Cyfuture India Pvt. Ltd.

Independent Service Auditors' Report on Management's Description of

Providing Data Centre Services including Web Site Hosting, Web Application Hosting, Server co-location, Disaster Recovery, Backup, email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services

Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of Controls

For the period, April 01, 2019 to September 30, 2019

(SSAE 18 - SOC 1, 2 & 3 Type 2 Report)

Prepared by: Manoj Jain

www.riskpro.in

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Cyfuture India Pvt. Ltd. (Cyfuture)

Scope

We have examined the attached Cyfuture India Pvt. Ltd.'s (Cyfuture) description of its system titled "**Providing Data Centre Services including Web Site Hosting, Web Application Hosting, Server co-location, Disaster Recovery, Backup, email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services"** throughout the period April 01, 2019 to September 30, 2019 included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period April 01, 2019 to September 30, 2019 to provide reasonable assurance that Cyfuture's service commitments and system requirements would be achieved based on the trust service criteria for security, availability and confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security *Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria). Cyfuture has determined that Processing Integrity and Privacy Trust Services Principles are not applicable to the services provided to its client and are not included in the description.

The information included in Section 5, "Other Information Provided by Cyfuture" is presented by management of Cyfuture to provide additional information and is not a part of Cyfuture's description of its system made available to user entities during the period April 01, 2019 to September 30, 2019. Information about Cyfuture's business continuity planning etc. has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Cyfuture's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls

Cyfuture does not use any subservice organisations.

Service Organization's Responsibilities

Cyfuture 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 the service commitments and system requirements were achieved.

Cyfuture has provided the accompanying assertion titled, Management of Cyfuture's Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. Cyfuture is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in Cyfuture's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period April 01, 2019 to September 30, 2019.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

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. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in Cyfuture's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period April 01, 2019 to September 30, 2019.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period April 01, 2019 to September 30, 2019, and the subservice organization and user entities applied the controls contemplated in the design of Cyfuture's controls throughout the period April 01, 2019 to September 30, 2019.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period April 01, 2019 to September 30, 2019, and user entities and subservice organization applied the controls contemplated in the design of Cyfuture's controls, and those controls operated effectively throughout the period April 01, 2019 to September 30, 2019.

Description of Test of Controls

The specific controls we tested and the nature, timing, and results of our tests are presented in the section 4 of our report titled "**Independent Service Auditors' Description of Test of Controls and Results"**

Restricted Use

This report, including the description of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Cyfuture; user entities of Cyfuture's systems during some or all of the period April 01, 2019 to September 30, 2019; and those prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations or other parties
- Internal control and its limitations
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Manoj Jain, CPA
(Colorado Membership Number - 0023943)

November 01, 2019
Mumbai, India

SECTION 2

MANAGEMENT OF CYFUTURE’S ASSERTION

Management of Cyfuture’s Assertion

xxxx

SECTION 3

DESCRIPTION OF CYFUTURE’S “SYSTEM”

THROUGHOUT THE PERIOD

APRIL 01, 2019 TO SEPTEMBER 30, 2019

Description of Cyfuture's system throughout the period April 1, 2019 to Sep 30, 2019.

Background and Overview of Services

Cyfuture India Pvt. Ltd is a leading provider of enterprise hosting, cloud hosting, website hosting, and application hosting services to global clients across multiple industries. We have an impressive track record of executing and managing large scale IT infrastructure projects for several Fortune 500 firms, government institutions and small & medium enterprises. Our hosting solutions provide our clients the much needed freedom to focus and grow their business while we effectively manage their mission-critical data center infrastructure and maintenance.

Organizational business goals are varied. And, so are our hosting solutions. The only thing constant is our years of expertise and ability to provide customized solutions to each client according to their distinct business needs. Our team of engineers ensure that the data center infrastructure of our clients are up and running with regular system upgrades to ensure maximum security of their data and increased efficiency of their computing systems.

We currently own and operate state-of-the art Tier III data center facilities in Noida and Jaipur (India) which are equipped with cutting-edge hardware and software to deliver best-in-class data center and cloud hosting solutions.

Cyfuture is certified against the requirements of ISO 27001:2013, ISO 9001: 2008 & HIPAA

Significant Changes during the Review Period

None

Subservice Organizations

Cyfuture does not use any subservice organisation.

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 Cyfuture for providing Data Centre activities including Co-Location Services, Security Services, Dedicated Hosting, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services.	
Products and Services NOT in Scope	
The report does not cover the following services. • Cloud Hosting services using CloudOye Application. • Third party Cloud hosting services such as AWS/Azure	
Geographic Locations in Scope	
Noida, India	SDF G-13&14, Noida Special Economic Zone (NSEZ), Noida- 201305, UP.

All the above material activities and operations in scope are performed from the above 01 office location. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report. The data center site at Jaipur, India are specifically excluded from the scope of this report.

Principal Service Commitments and System Requirements

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

Cyfuture establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cyfuture's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, information technology (IT) and other hardware,
- Software including application programs and IT system software that support application programs,
- People including executives, sales and marketing, client services, product support, information processing, software development, IT,
- Procedures (automated and manual), and
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Cyfuture's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Cyfuture's customers are not included within the boundaries of its system.

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

Control Environment

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

Integrity and Ethical Values

Cyfuture 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 fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Cyfuture 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.

Board of Directors

Business activities at Cyfuture are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its promoter director Mr. Ratan Chand Bairathi, Ms. Shilpi Agrawal, Mr. Rajiv Bairathi & Mr. Anuj Bairathi as the CEO. Oversees the company's India operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

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

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimise those risks that are determined to pose an unacceptable level of risk to Cyfuture. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Cyfuture has operationalized 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 Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at Organizational level.
- Risk analysis & evaluation for each asset in a process & at Organizational level.
- Risk treatment & residual risk.

Risk assessment comprises of calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk also to identify the areas where organization needs to focus over information security.

