Cyfuture India Pvt. Ltd.

Independent Service Auditor's 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 and Availability and the Suitability of the Design and Operating Effectiveness of Controls

for the period, November 1, 2016 to April 30, 2017

(SOC 2 Type II Report)

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 November 1, 2016 to April 30, 2017"** (description) included in Section III and the suitability of the design and operating effectiveness of controls to meet the criteria for the security and availability principles set forth in TSP Section 100 Principles and Criteria, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Technical Practice Aids*), (applicable trust services criteria). Cyfuture has determined that Confidentiality, Processing Integrity and Privacy Trust Services Principles are not applicable to the services provided to its client, and is not included in the description. 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. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service organization's responsibilities
In Section II, Cyfuture has provided the accompanying assertion titled "Management of Cyfuture's Assertion." Cyfuture is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy and method of presentation of both the description and the assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, maintaining and documenting controls to meet the applicable trust services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria 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 fairly presented based on the description criteria and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period November 1, 2016 to April 30, 2017.

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
Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate of fail.

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 Cyfuture's system that was designed and implemented throughout the period November 1, 2016 to April 30, 2017.

b) the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 1, 2016 to April 30, 2017, and user entities applied the complementary user-entity controls contemplated in the design and operating effectiveness of Cyfuture's controls throughout the period November 1, 2016 to April 30, 2017.

c) The controls tested, which together with the complimentary user-entity controls referred to in the scope paragraph of the report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services principles criteria were met, operated effectively throughout the period November 1, 2016 to April 30, 2017.

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

Intended use
This report, including the description of tests of controls and results thereof in Section IV 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 November 1, 2016 to April 30, 2017; 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
- 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
(Membership Number - 0023943)

May 16, 2017
Mumbai, India

SECTION 2

MANAGEMENT OF CYFUTURE'S ASSERTION

May 16, 2017

We have prepared the attached description of Cyfuture India Pvt. Ltd.'s (Cyfuture) "**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 November 1, 2016 to April 30, 2017**" (the description) included in Section 3 of this report, based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.33–.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, or Privacy* (the description criteria).

The description is intended to provide users with information about the **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**, particularly system controls intended to meet the criteria for the Security, Availability, principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

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

a) The description fairly presents the **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 throughout the period November 1, 2016 to April 30, 2017** based on the following description criteria:

i. 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 the following:
      - Infrastructure - The physical and hardware components of a system (facilities and equipment).
      - Software - The programs used to manage active customers and data center badge access.

Cyfuture India Pvt. Ltd.
Authorised Signatory

- People - The personnel involved in the operation and use of a system (operators, users, and managers).
- Procedures - The automated and manual procedures involved in the operation of a system.
- Data- The information used and supported by a system (transaction streams, files, databases, and tables

3. The boundaries or aspects of the system covered by the description
4. How the system captures and addresses significant events and conditions
5. The process used to prepare and deliver reports and other information to user entities and other parties
6. For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system
7. Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore
8. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria
9. 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 description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c) The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Cyfuture India Pvt. Ltd.

Authorised Signatory

Anuj Bairathi

SECTION 3

DESCRIPTION OF CYFUTURE'S SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2016 TO APRIL 30, 2017

Description of Cyfuture India Pvt. Ltd.'s System throughout the period November 1, 2016 to April 30, 2017

Background and Overview of Services

Cyfuture India Pvt. 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	
• Data Centre activities including Co-Location Services, Security Services, Dedicated Hosting, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services.	
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 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 or more frequently, if required. 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.

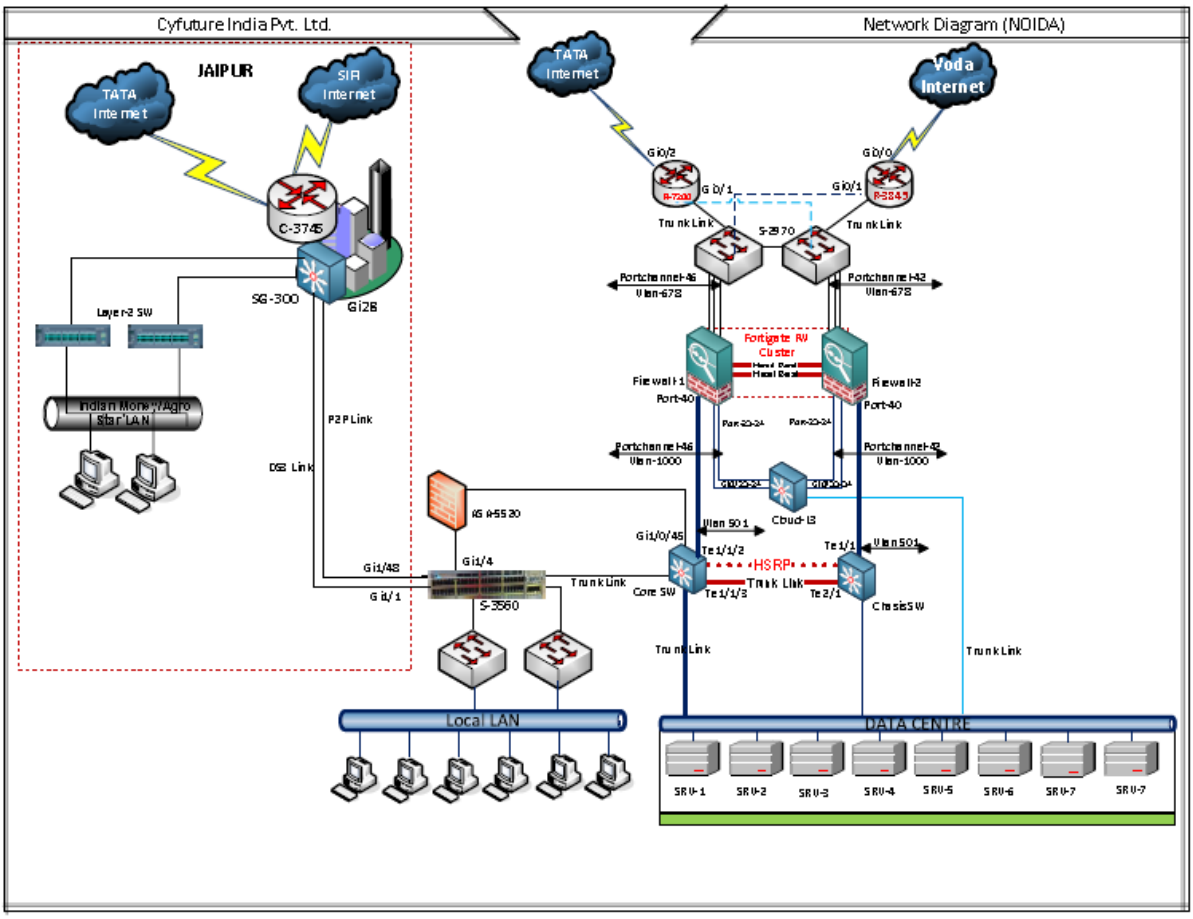
Electronic Mail (e-Mail)
Communication to Customer Organizations and project teams through e-Mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-Mail. E-Mail is also a means to draw attention of employees towards adherence to specific procedural 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 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.



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. 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 three 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 Data center / 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 repository .

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.

