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

Description of *“Entigrity Pvt Ltd.”*
relevant to Security, Availability, Processing Integrity Privacy and Confidentiality
As of May 11th, 2023

(SSAE 18 – SOC 2 Type II Report)

Section I

Assertion of Entigrity PVT. LTD.

Kratikal Tech Pvt. Ltd.
B-70, Second Floor, Sector 67, Noida, Uttar Pradesh 201301

We have prepared the accompanying description of *Entigrity Private Limited* system titled "Description of Development & Managed Service Activities as of May 11th 2023. 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).

In connection with your engagement to report on Entigrity Private Limited for provisioning offshore staffing throughout the period of May 20th 2022 to May 21st 2023 and the suitability of the design of controls and operating effectiveness to achieve the related control objectives stated in the Description, we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion on whether the Description fairly presents the system that was designed and implemented throughout the specified period and whether the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the specified period to achieve those control objectives, based on the criteria described in our assertion.

We confirm, to the best of our knowledge and belief. as of the date of your report, the following representations made to you during your examination.

1. We acknowledge our responsibility and reaffirm our assertion included in the Description.
2. We have provided you with all relevant information and access to all information such as records and documentation, including service level agreements. of which the service organization is aware and that is relevant to the Description and our assertion.
3. We have responded fully to all inquiries made to us by you during the examination.
4. We have disclosed to you any of the following of which we are aware:

   A. Instances of noncompliance with laws and regulations or uncorrected errors attributable to the service organization's management or employees that may affect one or more user entities.

B. Knowledge of any actual, suspected. or alleged intentional acts by the service organizations management or employees that could adversely affect presentation of the Description, or the completeness or achievement of the control objectives stated in the Description.

C. Design deficiencies in controls

D. Any events subsequent to the period covered by the Description of its system up to the date of your report that could have a significant effect on our assertion.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion on the fairness of the presentation of the Description and on the suitability of the design of the controls and operating effectiveness to achieve the related control objectives stated in the Description, based on your examination, and that your procedures were limited to those that you considered necessary for that purpose.

To the best of our knowledge and belief, no changes Entigrity Private Limited controls that are likely to be relevant to user entities or other factors that might significantly affect those controls have occurred subsequent to audit and through the date of this letter.

Best regards,

For Entigrity Private Limited

S · A · Parikh

Authorized Signature

KRATIKAL
SECURE FOR SURE

Section II

Independent Service Auditor's Report

To,

The Founder & CEO

Mr. Shalin Parikh

Entigrity Pvt Ltd.

We have examined Entigrity Pvt Ltd accompanying description in ***Section III*** titled " ***Offshore Accounting Solution "*** from the period 10th may 2022 to 11th may 2023 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 from the period 10th may 2022 to 11th may 2023 to provide reasonable assurance that Entigrity Pvt Ltd service commitments and system requirements were achieved based on the trust services criteria relevant to ***Security, Availability, Processing Integrity, Confidentiality, and Privacy*** set forth in **TSP Section 100, 2017** *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* .

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 organization's 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 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 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 complementary user entity controls assumed in the design of Entigrity Pvt Ltd 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 Pvt Ltd*"** that is not covered by this Auditor's Report, is presented by Entigrity Pvt Ltd management to provide additional information and is not a part of Entigrity Pvt Ltd description. Information about Entigrity Pvt Ltd 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 Pvt Ltd 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 Pvt Ltd 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 Pvt Ltd service commitments and system requirements were achieved. In ***Section II***,

Entigrity Pvt Ltd has provided its assertion titled ***"Assertion of*** **Entigrity Pvt Ltd*"*** about the description and the suitability of design and operating effectiveness of controls stated therein. Entigrity Pvt Ltd 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.

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.