Apart from the asset based risk assessment, Cyfuture has also conducted organization based risk assessment based on internal and external issues and needs and expectations of interested parties

The threats, vulnerabilities associated with every asset and at organizational are evaluated along with threat impact, Probability of occurrence and chances of detection (on a rating basis) of the threat to determine the Risk Factor, which are then put into an equation to derive a risk value; this risk value is then compared to the organizational threshold (i.e., accepted risk value) and treated appropriately (i.e., treat, transfer, avoid, accept).

The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a completed risk register and risk treatment plan. Any action plans will be tracked to completion.

Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Information Security Policies

Cyfuture has developed an organization-wide Information Security Policies. Relevant and important Security Policies (IS Policies) are made available to all employees via shared drive and intranet. Changes to the Information Security Policies are reviewed by IS Team and approved by CEO/CISO prior to implementation.

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. Cyfuture management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Performance monitoring reports cover server parameters such as disc space, incoming/outgoing network traffic, packet loss, CPU utilization etc. These system performance reports are reviewed by management on a periodic basis.

In addition, a self-assessment scan of vulnerabilities is performed using Open Vas tool on yearly basis. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Cyfuture has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to Cyfuture policies and procedures as part of their daily activities.

Cyfuture management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. Manager Service Delivery and Sr. Manager IDC are 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 Cyfuture’s processes to provide timely information to employees regarding daily operating activities and to expedite management’s ability to communicate with Cyfuture employees.

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. Cyfuture uses two factor authentication to access emails.

Components of the System

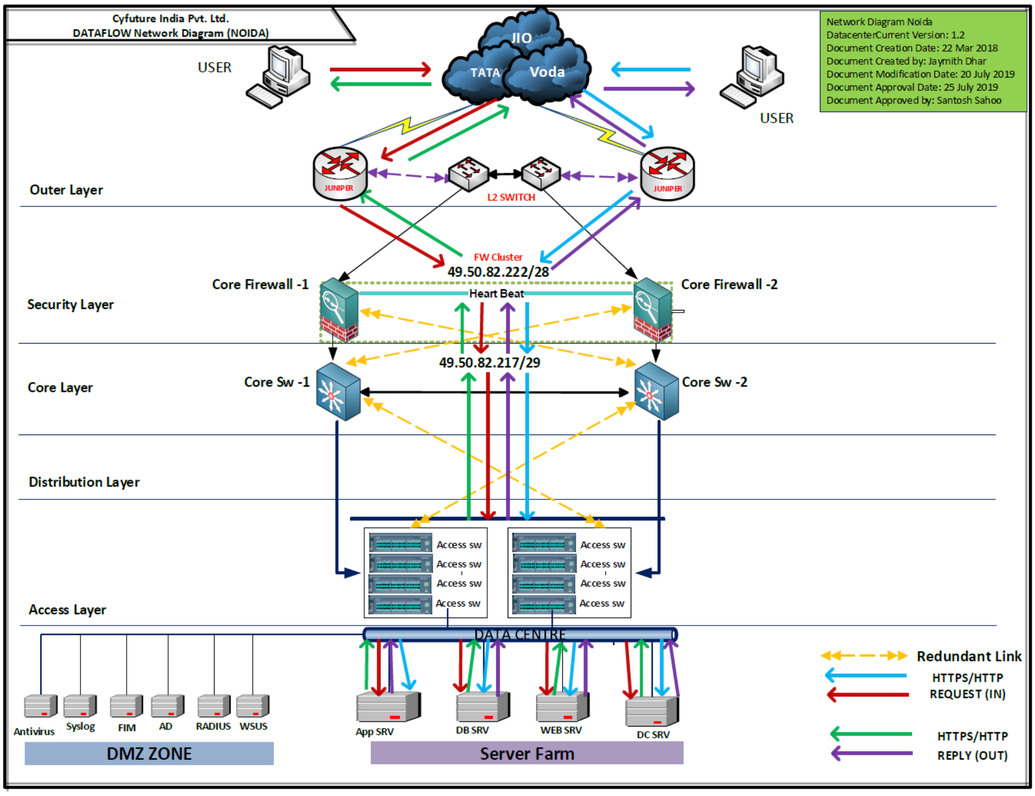
Infrastructure

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

Network Segmentation Overview

Cyfuture’s office is equipped with the latest hardware, software and networking infrastructure. Office is linked using high speed communication links, backed up by redundant networks.

Network Segmentation Diagram



Physical Structure Overview

Cyfuture's Office power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises, UPS units and backup generators supply power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. Generators and UPS are under AMC for preventive maintenance

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked and AMC is entered on completion of Warranty. Periodic fire drills are conducted in coordination with Admin and HR personnel. The fire drills reports are collected and analysis made upon it.

Physical Access

The entrance is secured with a security person, access control and CCTV surveillance. Physical and Environmental Security of Cyfuture is controlled and governed by physical security policies forming part of the Cyfuture IS Policy.

Entry to the Cyfuture offices is restricted to authorized personnel by a biometric access control system. All employees are provided with access cards. These cards open the door lock. Attendance is recorded through biometric system. All visitors have to sign the visitors register and are given inactive visitor card.

Employees are subjected to show their ID cards at the Security entrance and swipe in/thumb print the access management system. Employees are granted access only to those areas which they are required to access. Some members of the IT Support Team & Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to wear their access cards / employee identification cards at all times while within the facility.

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

ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR sends an e mail to IT department requesting the IT team to issue an access card to the new employee. The IT team ensures that the access card/biometric controls configured with the appropriate access rights, and then issues the same to the employee.

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

Security guards control visitor access at all entrance points. Surveillance cameras have been installed at various critical points within & around the facility. Backup of recordings is stored for one month.

Access by visitors, contractors and/or third party support service personnel's both entry and exit are monitored by security personnel. Photography, video, audio or other recording equipment, are not allowed inside secure premises, unless specifically authorized. Such accesses are recorded, authorized and monitored. Visitor, contract and/or third party service personnel to sensitive areas such as data centres are strictly on "need to have" basis and subject to the principle of least privileges, escorted, under video surveillance and supervised. Appropriate displays at the key entry points inform visitors of their responsibilities.

Access to the Server Room

Access to the data center is controlled by an bio metric access control system and access allowed to IT infra team.

