SSAE 18 - SOC 1 TYPE 2 REPORT (CYFUTURE)

For the period, 1st January 2023 to 31st July, 2023

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

Contents

SECTION 1

Management of Cyfuture’s Assertion

MANAGEMENT ASSERTION DOCUMENT

Date: 18-10-2023

Management of Cyfuture India Private Limited Assertion

We have prepared the accompanying description of the **Cyfuture India Private Limited** (Cyfuture) system titled **"Data Center Services Including Web Site Hosting, Web App Hosting, Server Co-Location, Disaster Recovery, Backup, Email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services"** throughout the period 1st January 2023 to 31st July, 2023 (description), 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 1 Type 2 Report (description criteria).

The description is intended to provide users with information about the system providing data center services including web site hosting, web app hosting, Server co-location, etc. that may useful when assessing the risk arising from interactions with Cyfuture controls meet the criteria related to internal controls **Security, Availability, Privacy, Process Integrity, and Confidentiality (Applicable Trust Services Criteria)**

As indicated in the description, Cyfuture does not use any sub-services organizations.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Cyfuture controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. The description fairly presents the system the period 1st January 2023 to 31st July, 2023 based on the following description criteria:

The description contains the following information:
1) The types of services provided
2) The components of the system used to provide the services, which are as follows:

a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

d) Procedures. The automated and manual procedures.

e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

3) The boundaries or aspects of the system covered by the description.

Cyfuture India Pvt. Ltd.
(Formerly known as Cyber Futuristics India Pvt. Ltd.)
Noida (Corporate office): Plot No. 197-198, Noida Special Economic Zone, Dadri Road, Phase II, Noida-201305 (U.P.) **Tel:** +91-120-6277700 | **Fax:** +91-120-6667766
Jaipur (Regd.Office): G1-227,228 & H1-236,239, Opp. Fire Station, EPIP Sitapura, Jaipur 302022 (RJ) **Tel:** +91-141-2770439/440 | **Fax:** +91-141-2770425
CIN No.: U72200 RJ 2001 PTC 017138 | **E-mail:** info@cyfuture.com | www.cyfuture.com

4) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

a) Complementary user entity controls contemplated in the design of the service organization's system.

8) In the case of a SOC type 1 report, relevant details of changes to the service organization's system during the period covered by the description.

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

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Company Name controls period of 1st January 2023 to 31st July, 2023.

c. The Cyfuture controls stated in the description operated effectively the throughout period of 1st January 2023 to 31st July, 2023 to meet the applicable trust services criteria if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Cyfuture period of 1st January 2023 to 31st July, 2023

Name: AJAI RAI

Signature: A Rai

Date:

18|10|2023

SECTION 2

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 January 01, 2023 to July 31, 2023(description), and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Cyfuture's Assertion" (assertion). The controls and control objectives included in the description are those that management of Cyfuture believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, "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 January 01, 2023 to July 31, 2023. 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.

Cyfuture does not use any subservice organisations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed 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.

Service Organization's Responsibilities

Within Section 2 of this report, Cyfuture has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Cyfuture is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 01, 2023 to July 31, 2023.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. 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 achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2 of this report. 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 user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to therisk 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 January 01, 2023 to July 31, 2023.

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 January 01, 2023 to July 31, 2023, and the subservice organization and user entities applied the controls contemplated in the design of Cyfuture's controls throughout the period January 01, 2023 to July 31, 2023.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 01, 2023 to July 31, 2023, 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 January 01, 2023 to July 31, 2023.

Description of Test of Controls

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

Intended Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of management of Cyfuture; user entities of Cyfuture' systems during some or all of the period January 01, 2023 to July 31, 2023; and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting

and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements.

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

Spadhi

Sandip Padhi
Place: Date: 06-11-2023

SECTION 3

Description of Cyfuture’s “System” throughout the period January 01, 2023 to July 31, 2023

Description of Cyfuture's system throughout the period January 01, 2023 to July 31, 2023

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 is 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	Meghdoot , Plot no 197/198 Noida Special Economic Zone Noida Dadri Road, Noida Phase II Noida - 201305

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.