Opinion

In our opinion, in all material respects,

a. the description presents Entigrity Pvt Ltd **"*Description of*** Entigrity Pvt Ltd ***Customer Application"*** that was designed and implemented from the period 10th may 2022 to 11th may 2023 in accordance with the description criteria.
b. the controls stated in the description were suitably designed from the period 10th may 2022 to 11th may 2023 to provide reasonable assurance that Entigrity Pvt Ltd 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 Pvt Ltd controls throughout that period.

the controls stated in the description operated effectively from the 10th may 2022 to 11th may 2023 and provide reasonable assurance that Entigrity Pvt Ltd 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 Pvt Ltd 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 Pvt Ltd user entities of Entigrity Pvt Ltd **"** ***Description of*** **Entigrity Pvt Ltd** ***Customer Application"*** business partners of Entigrity Pvt Ltd that were subject to risks arising from interactions with the Entigrity Pvt Ltd **"*Description of Entigrity Pvt Ltd Customer Application"***, 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.

CPA Name: - Mr. Jay Maru

License No. 41401

6th October, 2023

Mumbai, India.

Jay
Dhiraj
Maru

Digitally signed
by Jay Dhiraj
Maru
Date:
2023.11.28
18:35:31 -05'00'

entigrity

Section III

Description of the Entigrity Pvt Ltd.

“*Offshore Accounting Solution*”

As of May 11th, 2023

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.

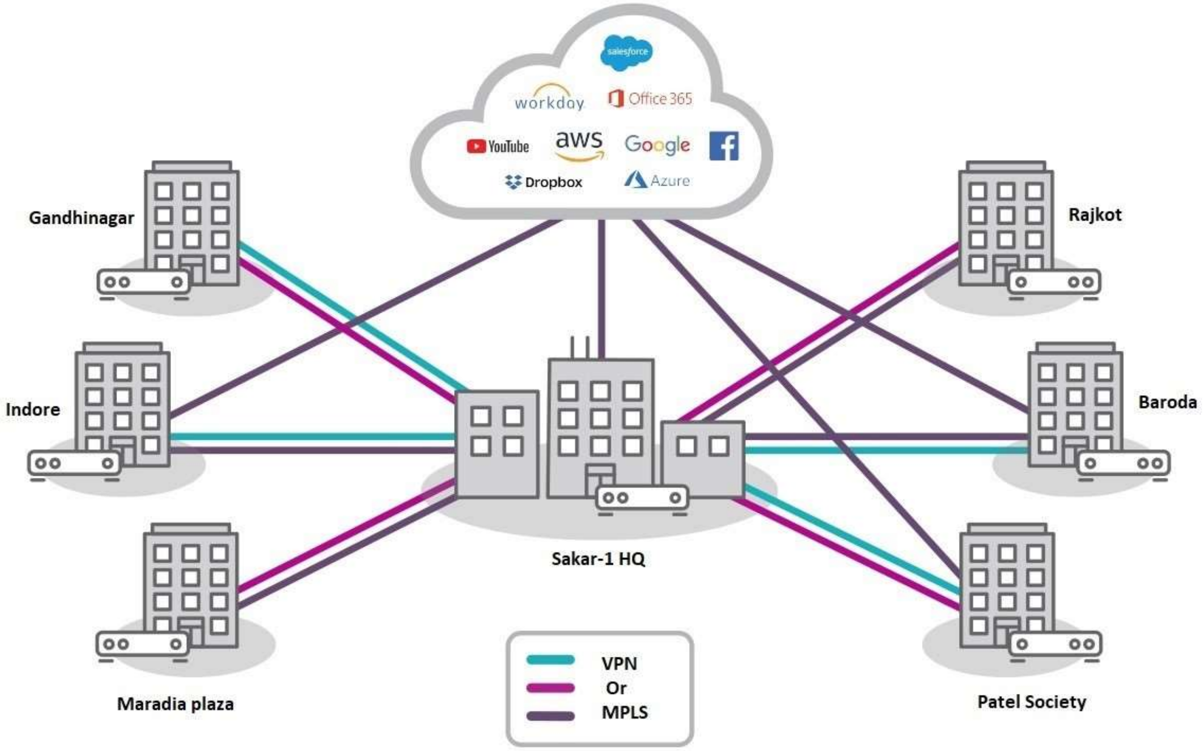
E.1.1. Network Segmentation Overview

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

Connectivity architecture Entigrity PVT LTD



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 are 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 are 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 Centre, 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 analyse 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.

entigrity

Section IV

Description of Criteria, Entigrity Pvt Ltd.