Cyfuture policies protect sensitive equipment such as servers, communication and power hubs and controls. Only Authorized personnel are allowed to enter such sensitive areas controlled with separate access cards and biometric systems. Third parties are allowed access to the data center only under the supervision of IT team members and prior information. Visitors are supposed to fill the data center access form.

Software

Firewalls

Fortigate 1500D with High Availability is installed and Configured for the Core Infrastructure in Active/Active Mode, where both the Firewalls being used for the Load Balancing and Fault Tolerance. The Firewalls include Antivirus, IPS, Antispam and other UTM features enabled for the protection of the Completed Infrastructure. The Device configurations comply with all security parameters and has been integration with the Radius server for Authentication. Any change to this device configurations comes with the network and security division. All configuration, backup and rules been documented for the compliance.

Network & Endpoint protection / monitoring

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, antimalware and Trojan protection from any source. This also includes the email scanning of the systems which prevents malicious scripts and viruses from the emails. Apart from which all systems are restricted to internet with the content filtering system routed through the proxy server.

Monitoring

Cyfuture has 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 Cyfuture's resources are monitored, tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity related issues. Addition of new information systems and facilities, upgrades, new version and changes are subject to formal system analysis, testing and approval prior to acceptance.

Patch Management

The respective vertical team of Windows/Linux/Network team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. 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 related and marked critical and security are managed and applied as they become available, windows systems are managed through the WSUS patch management system whereas Linux systems are managed through SVN repository and the network devices OS patching is being managed manually.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the system admin internally. Cyfuture uses Open Vas for vulnerability scans.

Virus Scans and Endpoint Security

McAfee Endpoint Security is installed with the feature of scanning the device automatically and log reports are reviewed by the system Admin. Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

All inbound and outbound e-Mails are scanned for viruses and are cleaned automatically using McAfee Email scan services. Anti-malware and security practices are the part of McAfee End point protection system and are in accordance with the Cyfuture Information Security Policy.

People

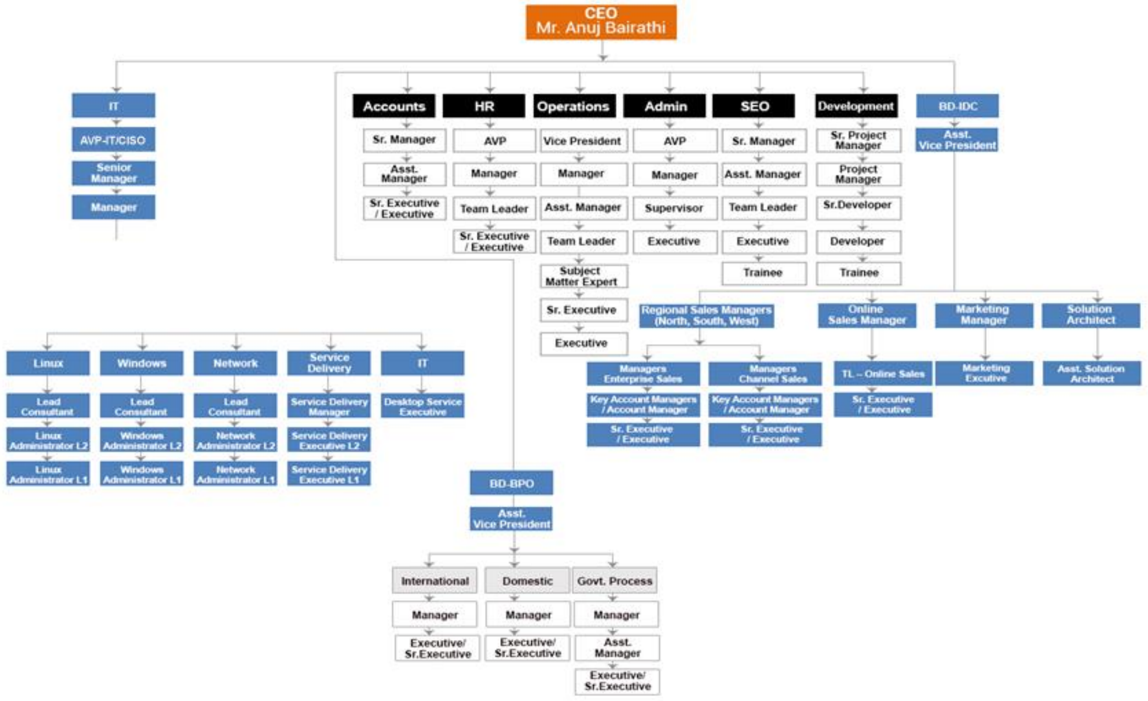
Organizational Structure

The organizational structure of Cyfuture 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 Cyfuture clients.

Mr. Anuj Bairathi manages and oversee all India operations. The management team meets Quarterly to review business unit plans and performances. Meetings with CEO and department heads are held to review operational, security and business issues, and plans for the future.

Cyfuture’s Information Security policies defines and assigns responsibility/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Organization Chart



Roles and Responsibilities

The following are the responsibilities of key roles.

Role of IT Infra Head

- To assess and identify resources required implementing and maintaining the Information Security System as per the Standard.
- Ensure compliance with applicable controls through regular review of data classification and authorized access.
- To organize management review meeting at the stipulated intervals and report the performance of the Information Security System to top management.
- Availability of Infrastructure/Human Resource and Monitoring.
- To impart training on Information Security system throughout the Company.
- To initiate action on: Corrective action on non-conformities, Development activities to maintain and improve Information Security systems, to represent the needs of customers in internal functioning, Approve & maintain Master List of Documents.
- Handling all Technical Issues
- Ensure VAPTs are conducted on 6 months basis

Role of Cyfuture CISO

- To work in co-ordination with Information Security Management Team, issue guidelines, incorporate appropriate procedures, conduct routine internal audit checks to verify the compliance to the Information Security Policies and Procedures and detect incidents..