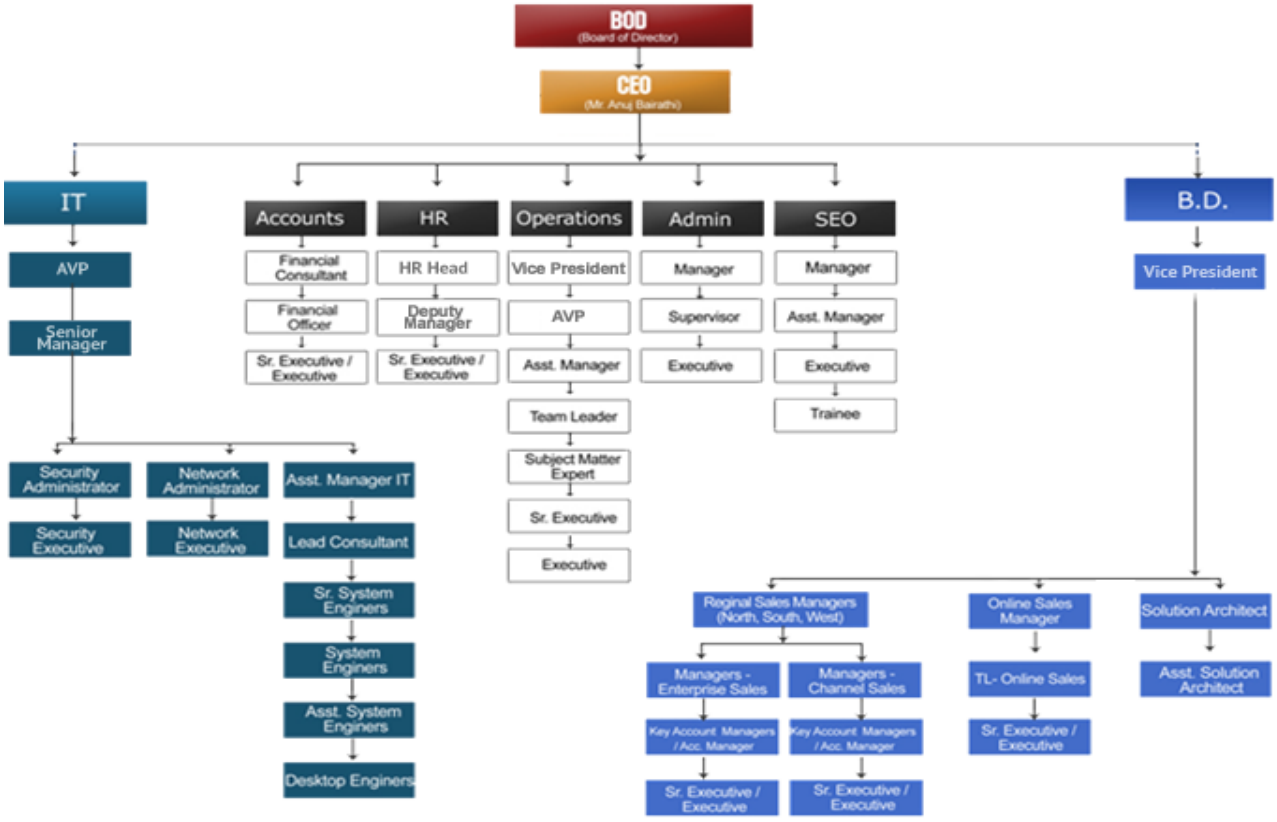
People

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.



Roles and Responsibilities

The following are the responsibilities of key roles.

Role of IT 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/ team 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

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.

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 access cards provided to them by Cyfuture \ on their termination of employment.

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 security and availability trust services criteria and Cyfuture related controls are included in section 4 of this report, “Independent Service Auditors 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.

- User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Cyfuture for processing.
- User Organizations are ultimately responsible to limit access to only those Cyfuture employee who require to perform their job responsibilities and that all users are assigned unique accounts.
- User Organizations are responsible for monitoring and reviewing their business processes.
- User Organizations are responsible for ensuring end customer privacy.
- User Entity should establish confidentiality procedures to ensure that all inputs have been authorized, have been accepted for processing, and are accounted for. Any missing or unaccounted source documents or input files have been identified and investigated. These processes require that exceptions be resolved within a specified time period.
- User Organizations are responsible for defining criteria for processing and rejecting items input into their systems.
- User Organizations are responsible for working with Cyfuture to resolve any input discrepancies or quality issues.
- User Organizations are responsible for reviewing the completeness and accuracy of the inputs / processing services performed by Cyfuture.
- User Organizations are responsible for working with Cyfuture to jointly establish service levels and revise the same based on changes in business conditions.
- User Organizations are responsible for initiating and implementing changes to the applications managed by User Organizations.