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 authentications to access emails.

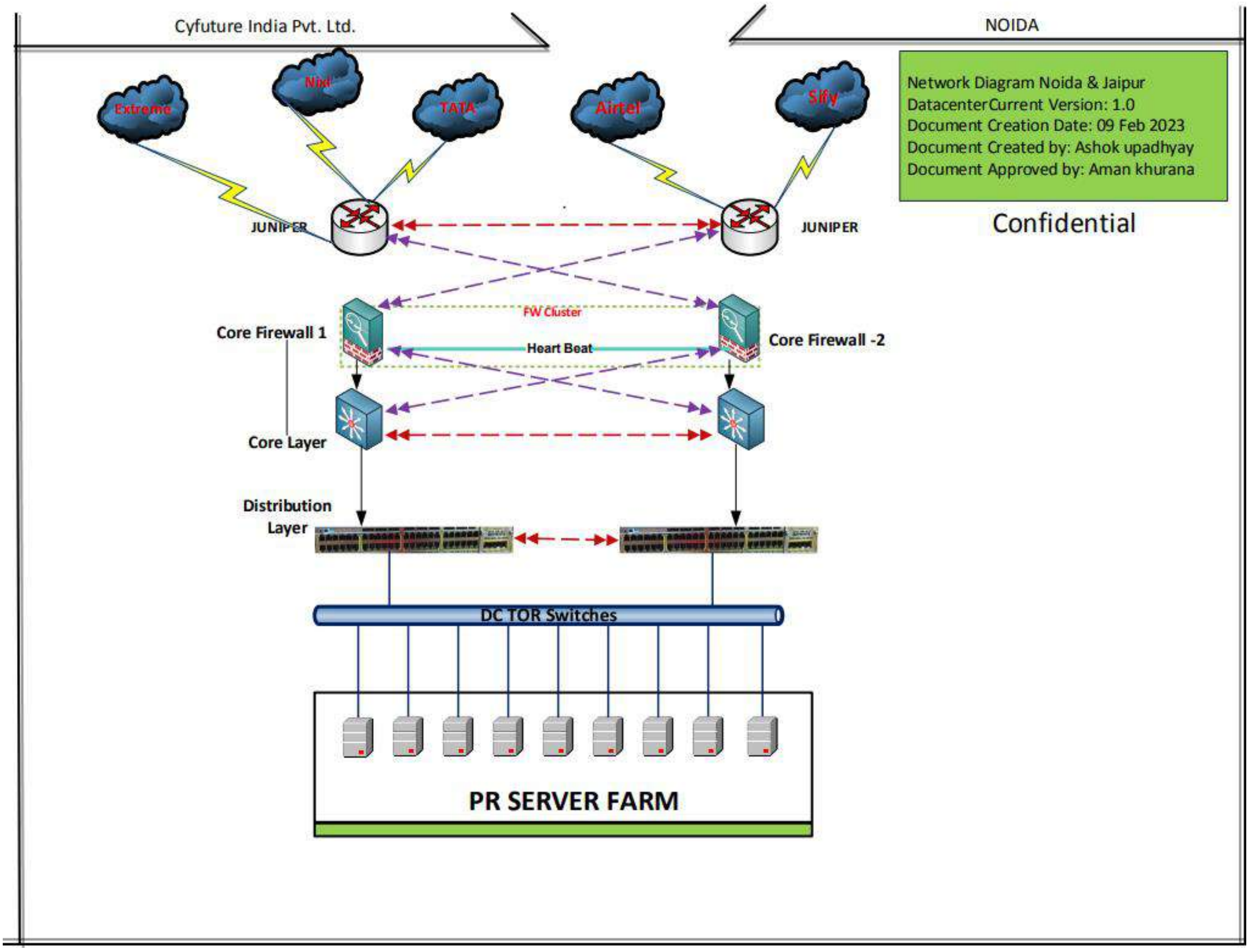
Components of the System

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 a 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 Harmony Endpoint protection for vulnerability scans.

Virus Scans and Endpoint Security

Check Point Harmony Endpoint 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 check point Harmony Endpoint protection system and are in accordance with the Cyfuture Information Security Policy.