- Lead the System Administration Team and Information Security Management Team in the information security related activities.
- Prepare security briefs for Information Security Management Team.
- Maintain ISMS.
- Establish the Security Risk Assessment Process, and Review Risk Assessment Reports and status.
- Establish and support the Risk management process for CYF Information systems.
- Select controls and risk mitigation.
- Maintain the Statement of Applicability.
- Monitor ongoing compliance with security standards.
- Establish and maintain contacts with external security resources.
- Evaluate changes in asset base and resultant security implications.
- Manage the timely resolution of all issues and questions regarding responsibilities for Information security management within CYF that relate to achieving and maintaining full compliance with the Information Security Policies and Procedures..
- Ensure that responsibilities are defined for, and that procedures are in effect, to promptly detect, investigate, report and resolve Information security incidents within CYF.
- Seek legal guidance in case of illegal activities or hacking related to CYF. Notify such issues to the senior management and to the Information Security Management Team immediately.
- Evaluate and recommend on new security products to be implemented across CYF.
- Initiate protective and corrective measures if a security problem is discovered.

Assignment of Authority and Responsibility

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

Human Resources Policies and Procedures

Cyfuture maintains written Human Resources Policies and Procedures. The policies and procedures describe Cyfuture practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behaviour and competence.

The Human Resources department review these policies and procedures on periodic basis to ensure they are updated to reflect changes in the organisation and the operating environment. Employees are informed of these policies and procedures upon their hiring during Induction. Personnel policies and procedures are documented in the Cyfuture Human Resources Policy at intranet hr.cyfurure.com.

New Hire Procedures

New employees are required to read HR corporate policies and procedures and are provided online access to these policies along with HR manual. Hiring procedures require that the proper educational levels have been attained along with required job related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Reference checks are completed for prospective employees. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

New Joiner Trainings

HR coordinates to provide HR training and information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely onboarding tracker and feedback forms from employees.

Employees are required to complete security awareness training at the time of joining. Training is documented, monitored and tracked by management.

Employee Terminations

Termination or change in employment is being processed as per Cyfuture HR related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment. All employees, contractors and third-party personnel are required to return physical and digital Identification/access tokens provided to them by Cyfuture or its clients on their termination of employment or contract.

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

Code of Conduct and Disciplinary Action

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

Procedures

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

Help Desk

Cyfuture has put in place a IT helpdesk function to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to business and ensures that changes to any component of Cyfuture's information assets and infrastructure are controlled and managed in a structured manner. All requests are logged in ticketing tool WHMCS and resolved within the maximum resolution time as defined.

Change Management

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

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

All changes are recorded, approved, implemented, tested and versioned before moving to production environment. The impact of implementing every significant change are analyzed and approved by the IS team Head before such implementation. A sign-off obtained from the personnel who had requested for the change after implementation of the change.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk or Corp IT networking ticketing tool. For Network incidents, Cyfuture IT team received incident tickets via WHMCS ticketing tool and are resolved by them. IT team operates 24X7 for all support functions.

The help desk personnel or IT team study and escalate all security incidents to the designated team for further escalation/resolution. All security incidents are reviewed and monitored by the IT Team. Corrective and preventive actions are completed for incidents.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures and the actions proposed are approved by CISO.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. The default access levels for different departments are defined and documented in Cyfuture HR/Admin policy and IS policies. Any additional access is recommended by the line manager and approved IT Head. Company has standard configuration that is implemented across Desktops & laptops individually.

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

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

Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated by an associated password. Remote access to critical resources is not permitted to any employee.

Passwords are controlled through Password policy of the domain controller and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.

Administrative Level Access

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

Confidentiality

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

Backup and Recovery of Data

Cyfuture has developed formal policies and procedures relating to backup and recovery. Backup policy is defined in the Backup Policy. Suitable backups are taken and maintained.

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 “Backup Policy”

Applicable Criteria and related Controls

The control objectives and Cyfuture’s related controls are included in section 4 of this report, “Independent Service Auditor's Description of Tests of Controls and Results”.

Applicable Trust Services Criteria and related Controls

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

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

User- Entity Control Considerations

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

- **Contractual Arrangements**
    - User organizations are responsible for understanding and complying with their contractual obligations to Cyfuture such as providing input information, review and approval of processed output and releasing any instructions.
- **Other Controls**
    - User Organizations are responsible for ensuring end customer privacy.
    - User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Cyfuture for processing.
    - User Organizations are responsible for their network security policy and access management for their networks, application & data.
    - User Organizations are responsible for working with Cyfuture to jointly establish service levels and revise the same based on changes in business conditions

SECTION 4

INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Control environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
	The Company has a mission and vision statements. Additionally, the entity has developed a clearly articulated statement of ethical values that is understood at all levels of the organization.	Inspected the mission/ vision statement of the company to determine that the vision statement is documented.	No exceptions noted
	The Company has implemented a whistle blower program to identify financial irregularities, unethical practices and frauds. This policy is posted on website as well.	Inspected the whistle blower policy to determine that it is implemented.	No exceptions noted
	The entity has code of conduct within the Employee Handbook that establishes standards and guidelines for personnel ethical behaviour. Personnel are required to read and accept the entity's code of conduct	Inspected the Code of Conduct policies to determine that the entity has established standards and guidelines for personnel ethical behaviour including code of conduct.	No exceptions noted
	All new employees have to read and sign the Confidentiality Agreement/NDA upon joining.	Selected a sample of new joiners and inspected personnel file to determine that Confidentiality agreements / NDA are signed.	No exceptions noted Confidentiality agreements/ NDAs sampled for 5 candidates. Signed by all employees
	As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of the Acceptable Use Policy (AUP).	Selected a sample of new joiners and inspected the acknowledgement from them of the Acceptable Use Policy	No exceptions noted Verified the understanding of AUP
	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	Selected a sample and inspected the vendor agreements to determine that the agreements define the terms, conditions and responsibilities of these vendors and their subcontractors.	No exceptions noted
	Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected Client Escalation Matrix and determined that customer have a mechanism to communicate with the company.	No exceptions noted
	The company has the following certifications. 1. ISO 27001:2013 2. PCI DSS 3. ISO 20000-1:2011 4. ISO 9001:2015	Inspected the following certifications to determine these are in place and valid. 1. ISO 27001:2013 2. PCI DSS 3. ISO 20000-1:2011 4. ISO 9001:2015	no exceptions noted
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of		