SECTION 4

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

Criteria Common to Security and Availability Principles

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC1.0	***Common Criteria Related to Organization and Management***				
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	The entity's organizational structure does not provide the necessary structure, resources, and information flow to manage security, availability, processing integrity and confidentiality activities.	Company has documented organization chart, authority, reporting lines and responsibilities for management of its information systems. As part of the its management processes and periodic corporate risk assessments, the management evaluates and identifies changes required to meet changing commitments & requirements.	Inspected the IS Team Structure, Org Structure and Responsibilities Authority to determine that i. Organization Chart is available ii Allocation of information security responsibility is documented	No exceptions noted.
			Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed	Inspected the Intranet to determine that i. Organization Chart is available ii Allocation of information security responsibility is documented	Exceptions noted The organisation charts were last updated in March 2015 and have not been updated since.
			Monthly management meetings are held by the CEO with various departments to understand the operations. Annual review meeting is held with the CEO and all HODs to discuss business, issues and other operational aspects. Minutes are maintained for the meetings held.	Inspected the monthly management meeting minutes and the Yearly HOD meeting minutes to determine that these meetings are held to discuss business operations.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Company has Information security related policies and procedures including Information Security Management Policy that describes information security processes, practices and organization.	Inspected IT Policies to determine that these are documented and approved by CISO	No exceptions noted.
			Information Security Policy & Procedures related to HR policies, information technology & network policies governing IT security, and Facilities related policies are reviewed by the Management at least annually and changes are approved by the CISO.	Inspected IT Policies and Procedures & Email Trail to determine that these are approved by CISO.	No exceptions noted.
		The roles and responsibilities of key managers are not sufficiently defined to permit proper oversight, management, and monitoring of security, availability, processing integrity and confidentiality activities.	Company has documented and defined roles and responsibilities in written job descriptions and communicated to managers and their supervisors. Allocation of information security responsibility is documented by the Company	Inspected job descriptions of IS team to confirm that Information Security activities are responsibility of IT. Inspected the roles and responsibilities document to determine that roles and responsibilities are defined.	No exceptions noted.
			The responsibility of AVP IT is assigned to CISO. Job description for CISO is documented.	Inspected job descriptions of CISO to confirm that Information Security activities are responsibility of IT. Inspected the 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 review process, for needed changes and where job duty changes are required necessary changes to these job descriptions are also made.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised on a yearly basis, if needed.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Reporting relationships and organizational structure do not permit effective senior management oversight of security, availability, processing integrity and confidentiality activities.	Management reviews reporting relationships and organizational structures periodically.	Inspected the organisation structure and reporting lines to determine that management reviews reporting relationships periodically.	Exceptions noted The organisation charts were last updated in March 2015 and have not been updated since.
		Personnel have not been assigned responsibility or have not been delegated insufficient authority to meet security, availability, processing integrity and confidentiality commitments and system requirements.	Roles and responsibilities are defined in written job descriptions.	Inspected the job descriptions, roles & responsibilities to determine that these are defined in written job descriptions.	No exceptions noted.
		Responsibility and accountability for privacy and data protection are not assigned to personnel with sufficient authority within the entity to manage risk and compliance.	AVP-IT (CISO) is responsible for privacy and data protection policies	Enquired with AVP-IT/CISO to determine that he is responsible for privacy and data protection policies	No exceptions noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Personnel have not been assigned responsibility or have been delegated insufficient authority to meet security, availability, processing integrity and confidentiality commitments and system requirements.	Company has documented and defined roles and responsibilities in written job descriptions and communicated to managers and their supervisors.	Inspected the job descriptions, roles & responsibilities to determine that these are defined in written job descriptions.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Job descriptions are reviewed on an annual basis as part of the review process for needed changes and updated if such changes are identified.	Enquired with the Manager HR that job descriptions are reviewed by management on a periodic basis for needed changes and updated if such changes are identified.	No exceptions noted.
		Responsibility and accountability for privacy and data protection controls are not assigned to personnel with sufficient authority within the entity to manage risk and compliance.	The company does not maintain any privacy / PII information.	Enquired with CISO that the entity does not maintain any privacy / PII information	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, processing integrity and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	Newly hired, newly assigned, or transferred personnel do not have sufficient knowledge and experience to perform their responsibilities.	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.	Inspected the Job descriptions document and determined that the requirements for each role in terms of skills, qualifications and experience are documented in the Competency Matrix and candidates' abilities to meet these requirements are evaluated as part of the hiring process. Inspected a sample of positions from org chart and determined that - i. if positions have formal job descriptions ii. If roles & responsibilities are defined iii. If JDs have job requirements (in terms of skills, knowledge, abilities, qualifications and experience) Selected a sample of new joiners and inspected the personnel files for the competency checks such as interviews and written tests.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Personnel do not have sufficient periodic training to perform their responsibilities.	During the interviews, the Interviewer uses the Competency Matrix and the job description for evaluation. The JD highlights the technical skills required. The Interview rating sheet along with the feedback report is sent to HR for final approval and selection. Assessment tests are carried out for certain senior technical positions where it is difficult to assess the candidate based on the interview. These assessment tests are forwarded to the Hiring Manager.	Inspected a sample and determined that competency tests such as rounds of interviews i.e. Interview Rating Sheet and Online Tests. Inspected the personnel files and Online Technical Assessment Test for employees who joined during the period being audited and determined that competency checks such as interviews and Online tests i.e. "Reasoning, Maths and English" were conducted and results considered while selection.	No exceptions noted.
			Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position. Managers for new employees prepare training plan based on the project and work experience. At the end of training Manager will record completion. The induction training given by HR includes Information Security training. This training includes the HR, and IT Policies are explained. Management has established a training process - Development and Training Needs which has details of Recommended Training Area and Priority which is filled by the Department head. Priority is on a 3-pointer scale.	Inspected the Induction Training Feedback forms of HR that all new employees undergo induction training and the CISO conducts a refresher training for all employees from time to time. Inspected the Competency Matrix sheet. Inspected New Hire Induction Training Presentation to ensure that 1) it includes policies on Security. 2) it includes information concerning Password Management and Clean Desk and on all IT Security Policy. Reviewed training records for sample of new employees during the audit period.	No exceptions noted
			HR Dept maintains a training calendar that is used to monitor planned and budgeted trainings during the year.	Inspected the Training Calendar to determine that the trainings that are planned and budgeted are reviewed regularly and used for future training needs	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Technical tools and knowledge resources are insufficient to perform assigned tasks.	Management evaluates the need for additional resources in order to achieve business objectives, as and when needs arise.	Inspected the Candidate Requisition Form filled by the HOD to determine that HR budgets and resource requirements are fulfilled.	No exceptions noted
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Personnel did not comply with the entity's requirements for conduct.	There is a contractual mechanism for customer feedback, complaints or issues though the project management teams	Inspected the mailers sent to customers and Customer Management System for feedback and complaints.	No exceptions noted
			All new employees get an appointment letter with Confidentiality clause which they have to read and sign. This clause has details of confidentiality terms. All employees additionally sign Security Acceptable Use Agreement.	Inspected personnel file for the sample of employees to determine if Appointment letter and Security acceptable use agreement have been properly signed.	No exceptions noted
		A candidate with a background considered to be unacceptable by management of the entity is hired by the entity.	HR reference checks are conducted post Joining and completed within a maximum period of 60 days. HR verifies the Past Employment record, qualification records, identity checks upon joining. HR Verifies the from Previous Employer of the employee. For special positions, i.e. Higher Positions and Sales positions Personal Contact Verifications are also conducted.	Inspected the personnel files for a sample of new joiners to determine document review by HR and reference checks carried out for new joiners. Enquired with the HR Head that third party background checks including criminal records and address checks are not carried out.	No exceptions noted
			The entity has established standards and guidelines for personnel ethical behavior as part of the Employee Handbook.	Inspected the Intranet site and to determine that the entity has established standards and guidelines for personnel ethical behavior.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC2.0	***Common Criteria Related to Communications***				
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	External users misuse the system due to their failure to understand its scope, purpose, and design.	System boundaries in terms of logical, physical boundaries, org structure, list of processes, system components are documented in the ISMS Scoping Document.	Inspected ISMS Scope document to determine that the Company has defined system boundaries. Inspected the screenshot for the Intranet Site where policies are uploaded and available to all users.	No Exceptions Noted
			Customer responsibilities and appropriate system descriptions are provided in client contracts. Policy and procedures documents for information security, system usage and HR related security are available on Intranet Site and is made available to all employees. Dos and Don'ts of system usage are provided in the induction and refresher training to all employees.	Inspected policies maintained at Intranet Site accessible to all employees and verified that policies related to information security, HR and systems are provided on Intranet site and all employees have access to it. Inspected Client contracts for terms related to brief requirements of the system. Inspected training deck for the training that provided to all employees and determined that appropriate instruction on proper system usage provided to all employees.	No Exceptions Noted
		Internal users are unaware of key organization and system support functions, processes, roles, and responsibilities.	Entity's Organisation Structure, Process and organizational roles and responsibilities are part of ISMS documentation. Changes to the ISMS documentation are approved by AVP-IT prior to implementation.	Inspected the Roles and Responsibilities document which includes ISMS related roles and responsibilities defined. ISMS documentation is at the shared drive location so that it is available to all the employees.	No Exceptions Noted