“Offshore Accounting Solution”

As of May 11th, 2023

Controls Implemented by Entity	**Control Description**	**Test results**	**Exceptions**
Changes to system boundaries	Changes to system boundaries, network systems are communicated to clients, if it impacts their operations	Enquired with CISO whether changes to system boundaries were affected, but there are no changes in this period.	No exception noted.
Reporting of incidents to external users	Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	Selected a sample of incident reporting emails to clients / external users to determine that major incidents are reported to clients along with root cause.	No exceptions noted
Risk Assessment	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Examined risk assessment statement and risk register.	No exceptions noted
Patch Management	A patch management script is run periodically to automatically update user systems.	Inspected screenshot of patch management script to determine that patches are applied periodically, Patch report is also submitted.	No exception noted

Asset Register	List of all hardware is maintained as part of asset register.	Inspected the asset register / hardware list to determine that all assets are recorded.	No exception noted
Risk Management Policy	Company has defined a formal risk management process for evaluating risks based on identified vulnerabilities, threats, asset value and mitigating controls.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No exception noted
Vendor Onboarding process	Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate senior management during the procurement process.	Selected a sample of vendor agreements and inspected the security and confidentiality commitments to determine that these are included and part of the procurement /vendor onboarding process.	No exception noted
System Access reviews	IT system access is reviewed on a monthly basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected a sample of system access review reports to determine that access rights are reviewed regularly and user access lists are reconciled against active HR records.	No exception noted

VAPT	Results of the vulnerabilities are reviewed by the management	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No exception noted
Access Management Policy	Company has documented procedure for logical access controls	Inspected the access control policy and procedure and determined that these are documented.	No exception noted
Access Management Least Privileges	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No exception noted
Hardening standards	Company has established hardening standards production infrastructure that include requirements for implementation of security groups, access control, configuration settings, and standardized policies.	Inspected IT policies and procedures and SOP for system hardening used.	No exception noted.

Cloud Infra - Firewalls	Production hosts and Security Groups (which are the equivalent of Firewalls) are hardened according to Industry best practices. Only the required ports are opened for inbound access at the load balancer level.	Inspected AWS settings to determine that VPC has been setup and all production server are within the private subnet. Inspected the IAM settings and security groups to determine that only the production group has access to production resources.	No exception noted.
Network diagrams	Physical and logical diagrams of networking devices for office network include routers, firewalls, switches and servers, including wireless, are documented.	Inspected the system diagrams and networking diagrams to determined that these are documented.	No exception noted
VAPT	3rd party vulnerability scans are performed at least annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent VA reports from external agency to determine that VA are carried out and that these are discussed in management meetings.	No exception noted

VPN connection to client environment	Users access Client system only after logging into company network followed by connecting into client network using encrypted channels such as VPN, Citrix Clients decide on the type and level of encryption as per their policies.	Enquired with IT staff about use of VPNs relating to encryption and authentication of users to client systems	No exception noted
No access to external users	Company does not allow customers or external users to access its systems.	Enquired with IT team that external users cannot access company's network systems	No exception noted.
Active Directory	Infrastructure components and software are configured to use the Windows security using group policies & active directory.	Inspected the screens for Active Directory and Group policies to determine that authentication is through Active Directory. Observed a user sign-on process to determine if an ID and password were required to verify identity.	No exception noted
Creating client user accounts on cloud application	Client user's access to Entity applications hosted on AWS is granted during the onboarding process. User credentials for client employees is setup by Entity's IT team against a request from the client.	Inspected a sample of client requests for user setup within application to determine that users are created by entity only against authorised client request.	No exception noted.

Internal user access to cloud applications	Access to application instances hosted for the clients is restricted to IT support team and select client project team members who need access. IT Support team have admin rights and can add additional Entity's users on the client instances as per business requirements.	Selected a sample of clients and inspected the user list for application instance for those clients to determine that only IT team and select client project teams have access to client's production instances.	No exception noted.
User-id for non-AD accounts	Systems not using the shared sign-on functionality are required to be implemented with separate user ID and password submission.	Enquired with IT Head that all accounts are AD accounts	No exception noted
IAM on AWS/GCP	Cloud infrastructure is configured to use the AWS's identity and access management system (IAM). Relevant groups have been added in IAM.	Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources.	No exception noted.

