Cyfuture India Pvt. Ltd.

REPORT ON SYSTEM & ORGANIZATION CONTROL (SOC)

SOC 2 TYPE 2 REPORT RELEVANT TO SECURITY TRUST SERVICE CRITERIA FOR THE PERIOD OF 1ST JANUARY 2023 TO 31ST JULY 2023

Statement of Confidentiality

This report, including the Description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's systems for using the Customer Support Services relevant to the Security, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

Independent Service Auditors' Report on Description of Cyfuture's System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability, Confidentiality, and Processing Integrity Trust Service Principles.

To the Cyfuture's Management Scope

We have examined the attached Description of the system in Section 3 of Cyfuture India Private Limited (hereinafter collectively referred to as "Cyfuture" or "Service Organization") throughout the period 1st January 2023 to 31st July, 2023 (the 'period') related to the Security Operations Center (SOC) and Central Command Centre (CCC) Services, based on criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Cyfuture's system, particularly information about system controls that Cyfuture's has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity and Confidentiality ("Applicable Trust Services Criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("AICPA, Trust Services Criteria").

The Description indicates that certain applicable trust services criteria specified in the Description can be met only if the entity controls contemplated in the design of the Service Organization'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.

Cyfuture's Responsibilities

In Section II, Cyfuture has provided an assertion about the fairness of the presentation of the Description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Cyfuture is responsible for preparing the Description and assertion, including the completeness, accuracy, and method of presentation of the Description and assertion; providing the services covered by the Description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the Description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the 1st January 2023 to 31st July, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of a Service Organization system and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria involves:

- Performing procedures to obtain evidence about whether the Description is fairly presented based on the description criteria and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period 1st January 2023 to 31st July, 2023.
- 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.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a Service Organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, are subject to the risks that the system may change or that controls at a Service Organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

a) The Description fairly presents the system that was designed and implemented throughout the period 1st January 2023 to 31st July, 2023.
b) The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period 1st January 2023 to 31st July, 2023 and process applied the controls contemplated in the design of the Service Organization's controls throughout the period 01 December 1st January 2023 to 31st July, 2023.
c) The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period 1st January 2023 to 31st July, 2023. If complementary user entity controls contemplated in the design of the Service Organization's controls operated effectively throughout the period 1st January 2023 to 31st July, 2023.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV of the report.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is, intended solely for the information and use of Cyfuture, user entities of the system related to SOC and CCC services provided to its customers relevant to the Security, Availability, Processing Integrity and Confidentiality and system of Cyfuture during some or all of the period 1st January 2023 to 31st July, 2023, and 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, and 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.

Sandip Padhi

Place: Date: 06-11-2023

SECTION 2

MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

cyfuture
Thinking Future. Moving Ahead.

MANAGEMENT ASSERTION DOCUMENT

Date: 18-10-2023

Management of Cyfuture India Private Limited Assertion

We have prepared the accompanying description of the **Cyfuture India Private Limited** (Cyfuture) system titled **"Data Center Services Including Web Site Hosting, Web App Hosting, Server Co-Location, Disaster Recovery, Backup, Email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services"** throughout the period 1st January 2023 to 31st July, 2023 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Type 2 Report (description criteria).

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

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

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

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

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

The description contains the following information:
1) The types of services provided
2) The components of the system used to provide the services, which are as follows:
    a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

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

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

    d) Procedures. The automated and manual procedures.

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

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

3) The boundaries or aspects of the system covered by the description.
4) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

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

8) In the case of a SOC 2 Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

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

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

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

Name: AJAJ RAI

Signature:

Date: 18/10/2023

SECTION 3

DESCRIPTION OF THE SYSTEM

SYSTEM DESCRIPTION PROVIDED BY SERVICE ORGANIZATION

3.1 Overview of Operations

Cyfuture Datacenter and Cloud Technologies Private Limited ("Company") is in the business of providing data center services including but not limited to data center infrastructure as a service on a hosted On-Premises mode and enterprise cloud services which will be utilized by the customer for hosting content.