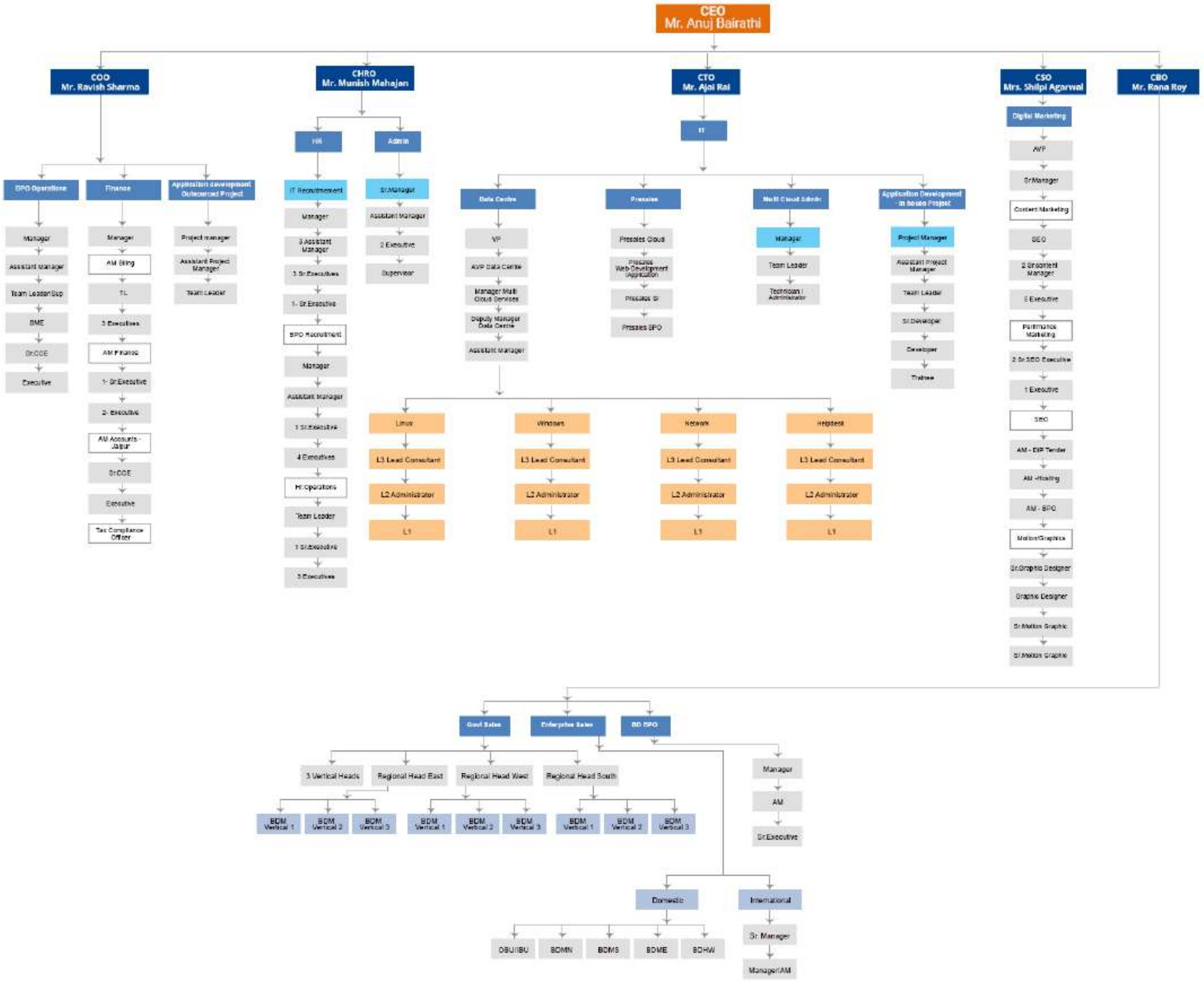
People

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.