		External users fail to address risks for which they are responsible that arise outside the boundaries of the system.	System requirement for client communication are documented as part of MSAs. System Boundaries are shared with the customers if it is required.	Inspected the system description document to determine that it defines system components.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC2.2	The entity's security, availability, processing integrity and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Internal and external users misunderstand the capabilities of the system in providing for security, availability, processing integrity and confidentiality and take actions based on the misunderstanding.	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts and service agreements.	Inspected sample of Client SOW and determined that terms related to delivery of services are covered.	No exceptions noted
			Company security related policies are communicated to employees through Information Security awareness training as a part of induction for new employees. Company Security related policies are at shared location so that the latest policy is available to all employees. The induction training given by HR includes security training. In this training the HR, Clean Desk, No Unattended System, Secure Password, Wear ID Card, First Aid, Fire Safety, No Tailgating Allowed, No Personal Use and security policies are explained.	Inspected the Intranet that includes slides on information security related aspects to determine that information security awareness trainings are carried out for new joiners.	No exceptions noted
		The entity fails to meet its commitments due to lack of understanding on the part of personnel responsible for providing the service.	Company security related policies are communicated to employees through Information Security awareness training as a part of induction for new employees. Company Security related policies are at shared location so that the latest policy is available to all employees. The induction training given by HR includes security training. In this training the HR, Clean Desk, No Unattended System, Secure Password, Wear ID Card, First Aid, Fire Safety, No Tailgating Allowed, No Personal Use and security policies are explained.	Inspected the Training Attendance sheet and Intranet site that includes policies on information security related aspects to determine that information security awareness trainings are carried out for new joiners.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Entity's policies relating to security, confidentiality is reviewed with new employees as part of their orientation, and the key elements of the policies and their impact on the employee are discussed.	Inspected Intranet website to ensure that 1. Policies on Security are conveyed to employees. 2. Training Records for induction are mapped for all new hires during the audit period Enquired with HR to determine the new joiners Induction is given through Intranet Website.	No exceptions noted
			Personnel are required to read entity's code of conduct and the statement of security and confidentiality practices upon hire.	Selected a sample of new employees and inspected the signed appointment letter to determine that Confidentiality agreement is signed as part of appointment letter. Inspected the Intranet website to determine that Code of conduct policy is part of Induction training of employees at the time of joining the organization.	No exceptions noted
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	The system fails to function as designed due to internal users' failure to meet with their responsibilities.	Company security related policies are communicated to employees through Information Security awareness training as a part of induction for new employees. Policy and procedures documents for significant processes that address system requirements are available on shared Intranet website.	Inspected the Intranet website to determine that IT security policies are published on Corporate Intranet. Enquired with HR to determine that Induction training is given through Intranet website	No exceptions noted
			Company has a skills training and competency program and annual training plan are developed on Employee Engagement Training Calendar based on training needs to ensure availability of relevant skills. Training needs are identified during performance appraisals and training plan prepared.	Inspected the Competency Matrix and Employee Training Calendar to determine that existing employees undergo several types of trainings and engagement as part of their technical and non-technical skills.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Personnel are required to read the entity's code of conduct and the statement of security and confidentiality practices upon hire.	Selected a sample of new employees and inspected the signed appointment letter to determine that Confidentiality agreement is signed as part of appointment letter. Inspected the Intranet website to determine that Code of conduct policy is part of Induction training of employees at the time of joining the organization.	No exceptions noted
		The system fails to function as designed due to external users' failure to meet their responsibilities.	Customer responsibilities are described in client contracts	Inspected a sample of client contracts to determine explicit responsibilities of customer	No exceptions noted
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, processing integrity and confidentiality of the system, is provided to personnel to carry out their responsibilities.	Controls fail to function as designed or operate effectively due to misunderstanding on the part of personnel responsible for implementing and performing those controls resulting in failure to achieve security, availability, processing integrity and confidentiality commitments and system requirements.	Policy and procedures documents for information security, system usage and HR related security are available on Intranet website and is made available to all employees.	Inspected policies maintained at Intranet Website accessible to all employees and verified that policies related to information security, HR and systems are provided on a shared folder and all employees have access to it.	No exceptions noted
CC2.5	Internal and external users have been provided with information on how to report security, availability, processing integrity and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	System anomalies are detected by internal or external users but the failures are not reported to appropriate personnel resulting in the system failing to achieve its security, availability, processing integrity and confidentiality commitments and system requirements.	Customer responsibilities are described in the customer contracts and in system documentation	Inspected a sample of customer SOW for the roles and responsibilities and determined that roles and responsibilities are clearly defined. .	No exceptions noted
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, processing integrity and confidentiality are communicated to those users in a timely manner.	Internal and external users misunderstand changes in system capabilities or their responsibilities in providing for security, availability, processing integrity and confidentiality due to system changes and take actions based on the misunderstanding.	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management policy. External Client communication is carried out on a timely manner by the Project Manager using a standard client specific escalation matrix.	Inspected the change management policy to determine that it is documented. Inspected a sample of client escalation matrix to determine that a defined client escalation process is documented and used for client communications.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Changes to software are authorized by the concerned department head or project head before implementation. Changes to system infrastructure are authorised by Sr Manager IDC/CISO	Selected a sample of system changes and inspected the change request to determine that the change is approved by Sr Manager IDC/CISO and also that it is entered in the change request log.	No exceptions noted
		Internal and external users are not aware of system changes.	A change request is maintained to track the changes.	Inspected the change requests to determine that change requests are made to track the changes. Selected a sample of system changes and inspected the change request to determine that the change is approved by Head - IT Infra and also that it is entered in the change request log.	No exceptions noted
			All relevant system users are informed about the changes through email system.	Inspected a sample of client SOW and determined that the communication and escalation plan are agreed with clients and incorporated in the SOW. Inspected a sample of requests of changes to systems for compliance with the company's change management policy.	No exceptions noted
		Changes in roles and responsibilities and changes to key personnel are not communicated to internal and external users in a timely manner.	New employees hired at senior levels are communicated to stakeholders by Head HR / AVP-IT through Email	Enquired through AVP-IT that Senior level employee joinees are communicated to clients through email.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***				
CC3.1	The entity (1) identifies potential threats that could impair system security, availability, processing integrity and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	Not all system components are included in the risk management process resulting in a failure to identify and mitigate or accept risks.	The IT department maintains an up-to-date listing of all software and the respective level, version, and patches that have been applied. A patch management script is run periodically to automatically update user systems. List of all hardware is maintained as part of asset register.	Inspected the software list and hardware list maintained by the IT to ensure that it is up to date. Inspected WSUS report to ensure that script runs on weekly basis for updating patches.	No exceptions noted
		Not all changes that significantly affect the system are identified resulting in a failure to correctly reassess related risks.	During the risk assessment and management process, CISO along with the Department heads updates Asset Inventory, Threats, Vulnerabilities, risks that threaten the achievement of business objectives annually	Inspected Risk Assessment performed during the period to determine updation of asset inventory, threats and risks and to determine that risk assessment is carried out atleast on an annual basis and approved by CEO.	Exceptions noted Risk Assessment carried out by the Company does not cover all information assets.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Personnel involved in the risk management process do not have sufficient information to evaluate risks and the tolerance of the entity for those risks.	The entity has documented Risk Assessment Process which states security risks of information assets in the company have been identified by respective asset owners and IT, risks are analyzed and appropriate controls identified to commensurate with and justified by the assessed risks. Risk Management policy identifies risk tolerances above which risk will need to be treated.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process. Inspected Departmental risk register and determined that information assets were identified, threats & vulnerabilities are identified, risks were evaluated, controls documented and gaps identified.	Exceptions noted Risk Assessment carried out by the Company does not cover all information assets.
		One or more internal or external risks that are significant threaten the achievement of security, availability, processing integrity and confidentiality commitments, and system requirements that can be addressed by security controls, are not identified.	Risk assessments are reviewed atleast on an annual basis for each department and risks covered include active risks as well as emerging risks. During the risk assessment owners identifies changes to objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential risks to system objectives. Risk Assessments are prepared by Asst Manager IT, verified by Sr Manager IDC and approved by CISO /CEO	Inspected the email to CEO requesting for approval risk assessment and other agenda items to determined that i. Risks were verified by Sr Manager IDC and approved by CISO /CEO ii. risks were evaluated using a defined; risk rating iv, risk treatment plans were defined and tracked.	No exceptions noted
			Risk is conducted both at asset and organisation level taking into consideration Probability, Harm, chances of detection. Prioritization is based upon risk rating. Risk assessment is performed on an annual basis.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No exceptions noted
			The internal audit, as part of ISO 27001, is carried out periodically. Results and recommendations for improvement are discussed with Top Management and CEO during Management Review Meetings.	Inspected the latest internal audit reports carried out under ISO 27001 to determine that periodic internal audits are carried out. Inspected a sample of project level audit reports for a sample of departments to determine that audits are performed.	Exceptions noted Internal audits scheduled for August 2016 were not carried out. No internal audit reports were available for these audits.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