3.2 Delivery Overview

Cyfuture has customers in different parts of the world and has been classified as a region, and each region has a leader who is ultimately responsible for delivering services to all customers served by that region. This framework enables Cyfuture to create processes and quality standards that are the same throughout the company. This makes it easier for regions to collaborate with each other and with Cyfuture's support organizations, and external partners. As a result, Cyfuture is able to maximize the use of existing resources and deliver high-quality and cost-effective services.

The end-to-end service delivery is focused on:

- Driving continuous improvement – Ensuring Cyfuture's services are delivered better, faster, and in a more cost-effective manner each year.
- Reducing delivery costs – Driving the costs of delivering services to a minimal amount without compromising delivery quality year-over-year.
- Increasing delivery accountability – Minimizing hand-offs in the organization, empowering employees to own their part of the business, and producing work outputs that impact customer success and metrics.
- Implementing consistent global standards – Utilizing enterprise-wide, industry standards, and leading practices within daily delivery operations to ensure optimal performance.
- Enhancing end-to-end service excellence – Ensuring customers receive 24 x 7 service at or above Service Level Agreement (SLA) expectations without interruption.

Cyfuture operates from below listed locations for SOC and CCC Services:

Location of Cyfuture office	Services Provided
Meghdoot , Plot no 197/198 Noida Special Economic Zone Noida Dadri Road, Noida Phase II Noida -201305	The Corporate Office

Cyfuture offers the following services, not all of which may be covered in this report or under the scope of services provided to their customers in accordance with their SLA.

3.3 Description of the Cyfuture Control Environment, Risk Assessment, Information and Communication, and Monitoring Processes

Cyfuture's internal control components include controls that may have a persistent effect on the organization, an effect on specific processes or activities, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or activities. When assessing internal control, Cyfuture considers the interrelationships among all the supporting components.

3.3.1 Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The objectives of an internal control structure are to provide reasonable, but not absolute, assurance as to the confidentiality, security, processing integrity, availability and reliability of the information, the protection of assets from unauthorized use or disposition, and that activities are executed in accordance with management's authorization or customer instructions. Cyfuture has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Cyfuture has implemented a process-based service environment designed to deliver quality services to its customers. The fundamentals underlying the services provided are the evolution of standardized, repeatable processes, the hiring and development of highly skilled staff, and an extensive customer management infrastructure.

Cyfuture has defined organizational structures, reporting lines, authorities, and responsibilities within the organization to meet its commitments and requirements as they relate to security, availability, confidentiality, and processing integrity. Entities have defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role.

Hiring Practices

Cyfuture has formalized hiring practices designed to determine whether new, rehired or transferred employees are qualified for their functional responsibility. Where legally permissible, all-new external hires are required to successfully complete employment screening prior to commencing employment. Where and to the extent legally permissible, Cyfuture's standard pre-employment background checks will include

verification of the individual's National ID, verification of the individual's education (when required by position), previous employment, and a criminal check. Additional screening may apply in certain situations. The specifics or extent of background checks performed are dependent upon the position for which the individual is applying. Every employee will be assigned a written job description upon onboarding.

All new employees are issued information that documents various procedural and administrative matters. All new employees are required to complete mandatory training including the Code of Business Conduct and sign a non-disclosure agreement that sets lasting expectations of the commitments we make to each other and our company, to our clients and shareholders, and to the communities in which we live and work. The Code of Business Conduct applies equally to everyone working at, with, or on behalf of Cyfuture. It discloses to the employees the corporate conduct guidelines and requires that employees keep corporate and customer information confidential. Cyfuture has an information security policy

and associated standards that documents and provide guidance to Cyfuture personnel and requires all employees to complete annual Security Awareness training. The entity has policies and procedures in place to establish acceptable use of information assets.