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	the development and performance of internal control.		
	Management Review Meetings headed by CEO are held every 12 months to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.	Enquired with management that there were no MRM conducted during the audit period. Inspected the Feb 2019 MRM meeting meeting minutes to determine that MRM were held within the last one year.	No exceptions noted No management review meetings were held during the audit period.
	The Management team meets atleast Monthly and discuss the business as well as operational issues	Selected a sample of management meetings held and inspected the minutes to determine that management meetings are held on a periodic basis.	Monthly MOMs are evident for the period of May, June ,July and Aug 2019.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	Organization charts are established that depicts authority, reporting lines and responsibilities for management of its information systems. These charts are communicated to employees and are updated as needed	Inspected the organization chart for an understanding of the hierarchy. Enquired with Management to determine that organisation charts are updated periodically.	No exceptions noted
	Company has Information security related policies and procedures that describes information security processes, practices and organization.	Inspected IT Policies and Procedures to determine that these are documented approved by AVP-IT	No exceptions noted
	Information Security Policy & Procedures related to HR policies are reviewed and approved by the Management at least annually.	Inspected IT Policies and Procedure to determine that changes during the audit period are approved by AVP-IT	No exceptions noted
	The responsibility of managing Information Security is assigned to AVP-IT. Allocation of information security responsibility is documented in Roles and Responsibilities	Inspected Roles and Responsibilities to determine that Information Security activities are responsibility of AVP-IT.	No exceptions noted
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	The company has documented HR Policies and procedures including recruitment, training and exit procedures.	Inspected the HR Policies and procedures to determine that these are documented	No exceptions noted
	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.	Inspected the HR Policies and a sample of related job description to determined that requirements for each role are documented and are evaluated as part of the hiring process. Selected a sample of new joiners and inspected the HRMS Tool for the competency checks such as interview notes.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.	Selected a sample of new joiners and inspected the offer letter / appointment letter to determine that new joiners accept the terms of employment.	No exceptions noted. Employment contracts evident
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of HR meeting minutes to determine that resource planning is reviewed periodically.	HR MOM Evident for resource planning with Management
	Internal HR Reference checks are conducted by HR team or the hiring manager through document verification and references checks with the former colleagues or managers provided in the resume. External BGV are not carried out.	Selected a sample of new joiners and inspected personnel file to determine that internal HR reference checks are carried out as per defined policies.	No exceptions noted External BGV are not carried out.
	Company does not employ contractors.	Enquired with HR Head that the company does not employee contract staff.	No exceptions noted
	Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position	Enquired with HR Head that all new employees undergo induction training.	No exceptions noted
	The induction training given by HR includes information security training. In this training the HR, physical access and security poliices are explained.	Inspected New Hire Induction Training Presentation to ensure that it includes policies on security and also covers identification and report of security breaches Selected a sample of new joiners and inspected the induction attendance/ training records to determine that new joiners undergo information security trainings.	Exceptions noted Induction training records are not available for the sample selected.
	An awareness refresher training is provided to all employees on at least annual basis.	Inspected training records for a sample of existing employees and determined that annual training was completed.	No Exceptions noted
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	Roles and responsibilities are defined in written job descriptions and communicated to employees and their managers	Inspected the IT policies / Roles and responsibilities document to determine that roles and responsibilities are defined.	No exceptions noted
	All critical roles that are likely to have external or internal pressures report into the CEO	Inspected the organisation chart to determine that all critical roles report into the CEO	No exceptions noted
	Job descriptions are reviewed by entity management on an annual basis as part of performance appraisals.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as an when required.	No exceptions noted
	Performance appraisals are performed at least annually.	Inspected a sample of performance appraisals for existing employees to determine that performance appraisals are performed at least annually	No exceptions noted
	Communication and Information		

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
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.		
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place. System Boundaries are shared with the customers when it is required.	Inspected the Information Security policies and scope document and the network diagram to determine that the Company has defined system boundaries.	No exceptions noted
	Customer responsibilities and appropriate system descriptions are provided in client contracts-MSA.	Inspected MSA/Client contracts for terms related to brief requirements of the system and customer responsibilities	No exceptions noted
	Security policies are published on intranet.	Inspected the Corporate Intranet site to determine that IT security policies available to internal users.	No exceptions noted
	An organizational wide incident management process is in place	Inspected ISMS / Information Security Policies to determine that incident management process is documented.	No exceptions noted
	Entity communicates its commitment to security as a top priority for its customers via contracts / website pages	Inspected a sample of customer and vendor contracts to determine that it contains clauses relating to confidentiality.	No exceptions noted
	All system changes that affect internal and external users are communicated in a timely manner	Inspected ISMS and related change management policies to determine how changes to system are communicated to users.	No exceptions noted
	Clients are provided with an escalation matrix that is used by clients to communicate with Cyfuture.	Inspected the escalation matrix, with esclation levels, to determine that clients can contact Cyfuture using these contact points.	No exceptions noted
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with AVP-IT/CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No exceptions noted
	New employees hired at senior levels are communicated to stakeholders by HR through Email	Enquired with CEO that senior management hires are communicated internally and if necessary, externally. Enquired that there was no senior level management hiring during the period for senior employees.	No exceptions noted
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / MSA	Inspected sample of Client contracts / MSA and determined that terms related to delivery of services such as availability and confidentiality are covered.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Customer specific SLA are monitored on monthly basis. These are shared with customers based on the customer requirements.	Inspected a sample of monthly MIS to determine topics that business operations were monitored and communicated to clients.	No exceptions noted
	Customer responsibilities are described in client contracts - MSA	Inspected a sample of client contracts MSA to determine explicit responsibilities of customer	No exceptions noted
	Users are informed of the process for reporting complaints and security breaches during induction Security Training.	Selected a sample of new employees and inspected evidence to determine that they attended Security Training during induction.	Exceptions noted Induction training records are not available for the sample selected.
	Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected Client Escalation Matrix and determined that customer have a mechanism to communicate with the company.	No exceptions noted
	Customer responsibilities are described in the customer contracts and in system documentation	Inspected a sample of customer Contracts-MSA for the roles and responsibilities and determined that roles and responsibilities are clearly defined. .	No exceptions noted
	AVP-IT/CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with AVP-IT/CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No exceptions noted
	Changes to system boundaries, network systems are communicated to clients, if it impacts their operations	Enquired with AVP-IT/CISO that changes to system boundaries are communicated internally and externally	No exceptions noted
	Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	Inspected the Incident Management Procedure to determine that major incidents are reported to clients along with root cause.	No exceptions noted
	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.		
	Management has a business planning process in place that examines existing objectives and establishes new objectives when necessary.	Inspected a copy of the Meeting Minutes done by Senior management to determine that strategic plans / business objectives are in place.	No exceptions noted
	Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process that includes risk assessment scales.	No exceptions noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of HR meeting minutes to determine that resource planning is reviewed periodically.	No exceptions noted
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a		