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 an 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 is 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"

Description of Control Objectives for Cyfuture

The following summarizes the control objectives covered as part of this description. The detailed controls for each of these control objectives are covered under Section 4 of this report and form an integral part of the description of the system. These controls are required to be part of the description and for clarity have been summarized within Section 4.

Control Objective #	Control Area	Description
Control Objective 1	Organization and Management	Control activities provide reasonable assurance that senior management provide planning and oversight of the organization's activities
Control Objective 2	Personnel Security Procedures	Controls provide reasonable assurances that people related risks are mitigated and that all hiring, continued employment, transfers and separation from employment are carried out in accordance with defined policies and procedures.
Control Objective 3	System Description and Communication	Controls provide reasonable assurance that system components are defined and communicated
Control Objective 4	Risk Management	Controls provide reasonable assurance that key risks are identified, assessment and mitigation strategies implemented in a timely manner.
Control Objective 5	Network Security	Controls provide reasonable assurance that network systems are secured and available as per requirement.
Control Objective 6	Physical Security	Controls provide reasonable assurance that physical access to the work area, computer equipment, storage media, and customer provided documentation is restricted to authorized individuals.

Control Objective #	Control Area	Description
Control Objective 7	Incident Management	Controls provide reasonable assurance that security related incidents are reported, evaluated and resolved in a timely manner
Control Objective 8	Change Management	Controls provide reasonable assurance that changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with policies, commitments and requirements.
Control Objective 9	System Availability	Controls provide reasonable assurance that systems are available as per defined SLA.
Control Objective 10	Environmental Safeguards	Controls provide reasonable assurance that adequate environmental safeguards have been enforced
Control Objective 11	Third Party Service Provider Security	Controls provide reasonable assurance that Third Party Service Providers are selected based on Vendor Selection Process, their roles and responsibilities, and performance requirement are formally defined and documented, and they are evaluated periodically.
Control Objective 12	Client Onboarding	Control activities provide reasonable assurance that client onboarding activities are comprehensive and as per defined onboarding processes.

Applicable Trust Services 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".

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

- 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

INFORMATION PROVIDED BY THE SERVICE AUDITOR

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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
1	**Organisation and Management** **Control Objective: Control activities provide reasonable assurance that senior management provides planning and oversight of the organization's activities**		
	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. Document Name – Joining Data 1st Feb 2023 to till date	No exceptions noted
	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 Document Name- Acceptableuserpolicy.pdf	No exceptions noted
	The company has the following certifications. 1. ISO 27001:2013	Inspected the following certifications to determine these are in place and valid. 1. ISO 27001:2013	no exceptions noted
	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 MRM conducted during the audit period. Document Name- 1) May 2023 MRM	No exceptions noted
	The Management team meets at least 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. Document Name- 1) May 2023 MRM	No Exceptions noted
	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 organization charts are updated periodically. Document Name- 1. 9563-5- Organisation roles responsibilities & authorities	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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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. Document Name- CYF- ISMS- MGT-002-CFT Role's responsibilities Version- 2.0	No exceptions noted
2	**Personnel Security Procedures** **Control Objective: Controls provide reasonable assurance that people related risks are mitigated and that all hiring, continued employment, transfers and separation from employment are carried out in accordance with defined policies and procedures.**		
2A	**New Hire Procedures**		
	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 Document Name- CYF-ISMS-POL-010-Human Resource Security Policy	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. Document Name- CYF-ISMS-POL-010-Human Resource Security Policy Version- 7.0 Document Name- JDSample.msg	No exceptions noted
	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. Document Name- appointment letter.pdf	No exceptions noted

	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. Document Name- 1. Joining Data 1st Feb 2023 to till date 2. Pre and Post Joining Policy Document	No exceptions noted
2B	**Training and Competency**		
	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. Document Name- Policy Refresher Date- 18th May 2023	No exceptions noted
	The induction training given by HR includes information security training. In this training the HR, physical access and security policies 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 Document Name- Policy Refresher Date- 18th May 2023	No exceptions noted
Ref No	**Controls Implemented by Cyfuture**	**Test Procedures**	**Test Results**
		records are not maintained for induction training. Document Name- Revised Induction.ppt	
	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. Document Name- Policy Refresher Date of Training- 18th May 2023	No exceptions noted
	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

