configurations and settings; and d) Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Re-performance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible process owner / control owner.

entigrity

G. Control Criteria and Control Description

Ref. #	Criterial Description
CC1.0: Common Criteria Related to Control Environment	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0: Common Criteria Related to Communication and Information	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0: Common Criteria Related to Risk Assessment	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0: Common Criteria Related to Monitoring Activities	
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	COSO Principle 17: 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.

Ref. #	Criterial Description
CC5.0: Common Criteria Related to Control Activities	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0: Common Criteria Related to Logical and Physical Access Controls	
CC6.1	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.
CC6.2	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.
CC6.3	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.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	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.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Ref. #	Criterial Description
CC7.0: Common Criteria Related to System Operations	
CC7.1	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.
CC7.2	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 analysed to determine whether they represent security events.
CC7.3	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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0: Common Criteria Related to Change Management	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0: Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.
Additional Criteria for 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.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
Additional Criteria for Confidentiality	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Kratikal tested the design of controls at Entigrity. The results of our testing are as below.

Trust Service Category: Security		
Domain - Control Environment		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 1.1 - The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Clauses relating to confidentiality and ethical behavior standards are signed and accepted by new joiners as part of an appointment letter.	No Exceptions Noted.
CC1.1.2	Personnel is required to read and accept the intellectual property and confidentiality agreement which include clauses on expected conduct upon their hire.	No Exceptions Noted.
Control Criteria 1.2 - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The entity's organizational structure ensures segregation and independence of the Top management.	No Exceptions Noted.
CC1.2.2	Responsibilities of the Top Management relating to oversight of internal controls are documented and accepted by the Top Management.	No Exceptions Noted.
CC1.2.3	Periodic meetings are conducted with key stakeholders responsible for designing, implementing and maintenance of internal control systems to ensure visibility.	No Exceptions Noted.
Control Criteria 1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning and management process and revises these when necessary to help meet changing commitments and system requirements.	No Exceptions Noted.
CC1.3.2	Job descriptions for employees and roles and responsibilities for all personnel tasked with designing, developing, implementing, operating, maintaining, monitoring, and approving system requirements are defined and communicated to all personnel including third parties.	No Exceptions Noted.
Control Criteria 1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Job requirements are documented in job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and performance review process.	No Exceptions Noted.
CC1.4.2	Employee competency and skills are evaluated and training for development (wherever necessary) for the same is provided.	No Exceptions Noted.

CC1.4.3	During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional resources in order to achieve business objectives.	No Exceptions Noted.
CC1.4.4	The entity conducts a previous employment check for all new employees. Criminal and reference check are conducted whenever requested by the client.	No Exceptions Noted.
Control Criteria 1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Personnel is required to read and accept the intellectual property and confidentiality agreement which include clauses on expected conduct upon their hire.	No Exceptions Noted.
CC1.5.2	Clauses relating to confidentiality and ethical behaviour standards are signed and accepted by new joiners as part of an appointment letter.	No Exceptions Noted.
CC1.5.3	Job descriptions and roles and responsibilities for personnel tasked with designing, developing, implementing, operating, maintaining,monitoring, and approving system requirements are defined and communicated to all personnel including third parties.	No Exceptions Noted.
CC1.5.4	Job descriptions are reviewed and approved by the appropriate personnel.	No Exceptions Noted.
CC1.5.5	Job requirements are documented in job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and performance review.	No Exceptions Noted.
CC1.5.6	Employee competency and skills are evaluated and training for development (wherever necessary) of the same is provided.	No Exceptions Noted.
CC1.5.7	Employee training program to promote awareness of information security requirements is conducted annually.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Communication & Information		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	A description of the system is posted on the intranet and is available to the entity's internal users. This description delineates the boundaries of the system and key aspects of processing.	No Exceptions Noted.
CC2.1.2	Process and guidelines documents for significant processes are available on the entity's intranet and made available to all employees.	No Exceptions Noted.
Control Criteria 2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Process and guidelines documents for significant processes which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are available on the entity's intranet and made available required users.	No Exceptions Noted.
CC2.2.2	An escalation matrix is defined and shared with relevant users for grievance redressal.	No Exceptions Noted.
CC2.2.3	Job descriptions and roles and responsibilities for maintaining, and monitoring system operations are defined and communicated to all personnel.	No Exceptions Noted.
CC2.2.4	System requirements relating to security, availability, and confidentiality based on the organization's commitments are identified and communicated to relevant internal users.	No Exceptions Noted.
Control Criteria 2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	System descriptions are made available to required and authorized external users that describe the boundaries of the system and describe significant system components as well as the purpose and design of the system.	No Exceptions Noted.
CC2.3.2	Agreements are established with clients that include clearly defined terms, conditions, confidentiality clauses, minimum privacy and security requirements and SLA.	No Exceptions Noted.
CC2.3.3	Client training for purposeful use of ticketing tool is conducted.	No Exceptions Noted.
CC2.3.4	Agreements are established with third-party vendors or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	No Exceptions Noted.