				Inspected a copy of the email sent by ISG to CEO to determine that the results are communicated to the CEO.	
		Changes that are not properly identified create risks due to the failure of those changes to undergo the risk management process.	During the annual risk assessment and management process, CISO along with other Department heads reviews and identifies emerging risks due to changes in business, regulatory, and technological environment.	Inspected the most recent email and determined that i. Risks were discussed in the meeting ii. current risks as well as emerging risks due to changes such as environment, technology, business objectives were considered iii. risks were evaluated using a defined; risk rating iv, risk treatment plans were defined and tracked.	Exceptions noted Annual management meeting minutes do not contain evidence that risk assessments were discussed and approved.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.	Controls and mitigation strategies selected, developed, and deployed do not adequately mitigate risk.	Vulnerability assessment & penetration tests are performed regularly	Inspected the latest vulnerability assessment/penetration test report performed internally and determined that vulnerabilities were closed.	No exceptions noted
			The internal audit, as part of ISO 27001, is carried out periodically. Project audits are randomly selected and carried out during ISO 9001 Internal Audits. Results and recommendations for improvement are reported to Department Heads and to the AVP-IT.	Inspected the latest internal audit reports carried out under ISO 27001 to determine that periodic internal audits are carried out. Inspected the latest internal audit reports of ISO 9001 to determine that periodic internal audits are carried out.	Exceptions noted Internal audits scheduled for August 2016 were not carried out. No internal audit reports were available for these audits.
			Business and system recovery plans are tested annually.	Inspected the most recent BCP / DR testing report and determined that (i) testing was as per BCP strategy ii. Reports are discussed and approved by the AVP-IT iii. actions from test report are complete.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Penetration test are carried out randomly and assessment of vulnerabilities are performed annually internally by the IT team. Based on the tests performed, the IT team provides report of the observations to AVP-IT which mentions the vulnerabilities, their rating and when they need to be fixed. The action plans are monitored by AVP-IT	Inspected the most recent VA /PT reports to determine that penetration testing and vulnerability assessments are carried out and actions from VA report have been completed.	No exceptions noted
			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
		Deployed controls and mitigation strategies create new risks that fail to be assessed.	During the annual risk assessment and management process, CISO /AVP-IT reviews and identifies emerging risks due to changes in business, regulatory, and technological environment.	Inspected the most recent email and determined that i. Risks were discussed in the meeting ii. current risks as well as emerging risks due to changes such as environment, technology, business objectives were considered iii. risks were evaluated using a defined; risk rating iv, risk treatment plans were defined and tracked.	Exceptions noted Annual management meeting minutes do not contain evidence that risk assessments were discussed and approved.
CC4.0	***Common Criteria Related to Monitoring of Controls***				
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Controls are not suitably designed, configured in accordance with established policies, or operating in an effective manner, resulting in a system that does not meet commitments and system requirements.	The internal audit, as part of ISO 27001, is carried out periodically. Project audits are randomly selected and carried out during ISO 9001 Internal Audits. Results and recommendations for improvement are reported to Department Heads and to the AVP-IT.	Inspected the latest internal audit reports carried out under ISO 27001 to determine that periodic internal audits are carried out. Inspected the latest internal audit reports of ISO 9001 to determine that periodic internal audits are carried out.	Exceptions noted Internal audits scheduled for August 2016 were not carried out. No internal audit reports were available for these audits.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Monthly management meetings are held by the CEO with various departments to understand the operations. Minutes are maintained for the meetings held.	Inspected the Monthly management meeting minutes to determine that these meetings are held to discuss business operations.	No exceptions noted
			Penetration test are carried out randomly and assessment of vulnerabilities are performed annually internally by the IT team. Based on the tests performed, the IT team provides report of the observations to AVP-IT which mentions the vulnerabilities, their rating and when they need to be fixed. The action plans are monitored by AVP-IT	Inspected the most recent VA /PT reports to determine that penetration testing and vulnerability assessments are carried out and actions from VA report have been completed.	No exceptions noted
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***				
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Not all system infrastructure or system components are protected by logical access security measures resulting in unauthorized modification or use.	Company has documented policy for access control for its systems. The IT Asset Management policy describes the asset acquisition and threat & risk assessment process that include requirements for configuration & access control procedure.	Inspected the access control policy and procedure and determined that management has documented and approved procedures for controlling access to entity system. Inspected the asset management policy for adequacy of acquisition, deployment controls.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Penetration test are carried out randomly and assessment of vulnerabilities are performed annually internally by the IT team. Based on the tests performed, the IT team provides report of the observations to AVP-IT which mentions the vulnerabilities, their rating and when they need to be fixed. The action plans are monitored by AVP-IT	Inspected the most recent VA /PT reports to determine that penetration testing and vulnerability assessments are carried out and actions from VA report have been completed.	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 and periodically evaluate access for assets under their custody.	Inspected the asset register and determined that assets, their owners, users are clearly documented and 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.	No exceptions noted
		Logical access security measures do not identify or authenticate internal and external users prior to permitting access to IT components.	Infrastructure components and software are configured to use the Windows security using Windows Active Directory access control.	Inspected access control procedure and Windows Active Directory and determined that authentication to systems access is through Domain Controller.	No exceptions noted
		Logical access security measures do not provide for the segregation of duties required by the system design.	A role based security process has been defined with in Active Directory and roles based on job requirements.	Inspected the access control policy and Active Directory. Inspected the list of users created in Active Directory along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access.	No exceptions noted
			Shared directory on company network use Domain Controller for role based authentication. Work on client processes is carried out on applications on client networks after logging in to their systems.	Inspected the list of users created under Domain Controller along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access. Enquired with IT staff about access to	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Client control access to & configuration of their systems.	client processes and found that access to it is controlled by client's access control mechanism.	
		Logical access security measures do not restrict access to system configurations, privileged functionality, master passwords, powerful utilities, security devices, and other high risk resources.	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by the Team Leads or Project Managers.	Inspected the email for higher/Privilege access request which is approved by the Team Lead or Project Manager.	No exceptions noted
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Valid user identities are granted to unauthorized persons.	Before a new employee joins the organization, the HR team updates the details of the new joinees through email along with their details includes Name, Designation, Team details and computer for the new individual. Based on this Email, the IT team creates logical access and the HR team creates the biometric access. Employee user IDs are removed from Active Directory list and biometric on the last date of employment manually based on the No Dues Form. Access on client systems is removed by IT Team on request by HR informing them about the exiting employee.	Enquired from HR and determined that biometric access is issued by HR based on the onboarding details. Inspected biometric access for a sample of new joiners for their card issue. Inspected the email from HR to IT to determine that the new joiner details are populated on the basis of which access are created.	No exceptions noted
			Any privileged access is created or modified by IT Infrastructure Team only based on an approval from the Team Lead or Project Manager.	Inspected the email for higher/Privilege access request which is approved by the Team Lead or Project Manager.	No exceptions noted
			Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees and found they are not allowed.	No exceptions noted
		A user that is no longer authorized continues to access system resources.	The leaving employee is supposed to get the clearance form signed from HR for Biometric deactivation, IT for systems access revocation on the last working day.	Inspected the clearance form checklist and determined that the access is removed from IT Servers and Biometric the same day when the employee has last working day.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees and found they are not allowed.	No exceptions noted
			Account sharing does not happen. Employees are prohibited from sharing IDs. This is included in the induction training.	Inspected Access Control list on Active Directory and determined there are no generic IDs which can be used as a shared ID. Enquired with IT staff about shared IDs. Enquired with a sample of employees about ID sharing.	No exceptions noted
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Internal and external users are not identified when accessing information system components.	Company has documented policy for access control for its systems. There are No External Users. All access to company system is through Active Directory authentication based sign in requiring combination of unique user ID and a password. The Shared Server Login is maintained Active Directory access list.	Enquired with AVP-IT that there are no External Users. Inspected the access control policy defined under Acceptable use Policy. Inspected the list of users created under Active Directory along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access.	No exceptions noted
		Valid user identities are assumed by an unauthorized person to access the system.	Entity users are configured on Active Directory for authentication and controlling user access management for their directory.	Inspected the list of users created under Active Directory along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access.	No exceptions noted
		External user access credentials are compromised, allowing an unauthorized person to perform activities reserved for authorized persons.	The company does not have any external facing applications.	Enquired with the head IT that there are no External Users.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Valid internal or external users obtain unauthorized access to the system resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	Role based security has been implemented with the help of Active Directory on shared directory. All users working on client processes gave the same default access. Users are given access to folders on file servers containing work instruction and associated documents. Team Leads and management have higher access. Users have been divided into several user groups in the domain.	Inspected the access control policy defined under Acceptable use Policy. Inspected the list of users created under Active Directory along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access.	No exceptions noted
		Access granted through the provisioning process compromises segregation of duties or increases the risk of intentional malicious acts or error.	Role based security has been implemented with the help of Active Directory on shared directory. All users working on client processes gave the same default access. Users are given access to folders on file servers containing work instruction and associated documents. Team Leads and management have higher access. Users have been divided into several user groups in the domain.	Inspected the access control policy defined under Acceptable use Policy. Inspected the list of users created under Active Directory along with the roles and determined that the access on shared folder is also controlled through Domain Controller along with read and write access.	No exceptions noted