The Human Resources Department and IT administrators are responsible for sending employee termination notifications to the teams upon an employee's termination or departure from Cyfuture. The security administration teams remove access upon receipt of the notification. Employees in sensitive positions are subject to immediate restriction from these areas upon termination or separation of employment. Employee keys, and, if applicable, mobile assets, are also collected upon termination or separation. Employees who are terminated by Cyfuture for certain, specific reasons (e.g., code of conduct violation) are escorted from the facility immediately upon termination.

Completed performance appraisals are reviewed by management and become a permanent part of the employee's personnel file. Training of personnel is integrated into the Individual Development Plan. Depending on the individual's roles, learning activities for the year are outlined as an objective in the Learning and Development Plans. In addition, Cyfuture has developed mandatory annual learning for the employees. Employees' managers or directors of IT are responsible for determining that staff complete appropriate training and remain qualified for their functional responsibilities.

Standards and Procedures

Every Cyfuture employee knows and uses the Company's values to guide their business decisions and actions. These values underscore Cyfuture's belief that an ethical, honest, inclusive, and transparent workplace is critical to the Company's long-term success. Cyfuture's values are an important competitive differentiator and intangible driver of our company's success.

Cyfuture maintains a system for policy and process documentation to be easily referenced by all employees. The policies, processes, and work instructions are documented in the respective process manuals and insubordinate documents. Processes that directly result in the delivery of products and services to the customer are documented and version controlled. The documentation includes interactions between processes, customers, and subcontractors. A disciplined understanding and consistent application of these documents by associates help ensure that the requirements for delivering quality products and services are met.

Cyfuture has a suite of policies and standards that documents the information security policy framework which is utilized by those involved in service delivery to create and implement an appropriate and effective Information Security Management System (ISMS) for client delivery unless Cyfuture is contractually obligated to follow client-specific information security policies. Within the content available, all of which is mapped to relevant industry, relevant legislation, regulation(s), and global standards, there is a defined baseline set of Control Standards. These Control Standards are divided into Trust Service Criteria (TSC) such as Common Criteria, Confidentiality, Processing Integrity, and Availability.

The entity has established a Data disposal policy which is aligned with Industry best practices for securely dispose off the data.

3.3.2 Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of the Cyfuture internal control system. The purpose of the risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. The management of Cyfuture also monitors controls to consider whether they are operating as intended and whether they are modified as appropriate for changes in conditions or risks facing the organization.

Risk management is a universal component of the services provided by Cyfuture to its customers, irrespective of the location or business area. The Cyfuture COO of IT leads programs, projects, or operations and has the primary responsibility to understand and manage the risks associated with their activities.

At a corporate level, there are multiple functions, including Legal, Cybersecurity, Internal Audit, Risk Management, Procurement, Employee Health and Safety, Contracts, and all of which provide risk management support through policy guidance and internal consulting services. The Internal Audit Team is responsible for assessing the risk and control environment through evaluation of financial, operational, and administrative controls, risk management practices, and compliance with laws, regulations, and Cyfuture policies and procedures. Internal Audit reports to the Cyfuture Senior Management and communicates significant findings and the status of corrective actions.

The entity has a documented Vendor Management policy that guides personnel when performing the third-party risk assessment process. The policy is reviewed and approved by the COO of IT on an annual basis.

Risks are periodically assessed and reviewed by senior management. Company policy and procedures are focused on risk management and are maintained, updated, and communicated to employees on a regular basis. In addition, the security function performs a formal risk assessment on an annual basis.

The results are delivered to management and the security team for review. Findings and recommendations from external assessments are categorized by severity and risk and remediated according to in line with an internally defined process.

Cyfuture has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system are included in the master services agreement and standard service level agreements.

3.3.3 Information and Communication

Information and communication are integral components of the Cyfuture internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Cyfuture, information is identified, captured, processed, and reported by various information systems, as well as through conversations with customers, vendors, regulators, and employees.
To help align Cyfuture’s business strategies and goals with operating performance and controls, the organization has implemented various methods of communication at a global level to ensure that all employees understand their individual roles and responsibilities and to ensure that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, regular management meetings for updates on business performance and other matters, broadcast video conferencing, the use of electronic mail messages to communicate time-sensitive messages and information.