CC2.3.5	Vendor agreements include responsibilities and protocol to be followed in case of failures, incidents, concerns and complaints.	No Exceptions Noted.
CC2.3.6	Escalation matrix is defined and shared with external users for grievance redressal.	No Exceptions Noted.
CC2.3.7	The periodic meeting is conducted with the client communicating the project status and project health as per the decided timelines.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Risk Assessment		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	System requirements relating to security, availability and confidentiality based on the organization's commitments are identified and communicated to relevant internal users.	No Exceptions Noted.
Control Criteria 3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.		
CC3.2.1	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating internal and external risks based on identified threats and the specified tolerances.	No Exceptions Noted.
CC3.2.2	During the risk assessment and management process, risk management personnel identify risks to internal operations and update the potential threats to system objectives. In response to the identification of such risks, management updates its processes, and controls, as needed.	No Exceptions Noted.
Control Criteria 3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No Exceptions Noted.
CC3.3.2	The risk assessment and management process include assessment of possible fraud including but not limited to incorrect reporting, loss of assets, corruption, unauthorized information acquisition and leakage.	No Exceptions Noted.
Control Criteria 3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No Exceptions Noted.
CC3.4.2	The risk assessment and management process include assessment of possible fraud including but not limited to incorrect reporting, loss of assets, corruption, unauthorized information acquisition and leakage.	No Exceptions Noted.
CC3.4.3	Periodic meetings are conducted to formulate product roadmap and prioritize functionalities for product enhancement and future releases.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Monitoring Activities		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 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.		
CC4.1.1	Compliance to system controls implemented for mitigating risks to the confidentiality, security, availability and related security policies are checked through internal assessments, and independent external audit. Based on the reported, necessary action is initiated to minimize risk exposure.	No Exceptions Noted.
CC4.1.2	Services are monitored periodically through service level management process that monitor compliance with service level commitments and agreements. Results are shared with management as per agreed schedule.	No Exceptions Noted.
CC4.1.3	Support team manager conducts periodic reviews of customer support and ticketing, and breaches.	No Exceptions Noted.
Control Criteria 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.		

CC4.2.1 CC4.2.2	Compliance to system controls implemented for mitigating risks to the confidentiality, security, availability and related security policies are checked through internal assessments, vulnerability assessment and penetration testing and independent external audit. Based on the reported, necessary action is initiated to minimize risk exposure. Operations and security personnel follow the ticketing system for recording, tracking resolving and escalating reported issues.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Control Activities		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	Compliance to system controls implemented for mitigating risks to the confidentiality, security, availability and related security policies are checked through internal assessments, vulnerability assessment and penetration testing and independent external audit. Based on the reported, necessary action is initiated to minimize risk exposure.	No Exceptions Noted.
CC5.1.2	Segregation of Duties is established for incompatible job responsibilities.	No Exceptions Noted.
Control Criteria 5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	Controls over the asset, access, change, incident, malware, backup, system acquisition and maintenance have been documented and implemented to support the achievement of objectives.	No Exceptions Noted.
CC5.2.2	System infrastructure including workstations, servers, databases, VPN, firewalls, routers and switches are configured as per defined Hardening guidelines.	No Exceptions Noted.
CC5.2.3	The dedicated Support team is tasked with the responsibility of addressing client queries, issues and complaints in stipulated time.	No Exceptions Noted.
Control Criteria 5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	Process and guidelines documents for significant processes that address system requirements are defined and available on the entity's intranet.	No Exceptions Noted.
CC5.3.2	Process and guidelines documentation are reviewed periodically and updated wherever necessary.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Logical and Physical Access Controls		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 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.		
CC6.1.1	Role-based access process has been defined and implemented. Privileged access to sensitive resources is restricted to defined user roles post requisite approval.	No Exceptions Noted.
CC6.1.2	Logical access rights are reviewed on a periodic basis.	No Exceptions Noted.
CC6.1.3	External access to cloud resources by employees is permitted only through a virtual private network (VPN) connection.	No Exceptions Noted.
CC6.1.4	Access to the application is through HTTPS communication channel or VPN (wherever requested by client).	No Exceptions Noted.
CC6.1.6	Data in transit is encrypted using TLS and disk-level encryption of data is ensured for data at rest.	No Exceptions Noted.
CC6.1.7	Password complexity standards are established to enforce control over access passwords.	No Exceptions Noted.
Control Criteria 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.		
CC6.2.1	HR/ Department Manager initiates access provisioning or modification request. Accordingly, accesses are provided after requisite approval.	No Exceptions Noted.
CC6.2.2	HR/ Department Manager initiates access revocation request for termination/ suspension of user accounts. Accordingly, accesses are revoked within 24 hours.	No Exceptions Noted.
CC6.2.3	Client access to the application is provided to authorized users based on roles requested and approved by the client.	No Exceptions Noted.
Control Criteria 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.		
CC6.3.1	Role-based access process has been defined and implemented. Privileged access to sensitive resources is restricted to defined user roles post requisite approval.	No Exceptions Noted.