SSH Access for cloud	Direct access to cloud infrastructure is possible only through encrypted SSH access by the IT team.	Inspected the properties of VPC security group and determined that the inbound connection to instances in the VPC is set to be accessed by a SSH connection. Inspected SSH settings in SSH client to determine that encrypted SSH key is required for connecting to AWS / Cloud infrastructure.	Not applicable
AWS MFA	For AWS console access, Multi Factor Authentication is implemented.	Inspected the user settings in AWS console for the production group members to determine that multifactor authentication has been enabled.	No exception noted.
Remote working policy	The Company has a remote working policy that requires that external access is granted on a need basis.	Enquired with IT staff about external access by employees and determined that external access is given to employees, the remote access policy has been amended	No exception noted.

Asset Register	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.	Inspected the asset register and determined that assets and their owners are clearly documented.	No exception noted.
Sensitive Areas - Privileged access	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.	Inspected screenshots of Active Directory to determine that administrator privileges for the domain were limited to IT team. Selected a sample of requests for privileged access and inspected the authorization email to determine that it is authorized by COO.	No exception noted.
Active Directory	Entity systems are configured to use the active directory.	Determined through enquiry with IT staff that all resources use active directory.	No exception noted.

No Active Directory for small firms	Company does not have office network / Active Directory etc. All user machines are independently monitored by the IT team on a periodic basis. Local Group policies require authentication on user machines through a password policy.	Enquired with Head IT that the company does not have Active Directory. Inspected the periodic monitoring records for a sample month / quarter to determine that IT team monitors the user devices on a periodic basis.	No exception noted.
Account sharing prohibited	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing.	No exception noted
Client network Access	Access to client network is governed by the Client according to their policies.	Enquired with IT staff about access to client networks and determined that IT has no control over client's network.	No exception noted
Access through VPN to Client network	Users access Client system only through an encrypted channels or VPN. Clients decide on the type and level of encryption as per their policies.	Enquired with IT staff about encryption and authentication of users to client systems	No exception noted

VPN, SSL or another encryption.	External users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.	Enquired with CISO about the authentication via user organization VPN. Inspected firewall configuration screens showing the list of whitelisted IP addresses.	No exception noted.
Password policy in AD	The following password parameters are in place for active directory: 1. length of 8-character length 2. alphanumeric, special character and upper-case lower case 3. password expires in 90 days 4. Password history is set at 3	Examined password controls and walkthrough of active directory to check live users.	No exceptions noted
Password policy - NO AD. local desktop	Password policy is set at the Local Policy level. Passwords are manually set on each user desktops by the IT team. These are 7 characters in length with complexity enabled. Passwords are reset by the IT team manually every 45-60 days by going to each user desktop and resetting the passwords. On next	Enquired with IT Head that passwords are manually set by the IT team and are reset every 45-60 days by the IT team.	No exception noted

	login, the user in the presence of IT team, will reset the password.		
Domain Controller / AD	Access to data is restricted to authorized applications through domain policies through Active directory. Access to Company systems is given only against authorization. Access given to new employees is one of least privileges.	Inspected group policy of the domain and determined that access requires a combination of user ID and unique password.	No exception noted.
Work in client environment only	All work is carried on the client systems and access to client systems is managed by the client.	Observed that users' connections to client systems require additional login to client system	No exception noted.
Secure VPN connecting to client environment	Access to client application on client networks is through Citrix sessions or remote desktop using SSL/VPN connections. Clients decide on the type and level of encryption as per their policies.	Enquired with IT staff about the encryption and authentication of connections to client applications and determined that it is as per Client's requirements.	No exception noted
Whitelisted IPs	External access is through firewall appliance that allows only the white listed IP addresses.	Inspected firewall console and determined that incoming connections are	No exception noted

		from whitelisted IPs only.	
Email to client for new joiner	Company sends emails to clients regarding access request for new user on client projects.	Inspected a sample of emails to clients requesting for access for users.	No exception noted
No printer access	Employees do not have access to printers or any other output device. Printer access is given for few teams such as HR.	Enquired with IT team that no printer access is given to employees and determined based on enquiry that output access is controlled.	No exception noted
Data Classification policy	All confidential data is classified as per the data classification policy	Inspected information security policies to determine that data classification policies are documented.	No exception noted
Access revocation	Access on client systems is removed by sending an email to the client manager informing them about the exiting employee.	Inspected access revocation requests sent to clients to determine that clients are informed of user exits.	No exception noted