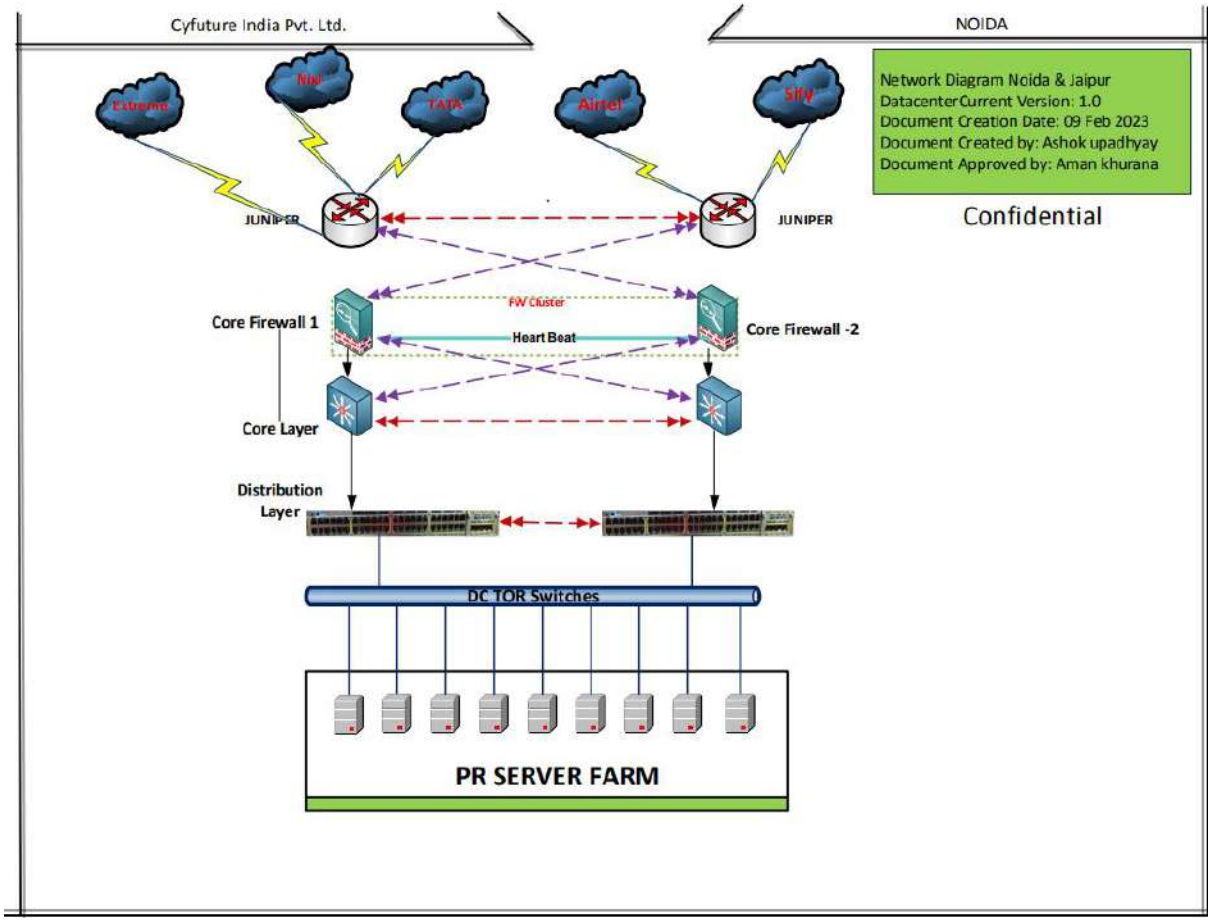
Cyfuture has defined policies, standards, and guidelines related to security, confidentiality, processing integrity, and availability and is made available for all employees on the internal share drive. Changes to the Policies, Standards, and guidelines related to security, confidentiality, processing integrity, and availability are published to the internal share drive. All employees undergo training as per the established process for annual security, confidentiality, and privacy training.