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	basis for determining how the risks should be managed.		
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment Procedure and process to determine that the Company has a defined and documented risk assessment process.	No exceptions noted
	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.	Inspected Risk Assessment performed during the audit period to determine updation of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No exceptions noted
	Identified risks are rated and get prioritized based on their Probability, impact, detection and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No exceptions noted
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
	A patch management script is run periodically to automatically update user systems.	Inspected screenshot of WSUS / patch management script to determine that patches are applied periodically,	No exceptions noted
	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 exceptions noted
	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 exceptions noted
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
	Emerging technology and system changes are considered when performing risk assessment	Inspected sample of Risk Assessment performed during the audit period to determine that risk assessment is carried out for emerging technology and system changes.	No exceptions noted
	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 exceptions noted
	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.		
	The internal audit function conducts system security reviews yearly. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No exceptions noted There were no internal audits

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
			performed during the audit period
	Audit calendar is established to cover all locations, business units and the frequency is adjusted to address high risks.	Inspected the Annual Audit Calendar / Audit Plan to determine that all locations and major departments are covered.	No exceptions noted
	IT system access is reviewed on a quarterly 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.	Exceptions noted System access review was started in July 2019 and was not in place throughout the audit period.
	Vulnerability assessment & penetration tests are performed quarterly by a third party PCIDSS ASV.	Inspected the latest vulnerability assessment /penetration test report performed by a third party PCIDSS ASV and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No exceptions noted
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.		
	Firewall is configured to log events that are reviewed on a periodic basis	Inspected the firewall configuration settings to determine that the firewall is configured to log events.	No exceptions noted
	Vulnerability assessment & penetration tests are performed quarterly by a third party PCIDSS ASV.	Inspected the latest vulnerability assessment /penetration test report performed by a third party PCIDSS ASV and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No exceptions noted
	Results of the vulnerabilities are reviewed by the management	Inspected the latest vulnerability assessment /penetration test report performed by a third party PCIDSS ASV and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No exceptions noted
	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.		
	Internal audits including access reviews are performed every yearly. Results and recommendations for improvement are reported to management. Audit has a rotation plan so that all areas are covered.	Inspected annual audit reports to determine that audits are performed periodically	No exceptions noted There were no internal audits performed during the audit period
	Segregation of duties is in place for critical functions and departments	Inspected the Information Security Policy and Procedures to determine that these define segregation of roles for major controls.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No exceptions noted
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.		
	Significant policies and procedures are uploaded to the intranet and available for all employees that require access to these policies/procedures.	Inspected the Corporate Intranet site to determine that IT security policies as well as other business function policies are available to internal users.	No exceptions noted
	All policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.	Inspected ISMS Roles and Responsibilities to determine that Roles and Responsibilities are documented and communicated.	No exceptions noted
	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.		
	Company has documented procedure for logical access controls	Inspected the access control policy and procedure and determined that these are documented.	No exceptions noted
	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 exceptions noted
	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 to determine that hardening standards have been established.	No exceptions noted
	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 exceptions noted
	3rd party vulnerability scans are performed at least quarterly 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 exceptions noted
	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 exceptions noted
	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.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
		Observed a user sign-on process to determine if an ID and password were required to verify identity.	
	The Company has a remote working policy that requires that external access is granted on a need basis. Currently, as a default, external access by employees is prohibited.	Enquired with IT staff about external access by employees and determined that external access is not allowed. Inspected Information Security Policy and determined that Company has remote working policies that are documented	No exceptions noted
	The IT department maintains an up-to-date listing of all software.	Inspected the software list maintained by the IT to ensure that it is up to date. Inspected the softwares installed in sample desktop to ascertain that current versions are installed.	No exceptions noted
	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 exceptions noted
	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 AVP-IT 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 privileged access is min access was authorized by AVP-IT	No exceptions noted
	Entity systems are configured to use the active directory shared sign-on functionality.	Determined through enquiry with IT staff that all resources use single signon through active directory. Inspected login requirement in Default Domain Policy and determined that all authenticated users are covered by domain policy.	No exceptions noted
	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 exceptions noted
	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 exceptions noted
	The following password parameters are in place for active directory: 1. length of 8 character length 2. complexity is enabled	Inspected the default password security setting in the domain group policy to determine that password settings are: 1. length of 8 character length	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	3. password expires in 30 days 4. Password history is set at 4	2. complexity is enabled 3. password expires in 30 days 4. Password history is set at 4	
	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 exceptions noted
	External access is through firewall appliance that allows only the white listed IP addresses.	Inspected firewall console and determined that incoming connections are from whitelisted IPs only.	No exceptions noted
	All confidential data is classified as per the data classification policy	Inspected information security policies to determine that data classification policies are documented.	No exceptions noted
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.		
	On the day of joining, HR will send a mail to IT Helpdesk providing the details of the new joiners. The IT then provides necessary access as per request Employee user accounts are removed from various application and network system as of the last date of employment manually based on access revocation request sent by HR department.	Inspected the Access Control procedure and determined that granting, modifying or deactivating access is only done against written authorization. Inspected access request forms / emails for a sample of employees to determine that written authorisation is in place. Inspected access revocation request /exit checklist for a sample of employees to determine that written authorisation for deactivation is in place.	No exceptions noted
	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 exceptions noted
	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 exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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 AVP-IT 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 privileged access is min access was authorized by AVP-IT	No exceptions noted
	Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees.	No exceptions noted
	Company does not employ contractors in its offices.	Enquired with IT staff about access to non-employees to determine that there are no contractors.	No exceptions noted