Exit Formalities	When an employee leaves the organization, the employee’s manager initiates the 'Exit Process'. HR informs respective teams / IT team within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures.	Selected a sample of exited users and inspected Email from HR to IT and Exit Checklist to determine that the exit process and related account deactivation is as per defined procedures. Inspected the domain screens to determine that the exited user has disabled status in AD server.	No exception noted
User deactivation email	HR team sends the user deactivation list to IT team within 24 hours from the time an employee is terminated or the last working day.	Inspected access revocation mail from HR to IT for sample off-boarded employees &amp; verified their disabled status in AD server.	No exception noted
Sensitive Areas - Privileged access	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.	Inspected screenshots of Active Directory to determine that administrator privileges for the domain were limited to IT team.	No exception noted

No access to non-employees	Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees.	No exception noted
No Domain Controller	Currently, the company does not have any office domain/network. All users are considered external users and access AWS directly.	The process of bringing the entire company network under one AD for better security is on. Intermittent solution is that some limited users are in domain controller and others users outside the controller are under workgroup and they are controlled by IT ops	No exception noted.
Role based access	A role-based security process is setup in Active directory with groups and roles based on job requirements.	Inspected the security groups in the domain and determined that security groups based on departments and roles have been defined	No exception noted
Role based Access - Cloud	A role-based security process has been defined within AWS infrastructure based on job requirements.	Inspected the AWS console screens to determine that security groups based on departments and roles have been defined	No exception noted.
Reactivation prohibited	Company does not allow reactivation of ID belonging to an exited employee.	Inspected IT policy about reactivation of IDs and determined that it is prohibited.	No exception noted

Sensitive areas Physical access Review periodically	A periodic review of physical access to sensitive areas against active employee list is carried out by IT.	Inspected a sample of access review reports for sensitive areas to determine that access rights are reviewed regularly.	No exception noted
Physical access review periodically	On a quarterly basis, Internal audit / HR performs a reconciliation that physical access for terminated employees has in fact been deactivated in the physical access system.	Selected a sample of quarters and inspected physical access reviews to determine that physical access reviews / reconciliations are performed periodically.	No exception noted
Media Handling policy	Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment	Inspected the media handling policy to determine that it is documented.	No exception noted
Media disposal	All data is erased from laptops and other media prior to destruction disposal	Inspected the media handling policy to determine that for all media that is disposed of, data is erased from these prior to disposal.	No exception noted
Firewall installation	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	Observed that firewall device has been installed in the office network. Inspected firewall console screens containing rules about ports, incoming connection types, whitelisted IPs and type of traffic and	No exception noted

	bound traffic filtering.	determined that configuration is in compliance with the policy and incoming connection are allowed only from whitelisted IPs.	
AWS Firewall	The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all Production system hosted at AWS. Only limited employees in the production group have access to production servers using SSH through a NAT gateway.	Inspected AWS settings to determine that VPC has been setup and direct access to production instances is only through 2048-bit SSH keys.	No exception noted.
Splunk for application logs	Splunk is used to collect application logs and send alerts based on threats assessments. All application logs are aggregated in the Splunk centralized logging server.	Splunk is used for collecting application logs. Carried out a walkthrough to confirm.	No exception noted
Whitelisted incoming traffic	Incoming connection are accepted from only whitelisted IPs in the firewall.	Inspected incoming connection configuration in the firewall and determined that whitelisted IPs are used to manage connections.	No exception noted