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Unauthorized persons gain physical access to system components resulting in damage to components (including threats to personnel), fraudulent or erroneous processing, unauthorized logical access, or compromise of information.	Entry to the premises is restricted to authorized personnel A biometric based physical access control system has been implemented to secure the perimeter of office premises. Only employees and approved contract employees are given these cards.	Observed that the entry to premises is restricted by biometric access. Physically Observed the Biometric based physical access control system used for entering & exiting the office as well as for sensitive rooms (data center & UPS room). During the audit, observed users entering and exiting only after gaining access through the biometric access.	No exceptions noted
			Physical access to office premises is monitored through CCTV installed at key points within the premises. CCTV recordings are saved for 30 days.	Observed that the CCTV are located across the premises and that the CCTV are working. Observed that HR department monitors the CCTV screens in the HR room, showing images of all cameras	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			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
			ID cards are created by the human resources department during the employee orientation period after all required background verification are completed. ID cards do not have physical access.	Selected a sample of new and terminated employees and inspected that the access rights were granted or deactivated in the biometric system.	No exceptions noted
			Physical access to sensitive areas is granted only to Tech IT Team and CISO. Access to restricted zone is given against written request by the CISO.	Inquired with Head IT that access to Server room and other sensitive areas is granted only to IT team (Tech team). Physically observed the server room biometric reader user list and the related application to determine that only the IT team and CISO. Physically observed the server room biometric reader user list to determine that only the IT team had access to the server room for Office 198 (Second Office).	No exceptions noted
			All visitors have to enter all details in the visitor register.	Inspected the visitor register for sample dates & visitor badges used by visitors.	No exceptions noted
			Visitor badges are for identification purposes only and do not permit access to any secured areas of 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
		Formerly appropriate physical access becomes inappropriate due to changes in user job responsibilities or system changes, resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	Upon the last day of employment, the human resources sends biometric access termination request for employees for whom it is the last day of employment and whose access is to be removed and their pass cards to be disabled.	Inspected the biometric deactivation and biometric log for a sample of exited employees to determine that deactivation was carried out in a timely manner	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		A formerly authorized person continues to access system resources after that person is no longer authorized.	Upon the last day of employment, the human resources sends biometric access termination request for employees for whom it is the last day of employment and whose access is to be removed and their pass cards to be disabled.	Inspected the biometric deactivation and biometric log for a sample of exited employees to determine that deactivation was carried out in a timely manner	No exceptions noted
		A user obtains the identification credentials and authentication credentials of a formerly authorized person and uses them to gain unauthorized access to the system.	Upon the last day of employment, the human resources deactivate physical access in Biometric for whom it is the last day of employment and whose access is to be removed and their pass cards to be disabled.	Inspected the sample list of terminated employees & the access revocation done by HR. Inspected the biometric system activation / deactivation log to ensure that access of terminated employees have been revoked.	No exceptions noted
			Employees are required to return their ID cards on the last day, and all ID badges are disabled and employees physically escorted from the office.	Inspected the sample list of terminated employees & the access revocation done by HR. Inspected the biometric system activation / deactivation log to ensure that access of terminated employees have been revoked.	No exceptions noted
			The sharing of access badges and tailgating are prohibited by policy.	Physically Observed the access badges are not shared & no tailgating observed.	No exceptions noted
			There is a security desk at the office entry manned by a security guard. There is a visitor register at the security desk where all visitors including contractors have to make an entry before entering the office.	Physically observed the security staff at the reception who ensure that the all visitors make an entry in the visitor book before entering the office.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC5.6	Logical access security measures have been implemented to protect against security, availability, processing integrity and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Threats to the system are obtained through external points of connectivity.	Company has documented policy & procedure for access control. Access to local system is controlled through Windows Active Directory based authentication and requires user ID and complex password. Access to Project files and Individual directories on shared Server system is controlled through Domain Controller based authentication and requires user ID and complex password. Access to client applications and data in client environment is managed by the clients.	Inspected the access control policy and determined that Access to local system is controlled through Active Directory based authentication and requires user ID and complex password. Inspected the shared server authentication and determined that access to Project files and Individual directories on shared Server system is controlled through Domain Controller based authentication and requires user ID and complex password.	No exceptions noted
			External points of connectivity at office network are protected by software based Fortigate 1500D firewall UTM. All data traffic to company network passes through the firewall. This firewall provides unified threat management services web filtering and inbound and out bound traffic filtering.	Inspected the screenshots of firewall to determine that firewall has been installed in the network. Inspected firewall console screens containing rules about ports, incoming connection types, and type of traffic and determined that configuration is in compliance with the policy.	No exceptions noted
			Incoming connection are rejected from blacklisted IPs in the firewall.	Inspected incoming connection configuration in the firewall and determined that IPs are blacklisted 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 to the company policy and hardening standards.	No exceptions noted
		Authorized connections to the system are compromised and used to gain unauthorized access to the system.	Firewall rules restricts the incoming IPs through blacklisting, the types of activities and service requests that can be performed from external connections. Access to modify firewall rules is restricted by management.	Inspected firewall console screens containing rules about ports, incoming connection types, blacklisted IPs and type of traffic and determined that is complies with the to the company policy and hardening standards.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Nonpublic information is disclosed during transmission over public communication paths.	All network access is through VPN configured on Firewall.	Inspected the firewall configuration and determined that the Users are setup on firewall for VPN Access.	No exceptions noted
		Removable media (for example, USB drives, DVDs, or tapes) are lost, intercepted, or copied during physical movement between locations.	Use of removable media is prohibited by policy except when authorized by management	Inspected McAfee antivirus console to determine that USB drives and other removable drives are disabled. Observed a sample of computers and determined that USB sticks are not read using Active Directory Group Policy. Inspected the training deck and determined that employees are informed about policy on USB drive	No exceptions noted
		Removable media used to make unauthorized copies of software or data are taken beyond the boundaries of the system.	Use of removable media is prohibited by policy except when authorized by management	Inspected Active Directory Group Policy to determine that USB drives and other removable drives are disabled. Observed a sample of computers and determined that USB sticks are not read. Inspected the training deck and determined that employees are informed about policy on USB drive	No exceptions noted
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Malicious or otherwise unauthorized code is used to intentionally or unintentionally compromise logical access controls or system functionality through data transmission, removable media, and portable or mobile devices.	Incoming Network Traffic including malicious code or attack on Server is blocked by Fortigate 1500D Firewall The Firewall is configured with its own Anti-Virus Program.	Inspected Network Diagram and Physical Network and found Fortigate 1500D Firewall installed where the ISPs land. Inspected the IT Information Security Policies to determine that antivirus policies are documented. Inspected the Fortigate 1500D/UTM screenshot for configurations relating to Antivirus protection for its own server.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			McAfee antivirus software is installed on workstations, laptops, and servers (except Linux servers). This system provides antivirus system 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 console for configuration details relating to antivirus policies.	No exceptions noted.
			The ability to install software on workstations and laptops is restricted to IT support personnel through Firewall level.	Inspected the IT Information Security Policies and determined that employees are not allowed to install any software or download software on their workstation without approval. Physically observed a sample of user machines to determine that admin access is disabled for the users.	No exceptions noted.
			Signature files are updated daily. McAfee console provides compliance reports about non-updated machines. IT team monitors McAfee console on a daily basis. McAfee console provides information about malware threats, policy violations, endpoints and trends.	Inspected a sample of desktops and servers and determined that antivirus is installed and signature files were updated. 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. Automated antivirus alerts are configured on McAfee and as such any malware /virus attack information is received by the IT Team.	No Exceptions noted.
			Any viruses discovered are reported to the IT Infra team either by the antivirus system (as Antivirus console) or by the affected employees. The affected employee logs a ticket in WHMCS. Immediate actions are taken and incident management plan is initiated for major outbreaks. McAfee application sends alerts to all users notifying them of a potential virus threat.	Inspected the IT Info Security Policy for antivirus procedures.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Business owners obtain and install applications without proper authorization.	The ability to install software on workstations and laptops is restricted to IT support personnel through AD Group Policy.	Inspected the IT Info Security Policy and determined that employees are not allowed to install any software or download software on their workstation without approval. Physically observed a sample of user machines to determine that admin access is disabled for the users.	No exceptions noted.
CC6.0	***Common Criteria Related to System Operations***				
CC6.1	Vulnerabilities of system components to security, availability, processing integrity and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	Inspected the Hardening procedures for Servers to determine that hardening standards are documented.	No exceptions noted.
			IT team receive requests for support through Internal IT Tool WHMCS and emails, which may include requests to McAfee, user passwords or notify IT team about incidents.	Inspected a sample of tickets in online tool WHMCS and determined that IT Incidents are being logged by users and resolved by the IT Infrastructure team.	No exceptions noted.
			Penetration test are carried out randomly basis and assessment of vulnerabilities are performed annually internally by the IT team. Based on the tests performed, the IT team provides report of the observations to CISO which mentions the vulnerabilities, their rating and when they need to be fixed. The action plans are monitored by External Auditors	Inspected the most recent VA /PT reports to determine that penetration testing and vulnerability assessments are carried out and actions from VA report have been completed.	No exceptions noted.