3.3.4 Monitoring

Cyfuture management is committed to maintaining effective communication with all personnel. Cyfuture management participates in regular meetings in order to discuss the status of current customer processing, organizational structure, and other matters of interest and concern. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved. In addition, all Cyfuture personnel attends meetings for updates on recent business performance and other matters. Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy.

Entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system are raised to the respective team for further resolution. The capacity management process is defined and documented which is reviewed and approved by the COO of IT on an annual basis. Forecasts reports are reviewed and approved by Senior Management to monitor and evaluate the current processing capacity and use of system components. Change requests are initiated if required and directed by the Senior Management based on approved forecasts. Processing capacity is monitored on a monthly basis and forecasted to meet business requirements.

Network Diagram



Network Management

Cyfuture has set up designated work areas or Zones for the CCC Services. These fully operational dedicated work areas which are linked to the Cyfuture'score network by Internet Protocol Security (IPSec) tunnels and via VPN for remote connectivity.

Cyfuture has installed and implemented all relevant network devices for the connectivity over the network including firewalls, IPS, routers, and switches, and servers are all secured within closed racks dedicated to the Cyfuture inside the hub/server room.

The Cyfuture network has been segmented into three networks within the perimeter Firewall:

- Management Segment,
- Infrastructure Segment
- Non-Operational Segment.

The Management Segment only has network devices like switches and servers placed on it, along with the management workstation that is used by Cyfuture CCC administrators to manage these devices. This segment is primarily used for network and server management for the SOC and CCC services.
The Infrastructure Segment connects routers, IPS, and firewalls which are high bandwidth devices and handle outside traffic to the SOC and CCC applications. This is the first point of access to the Cyfuture network that can be reached from an external destination. The external traffic is routed from the Infrastructure Segment to the Management and Non-Operational Segments based on firewall rules and another supplemental security device (s) configuration.

The Non-Operational Segment is used for user and workstation network access. The Non-Operational Segment only contains Cyfuture owned workstations, configured and managed as per internally approved hardening specifications. The workstations are used to connect to the Cyfuture network.

All incoming and outgoing traffic passes through the firewall. Access to the firewall and network devices is granted and restricted to network administrators using SSO authentication. A Cyfuture local Windows Active Directory (AD) domain environment has been created for user and computer authentication and domain authorization purposes. Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in risk register along with the mitigation steps

Physical Security

Cyfuture has a comprehensive physical security program consisting of the traditional controls based on industry standards. The security controls utilize a layered approach at each location in which the controls become more stringent progressing from the outermost perimeter of the facility to the interior restricted spaces.

Physical and environmental security policies and procedures have been developed and implemented by Cyfuture to control access to the office perimeter and other sensitive areas, including computer equipment, storage media, and documentation.

Access Restrictions

Physical security for a restricted area/zone begins at either the perimeter of the facility in which the zone resides or the building where the restricted area is located. Persons seeking

access to the office must have a legitimate business purpose before entering the building. Cyfuture employees and authorized contractors who have been granted unescorted access must use their building keys to open the doors to permit their entrance.

Fire drills are carried out by Local Authorities on an Annual basis. Local authorities review the Fire extinguishers and other physical and environmental security mechanism and report about their adequacy. Access to the Cyfuture building and IT components is removed when an employee resigns from the organization or transfers out to another location. When an employee resigns, the HR receives a completed employee Exit Checklist Form signed from the IT team confirming removal of access from the IT components, retrieval of all the assets belonging to the users and building keys allowing access to the facility. The process for granting and removing access for third-party contractors is the same as the process for granting and removing access for Cyfuture employees.