Content Filtering	Company has implemented content filtering system through firewall that blocks access to certain sites such as personal emails, storage etc.	Inspected firewall setting for content filtering to determine that content filtering is applied.	No exception noted
Firewall admin access	Access to modify firewall rules is restricted by management.	Inspected the user list on firewall application to determine that access to modify firewall rules is restricted to Administrators/IT team.	No exception noted
No data outside production for DR	There is no data stored outside production systems for any DR test.	Enquired with management about data stored outside its environment to determine that there is no data stored outside of production systems for any DR test.	No exceptions noted
No printer access	No confidential output is printed internally in the office. No customer confidential data resides in office premises.	Enquired with IT Staff about customer confidential information and determined that no customer information resides in office network.	No exception noted
Active Directory	Logical access to Company systems is restricted through active directory-based domain policies.	Inspected the access control policy for access control procedures and requirements of configurations	No exception noted.

Data Encryption	Data is stored in encrypted format using software supporting the AES.	Inspected evidence of encryption of data storage.	No exception noted
Removable media prohibited	Use of removable media is prohibited by policy except when authorized by management.	Inspected domain policies for removable media. Observed a sample of computers and determined that USB sticks are not read.	No exception noted
Secure VPN connecting to client environment	Access to client application on client networks is through Citrix sessions or remote desktop using SSL/VPN connections. Clients decide on the type and level of encryption as per their policies.	Enquired with IT staff about the encryption and authentication of connections to client applications and determined that it is as per Client's requirements.	No exception noted.
Encryption Policy	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies to determine that transmission of sensitive information over the internet happens only when the information is encrypted.	No exception noted

Encrypted VPN connections	VPN connections to both the corporate and cloud networks are encrypted.	Inspected the VPN connection settings to determine encryption is enabled.	No exception noted.
Access through VPN to client network	Access to client is through client VPN	Enquired with IT staff about encryption and authentication of users to client systems	No exception noted
Cloud Infra firewall.	The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all Production system hosted at AWS. database access is governed by security group policies and login credentials. Production database can only be accessed from production machines.	Inspected AWS settings to determine that VPC has been setup for xxx application & database, all production xxx servers (ih2 and nine) are within the private subnet and direct access to EC2 instances is only through 2048-bit SSH keys.	No exception noted.
Removable media prohibited	Use of removable media is prohibited by policy except when authorized by management	Inspected domain policies for USB drive. Observed a sample of computers and determined that USB sticks are not read	No exception noted

Laptop encryption	Storage for workstations and laptops is encrypted. Protects data at rest.	Enquired with Head IT that all storage for workstations and laptops is encrypted. Windows BitLocker is used	No exception noted
Backup media encryption	No media transfer of backups it is through google drive	Enquired with Head IT that all backup media are encrypted during creation	No exception noted
Antivirus installed	Automated backup systems are configured to send alert notifications to IT personnel regarding backup completion status	Inspected a sample of desktops and servers and determined that antivirus is installed and signature files were updated. Inspected the antivirus/firewall console for configuration details about updating and alerts.	No exception noted
Regular update of AV definitions	Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines.	Inspected a query report from the console showing not updated computers and determined that there were no such cases. Inspected the antivirus/firewall console for configuration details about updating and alerts.	No exception noted

Local admin access	The ability to install software on workstations and laptops is restricted to IT support personnel through domain policies. Local admin access is granted on a need-based approval from CEO.	Inspected the Information Security Policies to determine that users are not allowed to install any software. Inspected domain policies for local admin and determined that is it disabled for local users.	No exception noted
Reporting of virus detected	Any viruses discovered are reported to IT team either by the antivirus system or by the affected employees.	Inspected the antivirus/firewall console for configuration details about updating and alerts. Inspected the security training pack for the instructions to employee about virus incidence reporting.	No exception noted
Configuration standards	Management has defined configuration standards and hardening standards.	Inspected IT policies and procedures to determine that hardening standards have been established.	No exception noted