	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. Document Name- JDSamples	No exceptions noted
3	**System Description and Communication Control Objective: Controls provide reasonable assurance that system components are defined and communicated**		
	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
	Clients are provided with an escalation matrix that is used by clients to communicate with Cyfuture.	Inspected the escalation matrix, with escalation levels, to determine that clients can contact Cyfuture using these contact points.	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.	No exceptions noted
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / MSA	Inspected MSA/Client contracts for terms related to brief requirements of the system and customer responsibilities	No exceptions noted
	Customer specific SLA are monitored on monthly basis. These are shared with customers based on the customer requirements.	Inspected MSA/Client contracts for terms related to brief requirements of the system and customer responsibilities	No exceptions noted
	Customer responsibilities are described in client contracts - MSA	Inspected MSA/Client contracts for terms related to brief requirements of the system and customer responsibilities	No exceptions noted
	Users are informed of the process for reporting complaints and security breaches during induction Security Training.	Enquired with HR Head that new joiners attend Security Training during induction and that training records are maintained for induction training. Document Name- Revised Induction.ppt and inductiontraining.pdf	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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	Cyfuture is offering Data Center Services and Devaloping services are not Included.	No exceptions noted
4	**Risk Management** **Control Objective: Controls provide reasonable assurance that key risks are identified, assessment and mitigation strategies implemented in a timely manner**		
	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 Treatment Plan 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 and review is the part of internal audit. Document Name: - 1. 9593-CYF-ISMS-PLA-002-Risk Treatment Plan(4)	No exceptions noted
	Identified risks are rated and get prioritized based on their Probability, impact, detection and the existing control measures.	Inspected Risk Treatment Plan performed during the year to determine identified risks are rated Document Name:- Internal Audit	No exceptions noted
	List of all hardware is maintained as part of asset register.	Inspected the asset management Policy to determine that all assets are recorded. Document Name- 9596-CYF-ISMS-POL-003-Asset Management Policy(2)	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. Document Name- 9593-CYF-ISMS-PLA-002-Risk Treatment Plan(4)	No exceptions noted
5	**Network Security** **Control Objective: Controls provide reasonable assurance that network systems are secured and available as per requirement.**		

	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control policy document and determined that access is granted on least privileges basis as default and any additional access needs to be approved. Document Name- CYF-ISMS-POL-001-Access Control Policy	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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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 Document Name: 1. CYF-ISMS-POL-001-Access Control Policy 2. CYF-ISMS-POL-027- Physical Security Policy	No exceptions noted
	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 Document Name- CYF-ISMS-POL-025- Remote Access Policy	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. Document Name- List of Softwares.png	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. Document Name- 9596-CYF-ISMS-POL-003-Asset Management Policy(2)	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 Email to determine that administrator privileges for the domain were limited to IT team.	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

	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. Document Name- VPN Users.png	No exceptions noted
	The following password parameters are in place for active directory: 1. length of 8 character length 3. complexity is enabled password expires in 30 days 2. Password history is set at 4	1. Inspected the default password security setting in the domain group policy to determine that password settings are: length of 8 character length 2. complexity is enabled 3. password expires in 42 days 4. Password history is set at 24 Document name- 9632-CYF-ISMS-POL-019-Password Policy	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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. Document Name- Exit Process	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 and verified their disabled status in AD server. Document Name- Exit Process	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.	No exceptions noted
	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 Document Name- user-list.JPG	No exceptions noted
5A	**Network Security (Firewall)**		
	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. Document Name- Firewall.png	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. Document Name- Firewall.png	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. Document Name- Web Filtering.png	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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. Document List- 9645-CYF-ISMS-POL-018-Network Security, Encryption & information Transfer Policy	No exceptions noted
5B	**Network Security (Encryption)**		
	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. Document Name- CYF-ISMS-POL-018-Network Security, Encryption & information Transfer Policy	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. Document name- CYF-ISMS-POL-001-Access Control Policy	No exceptions noted
5C	**Network Security (Antivirus)**		
	Antivirus software is installed on workstations, laptops, and servers. This system provides antivirus system scans, email scans, content filtering and endpoint protection.	Inspected the antivirus/firewall console for configuration details about updating and alerts. Document Name- AV Dashboard.png	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. Document Name- AV Dashboard.png	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. Document Name- AV Dashboard.png	No exceptions noted