Visitor Access

Upon arrival at the Cyfuture facility, the visitor contacts the staff using the door phone at the entry gate. The receptionist contacts the individual who is being visited and informs him or her about the visitor. Details such as the visitor's name, their Cyfuture contact person, and entry and exit times are recorded within the Visitor Register. The employee accompanies the visitor to the relevant area within the facility and escorts the visitor back to the security desk after the completion of their visit.
Visitors' electronic devices are not allowed inside restricted zones/areas.

Background checks

The Cyfuture HR/COO of IT is responsible for performing background screening (education and employment verification) for all new hires joining Cyfuture. The following checks are made on all applications for employment:

- Completeness of applicant's curriculum vitae
- Confirmation of academic and professional qualifications
- Identification check
- Reference checks for residence and two previous employment records

For temporary staff, a similar screening process is performed. Where these staffs are provided through a third-party agency, the contract with the third party clearly specifies the agency's responsibilities for screening and the notification procedures they must follow.

Logical Security

Cyfuture has developed and implemented logical access security policies and procedures to control access to IT components and network devices. Access to the system is provided solely for the purpose of facilitating business-related activities in order to perform their day-to-day operational tasks. For Cyfuture resources**,** access controls on all desktops and systems that are used to provide services for SOC, and CCC are implemented based on "least privilege" or "need-to-know" principles and are only granted after approval from authorized personnel.

Logical Access Provisioning & deprovisioning

The employee/designated individual submits the access request form to access Cyfuture AD and other applications as part of the job responsibility to their respective Line Manager. Once approved, the access request form along with approval is submitted to the relevant team to provision the user access in AD and requested application. If rejected, the respective team communicates the rationale/justification for rejecting the request and the employee/manager will resubmit the corrected user access request form. Privileged access to sensitive resources

is restricted to defined user roles and is approved by the COO of IT.

When an employee leaves the organization or transfers to another location, HR initiates an email about the termination of the employee to the IT team. On the last working day of the employee, the IT team revokes the user access from AD and underlying IT components/application (if any) and confirms back to the HR documenting the access has been removed. The HR preserves the record for future references in the shared drive, which has restricted access only to authorized individuals. The entity has established a process to annually review user access privileges for appropriateness and access revalidation.

Password Policies

Passwords and other authentication mechanisms control the entry points to Cyfuture systems, applications, and their services. Protecting access to Cyfuture systems, solutions, and services by using secure passwords and authentication controls is critical to the security of Cyfuture, client, and third-party information. Password policies are implemented to provide the requirements for passwords and associated authentication controls and to describe their correct use, in order to limit access to information systems to authorized users only.

In accordance with Cyfuture password policy, the user account password is at least eight (8) complex characters. The password must be changed at least once every 90 days. After a maximum of five (5) invalid login attempts, the Cyfuture user login account is locked out for at least fifteen (15) minutes.

Change Management

The change management process is followed by Cyfuture to perform changes to the IT environment, an application hosted on the internal network as part of the application maintenance and service provided to the customers.

Change Management Process Documents

At the highest level, the objective of Change Management is to control and manage changes to services and associated IT and business Applications and to promote business benefit while minimizing the risk of disruption to services and therefore impact on the business. Change Management coordinates and controls the implementation of Change Requests. In the context of this report, Cyfuture provides support for configurational changes to its applications.

The change management process is followed for all changes that are performed by Cyfuture on the applications hosted within the Cyfuture network. Unauthorized changes are strictly prohibited, even under emergency conditions (for which the emergency change request process exists). All changes to the environment are subject to the change control process defined within the Procedure document. Key stakeholders are notified of changes that may impact their environment through an email notification or via Change Request Form (CRF) on system downtime. The process owner assesses the impact of implementing significant changes to the environment against security commitments and system requirements.

Documentation and Tracking of Changes

Change Initiation

Change Requests are documented and prioritized through a HelpDesk Portal and then assigned to the appropriate individual/workgroup for further proceedings.