Monitor infrastructure and software	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Inspected monthly reports from IT department that summarise non compliances with standards to determine that Infrastructure and software non compliances are tracked and reported	No exception noted
Penetration Testing	Penetration testing is performed by on a periodic basis	Inspected the latest penetration testing report to determine that periodic penetration tests are carried out.	No exception noted.
VAPT	Technical vulnerability management is implemented using the Nessus vulnerability scanner. Critical threats are reviewed and resolved timely.	Inspected a sample of VA scans to determine that the scans were executed. Inspected relevant evidence and management meeting minutes to determine that vulnerabilities were tracked and closed.	No exception noted.
Alerts from firewall for suspicious activity	The firewall protecting the corporate network notifies the IT team of suspicious activity. Alerts are responded to promptly.	Inspected evidence of the alert settings for the firewalls in place to determine IT team is notified.	No exception noted

IT Help desk support	IT team receive requests for support through phones and emails, which may include requests to reset user passwords etc.	Inspected a sample of IT support ticket emails reported by users to determine that support tickets are logged as emails.	No exception noted
Incident Management Policy	A formal, defined incident management process is documented in Information Security Policies for evaluating reported events.	Inspected ISMS / Information Security Policies to determine that incident management process is documented.	No exception noted
Incident Tracker	Incidents are reported to the IT team. These are tracked through an incident management tool.	Inspected the screenshot of the incident management tool to determine that incidents are tracked.	No exception noted
Incident ticket details captured	Reported incidents are logged as tickets and include the following details Severity Data and Time of incident Details Status Root Cause (High severity incidents only)	Inspected a sample of incident report to determine that incidents covered severity, date, time, details, status and root cause (if major) to determine that incidents are handled as per defined process.	No exception noted
Review of incidents in committee meetings	All security incidents are also reviewed and monitored by the Steering Committee. Corrective and preventive actions	Inspected minutes of Steering committee for discussion on incidents.	No exception noted

	are completed for incidents.		
Change Management for repeated incidents	Change management requests are opened for events that require permanent fixes.	Inspected Incident Management Procedure and determined that for some incidents, change requests are opened as part of resolution.	No exception noted
Incident management plan	Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Inspected ISMS / Information Security Policies to determine that incident management process is documented.	No exception noted
Privacy breach reported to CISO	Unauthorised access or disclosure of personal data is reported to senior management and CISO.	Inspected a sample of emails to senior management to determine that privacy data breach is reported to Senior Management	No exception noted
Code of conduct	HR policies include code of conduct and disciplinary policy for employee misconduct.	Inspected the Employee Handbook for Code of Conduct and Disciplinary Policy	No exception noted
RCA for incidents	Root cause analysis is performed for major incidents.	Inspected a sample of incident reports to determine that root cause analysis is performed for critical / major incidents.	No exception noted

Change management policy	Entity has defined its change management and approval processes in its information security policies.	Inspected Information Security Policy and determined that change management policy and procedures are defined.	No exception policy
SDLC Policy	Software design and development change procedures are documented in the SDLC Process.	Inspected the SDLC procedures to determine that software design and development change procedures are documented.	No exception noted
Change request tracker	All change requests are logged and change request ticket created. Major changes are approved by DDD	Selected a sample of change requests to determine that these are logged and that major changes are approved by DDD.	No exception noted
No Software development	The company does not use any applications for the client's processes / system in scope and hence there is no software development and related change management for applications.	Enquired with IT Head that no applications are used within the client process.	No exception noted
Development Peer review	All change requests must be peer reviewed by another programmer for consistency purposes.	Enquired with management to determine that informal code review is performed by a peer programmer.	No exception noted

Static code analysis	Security vulnerability scans on developed source and object code libraries using Static Code Analysis tools.	Inspected the static code analysis tool and reports to determine that continuous code analysis is part of the development process and covers code's reliability, security, maintainability, duplications.	No exception noted
Regression Testing	System and regression testing is prepared by the testing department using approved test plans and test data.	Inspected test plans for sample of releases to determine that test plans included steps for regression testing, security testing	No exception noted
Software code on GIT/SVN	Software code is maintained in SVN/GIT.	Inspected screenshot of SVN server to determine that software code is maintained in SVN /GIT	No exception noted
QA testing / UAT testing	Software development changes are tested through unit testing and QA testing followed by UAT. Each of these activities are captured &amp; monitored in change requests. Test plans used for testing QA team.	Inspected a sample of change requests for software development to determine that QA/UAT testing is carried out.	No exception noted