	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. Document Name- AV Dashboard.png	No exceptions noted
6	**Physical Security** **Control Objective: Controls provide reasonable assurance that physical access to the**		

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	work area, computer equipment, storage media, and customer provided documentation is restricted to authorized individuals.		
	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 are screened before entering the office.	No exceptions noted
	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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	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. Document Name: - Exit Records	No exceptions noted
	Employees are required to return their ID cards on the last day, and all ID badges are disabled.	Inspected the exit records 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. Document Name: - Exit Records	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. Document Name: - Exit Records	No exceptions noted
	The sharing of access badges and tailgating are prohibited by policy.	Physically Observed that access badges are not shared & no tailgating observed. Document Name:- Physical Security Policy	No exceptions noted
7	**Incident Management** **Control Objective: Controls provide reasonable assurance that security related incidents are reported, evaluated and resolved in a timely manner**		
	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. Document Name- Servicedesk Tool.png	No exceptions noted
	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. Document Name- CYF-ISMS-POL-011-Incident Management Policy	No exceptions noted
	Incidents are reported to the IT team. These are tracked through an incident management tool.	Enquired with the IT team No internal P1 or high-severity incident reported during the audit period.	No exceptions noted

	Reported incidents are logged as tickets and include the following details Severity Data and Time of incident Details	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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Status Root Cause (High severity incidents only)	Inspected the root cause analysis reports and Root cause analysis is performed for Major incidents. Document Name- #325640 - Unable to access the server 2. #852505 - Getting disk congestion issue in vSAN	
	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. Document Name- MOM-mail.jpg	No exceptions noted
	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. Document Name- CYF-ISMS-PRO-007-Incident Management Procedure Version -5.0 Document Name- CYF-ISMS-PRO-010-Change Management Procedure Version- 5.0	No exceptions noted
8	**Change Management** **Control Objective: Controls provide reasonable assurance that software development and maintenance activities are authorized, tested, approved, implemented and documented.**		
	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. Document Name:- POA Change Request Spam Gateway	Exceptions noted
	The company uses Standard VMware vCloud Network (vCAN) Packaged applications for the client's 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
	All change requests are submitted with implementation and rollback plans.	Inspected a sample of change requests to determine that they had rollback plans included. Document Name:- POA Change Request Spam Gateway	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. Document Name:- POA Change Request Spam Gateway	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 Document Name:- 9670-CYF-ISMS-POL-004-Change Management Policy(3)	No exceptions noted

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
9	**System Availability** **Control Objective: Controls provide reasonable assurance that systems are available as per defined SLA.**		
	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements	Inspected the capacity management policy to verify that the capacity demand is documented and reviewed by management. Document Name:- 9678-CYF-ISMS-POL-021-Capacity Management Policy	No exceptions noted
9A	**System Availability (Backup Procedures)**		
	Backup policy is defined in the information security policies	Inspected information security policies to determine that backup schedules, frequency of backups are documented. Document Name- 9680-CYF-ISMS-POL-006-Data Backup and Restoration Policy(4)	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. Document Name- Messages from IT Auto Notifications	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 Document Name- Messages from IT Auto Notifications	No exceptions noted
	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. Document Name:- CYF-ISMS-PLA - 001-Business Continuity Plan	No exceptions noted
10	**Environmental Safeguards** **Control Objective: Controls provide reasonable assurance that adequate environmental safeguards have been enforced**		
	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared.	Observed that fire extinguisher across all office premises that these are in working condition. Observed other environmental controls. Document Name:- CYF-ISMS-POL-027- Physical Security Policy	No exceptions noted

	Fire drill is conducted Six Monthly.	Observed the fire drill report and verified that there were no exceptions noted. Document Name- Mock Drill March 2023 -197-198	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