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.		
	A role based Organizational Units is setup in Active directory with groups and roles based on job requirements.	Inspected the Organizational Units in the domain and determined that security groups based on departments and roles have been defined	No exceptions noted
	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 exceptions noted
	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 exceptions noted
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
	Entry to the all office premises is restricted to authorized personnel. Physical access control system has been implemented to secure the facilities.	Observed that the entry to premises is restricted by biometric access. Physically Observed the Biometric based physical access control system used for entering &amp; exiting the office. During the audit, observed users entering and exiting only after gaining access through the physical access system.	No exceptions noted
	Physical access to office premises is monitored through CCTV installed at key points within the premises.	Observed that the CCTV are located across the premises and that the CCTV are working.	No exceptions noted
	There is a security desk at the office entry manned by a security guard	Physically observed the security staff at the reception who ensure that the all visitors and employees	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
		are screened before entering the office.	
	All visitors have to enter their details in the visitor register.	Inspected the visitor register for a sample of dates to determine that visitor register is maintained.	No exceptions noted
	Visitor badges are for identification purposes only and do not permit access to the facility.	Physically Observed that visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.	No exceptions noted
	All visitors must be escorted by a Company employee when visiting office facilities.	Physically Observed that all visitors are escorted by a Company employee when visiting Company office.	No exceptions noted
	ID cards that include an employee picture must be worn at all times when accessing or leaving the facility.	Physically observed a sample of employees that employees wear picture IDs at all times.	No exceptions noted
	Physical access is setup by the HR Dept for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas.	Selected a sample of new employees and inspected that the access rights were granted in the physical access system only to authorised new joiners.	No exceptions noted
	Physical access to sensitive areas / server rooms is granted only to privileged users / IT Team Access to such restricted zone is given against written request by the AVP-IT.	Inquired with IT Team that access to server room and other sensitive areas is granted only to IT team.	No exceptions noted
	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 exceptions noted
	Upon the last day of employment, HR Team sends exit email requesting for deactivation of physical access for terminated employees. Physical access is deactivated by the Admin Team	Inspected biometric system to determine that the employee ID numbers for the sample of exited employees were deleted from the biometric system.	No exceptions noted
	Employees are required to return their ID cards on the last day, and all ID badges are disabled.	Inspected the exit checklist for a sample of terminated employees to determine that ID cards are returned. Inspected the biometric system activation / deactivation log to ensure that access of terminated employees have been revoked.	No exceptions noted
	On a quarterly basis, Internal audit / HR performs a reconciliation that physical access for terminated employees has Infact 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.	Exceptions noted Physical access reconciliations to detect any errors in access revocations are not performed.
	No contractor is given access card.	Enquired with facilities about contractor access and determined no contractor has been given ID card for entering the office.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	The sharing of access badges and tailgating are prohibited by policy.	Physically Observed that access badges are not shared & no tailgating observed.	No exceptions noted
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.		
	Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment	Inspected the media handling Procedure to determine that it is documented.	No exceptions noted
	All data is erased from laptops and other media prior to destruction disposal. As a practice all faulty/disposed off hard drives / servers are kept in a secure area for future disposal. There was no disposal during the audit period.	Enquired with Head IT that all media that is to be disposed off is kept in a secure area for future disposal. Enquired with Head IT that there were no instances of media disposal during the current audit period. Inspected the photos of the disposed off media that is tagged as such and maintained separately.	No exceptions noted
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	External points of connectivity at office network are protected by firewall. The firewall provides unified threat management (UTM) services such as intrusion protection, web filtering and inbound and out bound traffic filtering.	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 determined that configuration is in compliance with the policy and incoming connection are allowed only from whitelisted IPs.	No exceptions noted
	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 exceptions noted
	Company has implemented content filtering system through firewall that blocks access to certain sites such as personal emails, storage etc.	Inspected firewall console screens containing rules about ports, incoming connection types, whitelisted IPs and type of traffic and determined that is complies with the company policy and hardening standards.	No exceptions noted
	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 exceptions noted
	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 exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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 exceptions noted
	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 exceptions noted
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.		
	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 exceptions noted
	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 exceptions noted
	Storage for laptops is encrypted.	Enquired with Head IT that all storage for laptops is encrypted.	No exceptions noted
	Backup media are encrypted during creation.	Enquired with Head IT that all backup media are encrypted during creation	Backup Tool have the capability and is evident.
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.		
	Antivirus software is installed on workstations, laptops, and servers. This system provides antivirus system scans, email scans, content filtering and endpoint protection.	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 exceptions noted
	Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines.	Inspected a query report from the console showing unupdated computers and determined that there were no such cases. Inspected the antivirus/firewall console for configuration details about updating and alerts.	No exceptions noted
	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 AVP-IT.	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 exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Any viruses discovered are reported to IT team either by the antivirus system or by the affected employees.	Inspected the antivirus console for configuration details about updating and alerts. Inspected the security training pack for the instructions to employee about virus incidence reporting.	No exceptions noted
	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.		
	Management has defined configuration standards and hardening standards.	Inspected IT policies and procedures to determine that hardening standards have been established.	No exceptions noted
	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 exceptions noted
	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 exceptions noted
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 analyzed to determine whether they represent security events.		
	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 exceptions noted
	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 exceptions noted
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.		
	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 exceptions noted
	Incidents are reported to the IT team. These are tracked through an incident management tool.	Inspected the screenshot of the incident management tool to	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
		determine that incidents are tracked.	
	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 exceptions noted
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.		
	All security incidents are also reviewed and monitored by the Management. Corrective and preventive actions are completed for incidents.	Inspected minutes of Meeting of IT for discussion on incidents.	Exceptions noted Incidents are not discusssed during the management meetings.