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Security or other system configuration information is corrupted or otherwise destroyed, preventing the system from functioning as designed.	Backups are done as per policy and transferred offsite to Jaipur DR location through dedicated and secured P2P Link only for the Organizations own Internal Server and data of those clients who have opted for a Backup Service.	Enquired with Head IT on the backup procedures to determine that backups are done locally and transferred to Jaipur Offsite DR location through dedicated and secured P2P Link only for the Organizations own Internal Server and for Clients who have opted for a Backup Service.	No exceptions noted.
CC6.2	Security, availability, processing integrity, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Breaches and incidents are not identified, prioritized, or evaluated for effects.	IT Team follows defined protocols as described in Incident Management Procedure document for evaluating reported events. CISO/AVP-IT monitors Security related events resolution.	Inspected Incident Management Procedures to determine inclusion of documented procedure for identifying incidents	No exceptions noted
		Corrective measures to address breaches and incidents are not implemented in a timely manner.	IT personnel follow defined protocols for evaluating reported events. Security related events are assigned to the CISO for evaluation. Incident Reporting form is used to track logged incidents and their timely closure.	Inspected Incident Management Procedures to determine inclusion of documented procedure for identifying incidents. Inspected the Incident Reporting form to determine that incidents are logged and action taken appropriately.	No exceptions noted
		Corrective measures are not effective or sufficient.	All security incidents are also reviewed and monitored by CISO. Corrective and preventive actions are completed for incidents.	Inspected the incident handling procedure document for identification and escalation of potential security related incidents/Events/breaches. Inspected incident reporting sheet for a sample of incidents from incident log and examined the incident closure and actions Taken.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
			As per the incident management procedure, lessons learnt and Identification of Security Improvements shall be prepared and reviewed.	Inspected Incident Management Procedure and Incident Forms and determined that lessons learnt and Identification of Security Improvements are prepared and reviewed for all Incidents.	No exceptions noted
		Lack of compliance with policies and procedures is not addressed through sanctions or remedial actions, resulting in increased noncompliance in the future.	Incident logs are monitored and evaluated by the CISO. All incidents are tracked by CISO until resolved.	Inspected the security incident reporting form & the corrective actions taken to verify that action was taken on the security incidents	No exceptions noted
			HR policies include code of conduct and disciplinary policy for employee misconduct.	Inspected the Intranet Portal for Code of Conduct and Disciplinary Policy	No exceptions noted
		Breaches and incidents recur because preventive measures are not implemented after a previous event.	Change management requests are opened for events that require permanent fixes.	Inspected Incident Management Procedure and determined that Learning from Incidents and identification of Security Improvements is done with each incident that require permanent fixes.	No exceptions noted
CC7.0	***Common Criteria Related to Change Management***				
CC7.1	The entity's commitments and system requirements, as they relate to security, availability, processing integrity and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Commitments and system requirements are not addressed at one or more points during the system development lifecycle, resulting in a system that does not meet commitments and system requirements.	Entity has documented its change management and approval processes as part of Information Security Policies. The scope of Change management process includes the management of any installation or alteration to hardware, network and system or application software.	Inspected Change Management Policy document and determined that the management of any installation or alteration to hardware, network and system or application software are controlled through change management policy.	No exceptions noted
			Changes are either approved by the Senior Manager-IDC or CISO after recommendation from IT Infrastructure Team.	Inspected Change Management policy for system changes and determined that policy addresses approval. Inspected a sample of change requests and determined that process followed the change management Policy.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	System components are not updated for changes in requirements, resulting in a system that does not meet commitments and system requirements.	Changes to system infrastructure and software are authorized by the Senior Manager-IDC or CISO before implementation.	Selected a sample and inspected the change requests for approval of system changes	No exceptions noted
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	Identified breaches, incidents, and other system impairments are not considered during the change management lifecycle.	Identified breaches and incidents are notified during the change management process to CISO.	Enquired with AVP-IT to determine that for some incidents, change requests are opened as part of resolution.	No exceptions noted
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, processing integrity and confidentiality commitments and system requirements.	System changes are not authorized by those responsible for the design and operation of the system, resulting in changes to the system that impairs its ability to meet commitments and system requirements.	Changes to system infrastructure and software are authorized by the Senior Manager-IDC or CISO before implementation.	Selected a sample and inspected the change requests for approval of system changes	No exceptions noted
		System changes do not function as intended, resulting in a system that does not meet commitments and system requirements.	System change requests for changes to system components are reviewed and approved by Senior Manager-IDC or CISO prior to work commencing on the requested change.	Inspected Change Management policy for system changes and determined that policy addresses approval from Senior Manager-IDC or CISO. Inspected a sample of change requests and determined that process followed the change management process.	No exceptions noted
			Changes are reviewed and approved by the Senior Manager-IDC or CISO prior to implementation.	Inspected Change Management policy for system changes and determined that policy addresses approval from Senior Manager-IDC or CISO and covers information regarding scheduled impact and technical impact. Inspected a sample of change requests	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
				and determined that process followed the change management process.	
			Any changes in server & firewall configurations require approval by the Senior Manager-IDC or CISO.	Inspected IT Manual and determined that any changes to servers and firewall are categorized as a change and requires approval from Senior Manager-IDC or CISO. Inspected a sample of changes requests related to servers and firewall changes for compliance with the policy.	No exceptions noted
		Unauthorized changes are made to the system, resulting in a system that does not meet commitments and system requirements.	Infrastructure changes are raised by IT infrastructure team member which are reviewed & approved by CISO or Senior Manager-IDC of the organization.	Inspected the Change Request Form & verified approval by Senior Manager-IDC or CISO for sample changes	No exceptions noted
		Unforeseen system implementation problems impair system operation, resulting in a system that does not function as designed.	All change requests must be submitted with implementation plan, Rollback Plan Testing plan, Impact and Risk Analysis.	Inspected Change management policy and Change request form to determine that implementation plan, Rollback Plan Testing plan, Impact and Risk Analysis of the change is documented and maintained.	No exceptions noted
			Post implementation procedures that are designed to verify the operation of system changes are performed for one week after the implementation for other than minor changes, and results are shared with users and customers as required to meet commitments and requirements.	Enquired from CISO that the organization gives a 2-week Post Implementation Support.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Test Results
		Incompatible duties exist within the change management process, particularly between approvers, designers, implementers, testers, and owners, resulting in the implemented system not functioning as intended.	The change management Policy has defined the role and responsibility of Change Management Committee for approval of changes.	Inspected the Change Management Policy to determine that the policy defines role and responsibility of Change Management Committee for approval of changes.	Exceptions noted The Change Management policy requires that changes be approved by the change management committee. However, in practice, change management requests are approved only by CISO.