Ref No	Controls Implemented by Cyfuture	Test Procedures	Test Results
	Company has multiple ISPs in place to provide redundancy in case of link failure	Inspected the Screenshot of ISP Route to determine that the company has multiple ISPs in place. Document Name- ISP Route.png	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. Document Name- Security Agreement 22-23	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. Document Name- Mock Drill March 2023 -197-198	No exceptions noted
11	**Third Party Service Provider Security** **Control Objective: Controls provide reasonable assurance that Third Party Service Providers are selected based on Vendor Selection Process, their roles and responsibilities, and performance requirement are formally defined and documented, and they are evaluated periodically.**		

	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. Document Name- 1. Supplier Re-evaluation Forms.doc 2. Approved Supplier List	No exceptions noted
	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. Document Name- Approved Supplier List	No exceptions noted
12	**Client Onboarding** **Control Objective: Control activities provide reasonable assurance that client onboarding activities are comprehensive and as per defined onboarding processes.**		
12A	**Client Contracts**		
	Processing is performed appropriately in accordance with client SLAs.	Inspected a sample of monthly MIS to determine topics that business operations were monitored and communicated to clients. Document Name- 2857332600.pdf	No exceptions noted
Ref No	**Controls Implemented by Cyfuture**	**Test Procedures**	**Test Results**
12B	**Client Support**		
	WHMCS Application (ITSM Tool) is used for providing client support for CloudOye cloud services. The application has role based access and only the setup and the support team have access to the client tickets.	Inspected the role based access for the Support application to determine that access to the application is based on defined roles.	No exceptions noted
	Client requirements for creation of cloud infrastructure / VM are documented in Bill of Material (BOM) / client email requests or purchase orders. Client's written request serves as a documented instruction for creation of Virtual machines on the Cloud services.	Selected a sample of Purchase Orders, email requests to determine that client requirements are written and documented	No exceptions noted

	Services Delivery team coordinates with the Setup Team to get the VM setup completion. On completion, admin login credentials are sent to client SPOC via email.	Selected a sample of client request/Purchase orders and inspected the corresponding VM creation to determine that VM creation is as per client request and that the email is sent to the client as confirmation.	No exceptions noted
	Service Delivery team maintains a client escalation matrix for large enterprise customers.	Inspected the escalation matrix, with escalation levels, to determine that clients can contact Cyfuture using these contact points.	No exceptions noted
	Administrators for Vcenter console are integrated with Cyfuture Active Directory. Only authorised users can access Vcenter and accordingly provide services to clients through the VCenter	Enquired with IT Head that users on Vcenter are synchronised to the Active Directory.	No exceptions noted
	WHMCS Application (ITSM Tool) is used for providing client support for CloudOye cloud services. The application has role based access and only the setup and the support team have access to the client tickets.	Inspected the role based access for the Support application to determine that access to the application is based on defined roles.	No exceptions noted
	Administrators for Vcenter console are integrated with Cyfuture Active Directory. Only authorised users can access Vcenter and accordingly provide services to clients through the VCenter	Enquired with IT Head that users on Vcenter are synchronised to the Active Directory.	No exceptions noted
	Service deprovisioning is carried out after confirmation that all pending dues are paid up. Resources are deleted by the setup team	Enquired with Services team that clients are deactivated / deleted and their services are deprovisioned only after approval from CRM Team.	No exceptions noted
	Managed services provided by Cyfuture are documented as part of the client contract/purchase requests. Sometimes, clients may send an email for requesting for services, which may be acted upon by Cyfuture	Selected a sample of Purchase orders/ email requests and inspected the Requirements Documents to determine that the managed services opted by the clients are setup in the application based on client instructions	No exceptions noted Email requests from clients for new services or changes to services are also accepted.
Ref No	**Controls Implemented by Cyfuture**	**Test Procedures**	**Test Results**

	Services / Support team provides the managed services as per the client instructions. All instructions are received via tickets in the WHMCS ticketing tool.	Selected a sample of service requests tickets from the WHMCS application to determine that these are received as tickets and that the tickets are resolved within defined SLA.	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.