Release plan / UAT testing	There is a formal release process for releasing builds. Release notes contain what all is released in the release. The testing team does the complete testing of the release. On receipt of sign off mail from the testing team the release is deployed on production servers.	Selected a sample of releases during the audit period and inspected the release notes and the related approval to determine that all releases are tested and approved before deployment	No exception noted
Separate environment for changes	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.	Enquired with the management to determine that separate environments are maintained for development, testing and production and also to understand about process to carry out major changes.	No exception noted
Rollback plans	All change requests are submitted with implementation and rollback plans. Code repository &amp; deploy tool has a turnover process that includes back out steps commit is to be reverted.	Inspected a sample of change requests to determine that they had rollback plans included.	No exception noted

Communication of changes	Changes are communicated to the appropriate client and user community if the change has any potential impact on the user base.	Enquired with management that changes are communicated to clients and end users if it has impact on those users.	No exception noted
Segregation of Roles in change management	The change management process has defined roles and assignments thereby providing segregation of roles in the change management process.	Inspected the Change Management Policy and Procedures to determine that these define segregation of roles for change management.	No exception noted
Risk Assessment considers changes	A risk assessment is performed on a periodic basis. The risk assessment includes identifying potential threats and assessing the risks associated with identified. Change requests are created based on the identified needs.	Inspected the risk management procedures to determine if change requests are created based on identified needs.	No exception noted
High Severity incidents require changes	For high severity incidents, change requests are created.	Inspected Incident Management Procedure and determined that for some incidents, change requests are opened as part of resolution.	No exception noted

Emergency Changes	A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review.	Inspected Change Management policy to determine that the policy considers process to manage emergency changes	No exception noted
Testing data is masked	Data for testing is obfuscated before being used in testing.	Enquired with management that SQL scripts are used to obfuscate test data and no actual data is used in testing	No exception noted
Production data in non-production env.	Data owners approve any storage or use of production information in non-production environments.	Enquired with management that any storage of data outside of production environment is approved.	No exception noted
Processing Capacity monitoring	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements Processing capacity is monitored by tools such as PRTG, Nagios on an ongoing basis.	Inspected a sample of capacity monitoring reports to verify that the capacity demand is documented and reviewed by management. Inspected PRTG/Nagios report to determine that tool monitors and reports on uptime, outage and response time.	No exception noted

AWS processing capacity - CloudWatch	Processing capacity for cloud infrastructure for AWS is monitored by AWS CloudWatch on an ongoing basis.	Inspected CloudWatch settings to determine that alerts & thresholds have been setup for abnormal conditions such as low CPA utilization, network out, free storage etc.	No exception noted.
Redundancy	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inspected redundancy measures for firewall and determined that there is a backup firewall in a high availability configuration	No exception noted
Backup policy	Backup policy is defined in the information security policies	Inspected information security policies to determine that backup schedules, frequency of backups are documented.	No exception noted
Automated backup scripts	Automated backup systems are in place to perform scheduled differential and full back up of production systems and internal office data.	Inspected screenshots of the backup systems to determine that backups are scheduled to be taken on a regular basis.	No exception noted
Local office backup	Backups are performed on external hard drives or tapes on finance data.	Enquired with IT Head that backups are performed on external hard drives/tapes	No exception noted

Alerts for failed backup	Automated backup systems are configured to send alert notifications to IT personnel regarding backup completion status.	Inspected a sample of automated alerts for backup to determine that these are configured in the backup systems	No exception noted
No backup on external drives	No backups are performed on external hard drives or tapes.	Enquired with IT Head that no backups are performed on external hard drives/tapes	No exception noted

entigrity

Section V

Other Information Provided by Entigrity Pvt Ltd.

“Offshore Accounting Solution”

As of May 11th, 2023

Entigrity Pvt Ltd offers the data in this part only for informational purposes. There have been no audit processes carried out regarding this part by the Independent Auditor.

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.

END OF THE REPORT