Ref. Nos.	Entity Controls	Exceptions
Control Criteria 6.4 - The entity restricts physical access to facilities and protected information assets(for example, data centre facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Access to sensitive areas such as server and hub rooms is restricted to authorized personnel.	No Exceptions Noted.
CC6.4.2	Physical access is controlled by means of employee ID cards at entry and exit points and within the facilities. ID cards are collected during exit interviews for employees leaving the organization.	No Exceptions Noted.
CC6.4.3	Visitor entry is recorded in registers and controlled through separate badges and mandated escort by an employee.	No Exceptions Noted.
CC6.4.4	Critical points are recorded by closed-circuit television camera (CCTV).	No Exceptions Noted.
Control Criteria 6.5 - The entity discontinues logical and physical protections over physical assetsonly 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.		
CC6.5.1	The organization has defined a Record Maintenance guideline which prescribes protocol to be followed for classification of information.	No Exceptions Noted.
CC6.5.2	Data storing media is subjected to low-level formatting and physical destruction as part of asset disposal.	No Exceptions Noted.
CC6.5.3	Paper shredders are used in office premises to dispose-off confidential information present in paper form.	No Exceptions Noted.
Control Criteria 6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Network traffic is monitored and controlled through the firewall. Generated alerts are reviewed for any potential intrusion.	No Exceptions Noted.
CC6.6.2	The monitoring tool is used to index data from infrastructure components to monitor potential security threats and vulnerabilities and detect unusual system activity or service requests.	No Exceptions Noted.
CC6.6.4	Operations and security personnel follow a ticketing system for recording, tracking resolving and escalating reported issues.	No Exceptions Noted.
Control Criteria 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.		
CC6.7.1	The organization has defined a Record Maintenance Guidelines which prescribes protocol to be followed for classification of information.	No Exceptions Noted.

Ref. Nos.	Entity Controls	Exceptions

CC6.7.2	VPN, SSL, Secure File Transfer Protocol (SFTP), and other encryption technologies are used for defined points of connectivity and to protect the information in transit.	No Exceptions Noted.
CC6.7.3	Storage for workstations and laptops is encrypted.	No Exceptions Noted.
CC6.7.4	External storage devices such as removable USB storage drives are disabled on the workstations using group policies.	No Exceptions Noted.
CC6.7.5	Copy/ paste functionality is disabled on workstations that may be used to access application data hosted on cloud infrastructure.	No Exceptions Noted.
Control Criteria 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.		
CC6.8.1	The organization has installed anti-virus software on all workstations and servers for protection against malware.	No Exceptions Noted.
CC6.8.2	Anti-virus servers are configured to update virus definition automatically at a periodic basis.	No Exceptions Noted.
CC6.8.3	Anti-virus software is configured to scan servers and workstations for malware signatures on a continual basis with scheduled full scans.	No Exceptions Noted.
CC6.8.4	The ability to install software on workstations is restricted to IT support personnel.	No Exceptions Noted.

Trust Service Category: Security		
Domain - System Operations		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 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.		
CC7.1.1	Network traffic is monitored and controlled through the firewall. Generated alerts are reviewed for any potential intrusion.	No Exceptions Noted.
CC7.1.2	The monitoring tool is used to index data from infrastructure components to monitor potential security threats and vulnerabilities and detect unusual system activity or service requests.	No Exceptions Noted.
CC7.1.3	Vulnerability assessment, penetration testing and application security exercises are performed on a periodic basis.	No Exceptions Noted.
CC7.1.4	Operations and security personnel follow a ticketing system for recording, tracking resolving and escalating reported issues.	No Exceptions Noted.
CC7.1.5	Infrastructure components requiring updates are patched periodically with applicable patches. These are tested in a test environment identical to the production prior to deployment.	No Exceptions Noted.
CC7.1.6	System infrastructure including workstations, servers, databases, VPN, firewalls, routers and switches are configured as per defined Hardening guidelines.	No Exceptions Noted.
Control Criteria 7.2 - The entity monitors system components and the operation of those componentsfor anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity'sability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Network traffic is monitored and controlled through the firewall. Generated alerts are reviewed for any potential intrusion.	No Exceptions Noted.
CC7.2.2	The monitoring tool is used to index data from infrastructure components to monitor potential security threats and vulnerabilities and detect unusual system activity or service requests.	No Exceptions Noted.
CC7.2.4	Operations and security personnel follow a ticketing system for recording, tracking resolving and escalating reported issues.	No Exceptions Noted.
Control Criteria 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.		
CC7.3.1	The defined Incident Management process addresses: i) Identification of incidents/ events ii) Roles and responsibilities iii) Communication strategies in the event of a compromise	No Exceptions Noted.