Additional Criteria for Availability

Ref No	Criteria	Risks	Actual Control	Test Procedures	Gap
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Current processing capacity is not sufficient to meet availability commitments and system requirements in the event of the loss of individual elements within the system components.	Processing capacity is monitored on an ongoing basis using an online tool Nagios. Automated Alerts are configured in Nagios Tool for Monitoring.	Enquired with the Management about the frequency of capacity planning process and found that Capacity Planning forecasting about the resources are captured quarterly. Inspected Nagios Alert email to determine that system performance, resource utilization is monitored.	No exceptions noted
			Critical infrastructure components Firewall and Power have been reviewed for assignment of a minimum level of redundancy.	Inspected the Network Diagram and enquired with AVP IT that there are two Firewalls configured Load Balancer A10 Thunder for redundancy and determined that critical Infrastructure Component Firewall and Power is included for redundancy Inspected redundancy measures for firewall and determined that there is a backup firewall in a high availability configuration. Inspected redundancy measure for Power and determined that UPS and Genset act for redundancy. Observed and physically verified the two firewalls. The Backup firewall is installed on a standalone Server for quick installation.	No exceptions noted
		Processing capacity is not monitored, planned, and expanded or modified, as necessary, to provide for the continued availability of the system to meet the entity's commitments and system requirements.	Processing capacity is monitored on a regular basis using tool Nagios. Quarterly review meetings happen with IT Infra which includes analysis of processing requirements. Meetings can also happen more than once in Quarter. Management decides on steps to manage processing capacity so that it's in line with the plans.	Enquired with management about the frequency of capacity planning process and the various inputs that go in the discussion. Inspected Nagios event reports and Fortigate 1500D Firewall reports to determine that system performance, resource utilization is monitored. Inspected Quarterly review meeting minutes done by IT Infra and AVP-IT including processing requirements.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Gap
			Critical infrastructure components Firewall and Power have been reviewed for assignment of a minimum level of redundancy.	Inspected the IT Network Diagram and determined that critical Infrastructure Component Firewall and Power is included for redundancy. Inspected redundancy measures for firewall and determined that there are two firewall in a high redundancy configuration with a load balancer. Inspected redundancy measure for Power and determined that UPS and Genset act for redundancy. Observed and physically verified the two firewalls. The Backup firewall is installed on a standalone Server for quick installation.	No exceptions noted
			Processing capacity is monitored on a regular basis using tool Nagios. Quarterly review meetings happen with IT Infra which includes analysis of processing requirements. Meetings can also happen more than once in Quarter. Management decides on steps to manage processing capacity so that it's in line with the plans.	Enquired with management about the frequency of capacity planning process and the various inputs that go in the discussion. Inspected Nagios event reports and Fortigate 1500D Firewall reports to determine that system performance, resource utilization is monitored. Inspected Quarterly review meeting minutes done by IT Infra and CEO including processing requirements.	No exceptions noted
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Environmental vulnerabilities and changing environmental conditions are not identified or addressed through the use of environmental protections resulting in a loss of system availability.	Environmental controls (fire extinguishers, water sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. FM 200 gas based Fire Suppression system is installed as per Data Centre Tier 3 standards installed. Multiple unit air-conditioning is installed in Data Centre. Devices are checked and a daily basis and checklists are prepared.	Observed that fire extinguisher installed in the company have valid dates and fire detector panel is in working condition. Inspected the Admin Maintenance Tracker and determined that the fire alarms are inspected and are in working order. .	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Gap
			Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment such as servers, network devices and workstations and applications against power failures and fluctuations. DG set of sufficient capacity is provided to provide power during outage. DG set has sufficient diesel and is tested regularly. This equipment is tested on Quarterly Basis.	Physically observed the UPS and DG Set installed at the premises to determine that they are in good working condition. Inspected the UPS and DG preventive maintenance reports, vendor maintenance contracts to determine that UPS and DG are being maintained on quarterly basis.	No exceptions noted
			Company has 2 ISPs (1 Gbps and 1 Gbps) is in place to provide redundancy in case of link failure	Inspected the contract with ISPs for redundancy	No exceptions noted
		Environmental vulnerabilities are not monitored or acted upon increasing the severity of an environmental event.	The Admin Team maintains all the environmental controlled equipment's	Enquired with facilities personnel about frequency of checking of working of environmental controls. Inspected DG, UPS and AC maintenance report and determined that they are maintained internally on a periodic basis and any exceptions are resolved.	No exceptions noted
			Admin team monitors the temperature Data center on an hourly 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
			Environmental protections receive maintenance on at least on quarterly basis.	Inspected DG, UPS and AC maintenance report and determined that they are maintained on regularly basis on their own with no exceptions reported.	No exceptions noted
		Software or data are lost or not available due to processing error, intentional act, or environmental event.	Backups are done as per policy and transferred offsite to Jaipur DR location through dedicated and secured P2P Link only for the Organizations own Internal Server and data of those clients who have opted for a Backup Service.	Enquired with Head IT on the backup procedures to determine that backups are done locally and transferred to Jaipur Offsite DR location through dedicated and secured P2P Link only for the Organizations own Internal Server and for Clients who have opted for a Backup Service.	No exceptions noted

Ref No	Criteria	Risks	Actual Control	Test Procedures	Gap
			Backups are monitored for failure and alerts are automated. The incident management process is invoked if there is failure. Backups are tested on Random basis.	Inspected the Backup Alerts and determined that backups are monitored through Tool and failures are recorded as Incidents.	No exceptions noted
		Availability commitments and system requirements are not met due to a lack of recovery infrastructure.	Company uses a BCP strategy for its facilities which is commensurate with the criticality of continuity of operations and Client requirements. Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented. Company uses offsite DR site at its other office in Jaipur.	Inspected the policies and procedures relating to disaster recovery & Business Continuity plans.	No exceptions noted
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Recovery plans are not suitably designed and backups are not sufficient to permit recovery of system operation to meet the entity's commitments and system requirements.	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested at least annually.	No exceptions noted
			BCP Test results are reviewed by management and the contingency plan is adjusted.	Inspected the most recent BCP testing report and determined that (i) testing was as per BCP strategy (ii) Reports were discussed and approved by the AVP-IT (iii) actions from test report are complete.	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.