	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 exceptions noted
	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 exceptions noted
	Quarterly, management reviews all incidents that occurred during the quarter.	Inspected minutes of IT Meeing for discussion on incidents.	Exceptions noted Incidents are not discusssed during the management meetings.
	HR policies include code of conduct and disciplinary policy for employee misconduct.	Inspected the Corporate Website for Code of Conduct and Disciplinary Policy	No exceptions noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security 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 exceptions noted
	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.		
	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 exceptions noted
	All change requests for IT infrastructure are logged and change request ticket created. Major changes are approved by AVP-IT	Selected a sample of change requests to determine that these are logged and that major changes are approved by AVP-IT.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	The company uses Standard VMware vCloud Network (vCAN) Packaged applications for the clients processes / system in scope and hence there is no software development and related change management for applications. There is no Software Development internally.	Inspected the Cloudoye interface and agreement with VMware to determine that company uses Standard VMware vCloud Network (vCAN) Packaged Application within the client process. Enquired with AVP-IT that there is no Internal Software Development.	No exceptions noted
	CloudOye application related software development changes to CloudOye application are carried out by the vendor and periodic patches are provided to Cyfuture for deployment. Cyfuture tests these patches in development, before updating production instances. Rollback plans are documented.	Inspected a sample of change requests for deployment of patches for Cloudoye updates to determine that patch management are tested approved.	Pending
	All change requests are submitted with implementation and rollback plans.	Inspected a sample of change requests to determine that they had rollback plans included.	No exceptions noted
	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 exceptions noted
	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 exceptions noted
	A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review.	Inspected Change Management Procedure to determine that the policy considers process to manage emergency changes	No exceptions noted
	Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
	Entity has a documented BCP and DR guideline to be used in the event of an event necessitating systems infrastructure recovery.	Inspected the policies and procedures relating to disaster recovery & Business Continuity plans to determine that a plan and procedure has been documented with clear responsibilities on those required to respond.	No exceptions noted
	Business continuity and disaster recovery plans, including restoration of backups, are tested atleast annually.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested at least annually.	No exceptions noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
	New Third Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process.	Enquired with Management that vendors and third party service providers are selected based on a vendor due diligence.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
		Enquired with Management that there was no material third party vendor that was onboarded during the audit period.	
	A formal contract is executed between Company and Third Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.	Inspected a sample of vendor contracts to determine that vendors contracts are in place. Enquired with Admin head that there are no new vendors that are onboarded during the current period.	No exceptions noted
	There is no information sharing with vendors or any third party.	Enquired with Management that no confidential information is shared with vendors or third parties	No exceptions noted
	A confidentiality agreement is signed by all employee at the time of joining. In addition NDAs are signed with third parties wherever required.	Inspected the confidentiality agreement template to determine that agreements includes terms on confidentiality and non-disclosure.	No exceptions noted
	Company has limited number of vendors such as office lease, security service vendor and housekeeping services. There is no requirement for SOC2 for these vendors since no there is no information shared with these vendors.	Inspected a sample of customer and vendor contracts to determine that it contains clauses relating to confidentiality.	No exceptions noted
	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.		
	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements Processing capacity is monitored by tools such as 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 Nagios report to determine that tool monitors and reports on uptime, outage and response time.	No exceptions noted
	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 exceptions noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance.	Observed that fire extinguisher across all office premises that these are in working condition. Observed other environmental controls.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Devices are checked on a periodic basis and checklists are prepared.		
	Fire drill is conducted Six Monthly.	Observed the fire drill report and verified that there were no exceptions noted.	No exceptions noted
	Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. DG set of sufficient capacity is provided to provide power during outage.	Physically observed the UPS and DG Set installed at the premises to determine that they are in good working condition.	No exceptions noted
	Company has multiple ISPs in place to provide redundancy in case of link failure	Inspected the network diagram to determine that the company has multiple ISPs in place.	No exceptions noted
	IT Engineer monitors the temperature in server room on a daily basis and take corrective actions in case of discrepancy	Selected a sample of dates and inspected the server room temperature monitoring records to determine that server room temperatures are monitored.	No exceptions noted
	Vendor warranty specifications are complied with and tested to determine if the system is properly configured.	Inspected MSAs, building lease and vendor contract for maintenance of various environmental controls.	No exceptions noted
	Facilities and admin personnel monitor the status of environmental protections on a regular basis. Maintenance checklists are used where applicable.	Inspected environmental control check report and determined that maintenance reviews are carried out. Inspected the UPS and DG preventive maintenance reports, vendor maintenance contracts to determine that preventive maintenance is performed periodically.	No exceptions noted
	Backup policy is defined in the information security policies	Inspected information security policies to determine that backup schedules, frequency of backups are documented.	No exceptions noted
	Automated backup systems are in place to perform scheduled differential and full backup 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 exceptions noted
	Local office backup is carried out on local NAS device maintained within the server room. Frequency of data backup is multiple times a day.	Inspected the NAS backup screenshots/ console to determine that backup frequencies are defined for various local data.	No exceptions noted
	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 exceptions noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented.	Inspected disaster recovery & Business Continuity plans to determine that these are documented.	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	The entity has contracted with a third-party recovery facility to permit the resumption of IT operations in the event of a disaster at the IT data center.	Inspected the contract with the third party offsite vendor for BCP strategies.	No exceptions noted
	Business continuity plans, including restoration of backups, are tested at least annually.	Inspected BCP/DR test report to determine that BCP plans have been tested.	No exceptions noted
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company retains information as per the defined policies.	No exceptions noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company destroys or disposes of confidential information as per the defined retention policies.	No exceptions noted

SECTION 5

OTHER INFORMATION PROVIDED BY CYFUTURE

Other Information Provided by Cyfuture

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

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, Cyfuture’s disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls Cyfuture has implemented to safeguard against an interruption of service, the Company has developed a number of procedures that provide for the continuity of operations in the event of an extended interruption of service at Noida Data Center. In the event of an extended interruption of service, Cyfuture will utilize backup site maintained at Jaipur Data Center.

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.