	iv) Performing root cause analysis of the incident v) Temporary fix and corrective action	
Control Criteria 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.		
CC7.4.1	The entity has defined an incident response plan in-line with its defined incident management process to understand, contain, remediate, and communicate security incidents, as appropriate.	No Exceptions Noted.
CC7.4.2	Resolution of security events is reviewed at operations and security group meetings held periodically.	No Exceptions Noted.
CC7.4.3	Entity process includes probation, suspension, and termination as potential sanctions for workforce misconduct including but not limited to violation of data security, availability, confidentiality.	No Exceptions Noted.
Control Criteria 7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The entity has defined an incident response plan in-line with its defined incident management process to understand, contain, remediate, and communicate security incidents, as appropriate.	No Exceptions Noted.
CC7.5.2	For high severity incidents, a root cause analysis is conducted. Based on identified deficiency, change requests are initiated in-line with the Company's risk appetite for problem resolution.	No Exceptions Noted.
CC7.5.3	For critical deficiencies, an emergency change management process is also documented.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Change Management		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 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.		
CC8.1.1	A formalized process exists for managing infrastructure changes and updates/ patches.	No Exceptions Noted.

CC8.1.2	System and application change requests are recorded and tracked through a ticketing system. Changes must be reviewed and approved by authorized stakeholders.	No Exceptions Noted.
CC8.1.3	System changes, other than those classified as minor/ cosmetic, require the approval of the authorized stakeholder prior to implementation.	No Exceptions Noted.
CC8.1.4	Changes having an impact on the systems' security, confidentiality, availability, integrity is evaluated as part of the change management process.	No Exceptions Noted.
CC8.1.5	Changes having an impact on the systems' security, confidentiality, availability, integrity are identified and assessed communicated to relevant internal and external stakeholders in a timely manner.	No Exceptions Noted.
CC8.1.6	Changes are developed and tested in accordance with the change management process document.	No Exceptions Noted.
CC8.1.9	For critical deficiencies, an emergency change management process is also documented.	No Exceptions Noted.
CC8.1.10	For high severity incident ticket, a root cause analysis is conducted. Basedon identified deficiency, change requests are initiated which follow the change management process.	No Exceptions Noted.

Trust Service Category: Security		
Domain - Risk Mitigation		
Ref. Nos.	Entity Controls	Exceptions
Control Criteria 9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	No Exceptions Noted.
CC9.1.2	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No Exceptions Noted.
CC9.1.3	During the risk assessment and management process, risk management personnel identify requirements, internal operations, changes to business objectives and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, management updates its processes, and controls, as needed.	No Exceptions Noted.
Control Criteria 9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Third parties and vendors are subjected to a periodic review as part of the vendor management process. Critical vendors are identified and askedto fill out the vendor questionnaires. Response to the vendor questionnaires is evaluated by the Quality team.	No Exceptions Noted.

Trust Service Category: Availability		
Domain - Additional Criteria for Availability		
Ref. Nos.	Entity Controls	Exceptions
Additional Availability Criteria 1.1 - 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.		
A1.1.1	For applications deployed on the cloud, processing capacity is monitored on an ongoing basis in accordance with SLAs and issues resolutions.	No Exceptions Noted.
A1.1.2	The use of resources is monitored, and projections are made for future capacity requirements to ensure required system performance.	No Exceptions Noted.
Additional Availability Criteria 1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	Physical and environmental security measures such as CCTV, fire extinguisher, fire alarm, smoke detectors, biometric or RFID card access systems, UPS, and sprinklers are implemented.	No Exceptions Noted.
A1.2.2	Environmental protection mechanisms are serviced on a periodic basis.	No Exceptions Noted.
A1.2.3	Fire drills are carried out on an annual basis and records are maintained.	No Exceptions Noted.
A1.2.4	Backups including application source code and database are taken and retained as per defined schedule. Failed backups are reinitiated.	No Exceptions Noted.
A1.2.5	Recovery testing of randomly selected samples of the backup is conducted on an annual basis. Results of recovery testing are recorded and maintained.	No Exceptions Noted.
Additional Availability Criteria 1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	Business continuity and disaster recovery plans, including restoration of backups and emergency notification, have been developed. These are reviewed and tested annually.	No Exceptions Noted.
A1.3.2	Disaster recovery services for cloud-hosted application is provisioned on explicit customer request and subscription basis only.	No Exceptions Noted.

END OF THE REPORT

THANK YOU