Assessment of Change

The Cyfuture Change Coordinator (designated individual) reviews the submitted CRF for completeness and validates it is relevant to the services agreed with Clients. If the CRF is incomplete, the Change Coordinator contacts the Change Requester, requesting additional information in order for the Change to be assessed and authorized for planning. Based on this initial assessment, a CRF is authorized by Cyfuture to progress to Change Planning or is rejected and the Change Requester is advised of the reason for not granting initial authorization.

Change Planning

Once the change is accepted and authorized to progress, a risk and impact assessment is performed by Cyfuture to initiate solution design and/or validate the changing scope. As part of this process, system documentation and asset inventories related to the change are updated by Cyfuture and stored within portal with respective updates.

Change Approvals

Change requests are recorded in the Change Request Form and stored within portal which has restricted access only to authorized individuals. This activity is coordinated by the Cyfuture Change Coordinate in the form of a meeting that includes key stakeholders and required representatives. The changes are approved by the Change Coordinator or COO of IT. The purpose of these meetings is to ensure the risk and impact of the change are fully understood and accepted by key stakeholders prior to the scheduling and implementation of the change. If no significant concerns are raised, the change will progress as scheduled. If the change is considered to have an adverse impact on the environment, the change will be put on hold or returned for re-planning, and the change requestor is notified so that further discussions may be conducted.

Change Implementation

All changes are implemented during scheduled maintenance windows by Cyfuture personnel with the appropriate skills and experience. The Change Request Forms maintains a record of all changes that include approvers, the implemented solution, back-out plans, and any issues arising from the change. Due to their nature, emergency changes will be implemented based on business criticality and may fall outside or extend beyond the scheduled maintenance window.

Once the change is implemented, the Cyfuture Change Coordinator notify the stakeholders about the status of the implementation.

Review and Closure of Change

Cyfuture’s Change coordinator performs the post-implementation check, updates the change record status and then the change records will be Closed.

Rollback plan

A rollback plan is developed for all the changes by the Cyfuture Change requestor and updated within the change request form to roll back in case the change fails.

Incident Management

Cyfuture has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal.

The Cyfuture representative records incidents and assigns them to the respective teams for Internal incidents and client provided emails IDs for respective clients. Once assigned to the internal team, the team then communicates with the additional details related to the Incident report. A confirmation email is sent when the issue is resolved, and action is taken that addresses the issue.

Backup and restoration

Cyfuture has established process documents to encrypt backups to ensure confidentiality and integrity of the information. Regular backups of database servers are performed and in an event of backup failure, technical teams investigate until resolution is provided. Restoration is performed on the basis of requests from business and technical teams. A mirror image of critical data files are replicated periodically and stored on the second system for use in recovery and restoration in the event of system disruption or outage.

The entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the Director of IT on an annual basis.

3.2 Trust services principle and Description of Related Controls:

3.2.1 Security Category

CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Activities
CA-1 Entity has a documented Information security policy that is available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy is reviewed and approved by the management on an annual basis. CA-2 Entity has policies and procedures in place to establish acceptable use of information assets. CA-3 Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter. CA-4 Before an employee or a third-party vendor/contractor is engaged by the entity, the third-party personnel undergoes background screening. A background check includes, at a minimum, professional, educational, and employment checks. CA-5 Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties or subcontractors.

CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Activities

CA-6 Entity has defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role.

CA-7 Entity has defined organizational structures, reporting lines, authorities, and responsibilities within the organization to meet its commitments and requirements as they relate to security, availability, confidentiality, and processing integrity.

CA-8 Reporting lines and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.

CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Activities
CA-8 Reporting lines and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements. CA-6 Entity have defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role.

CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Activities
CA-9 Entity has defined processes for hiring, training, and performance appraisal to enable personnel to fulfill their responsibilities which are documented within the HR Policies. HR policies and procedures relating to recruitment and termination are maintained within the intranet portal. CA-6 Entity has defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role. CA-10 The experience, competence, and training of candidates for employment or assignment are evaluated before they assume the responsibilities of their position. CA-11 New employees are required to undergo security training at the time of induction. CA-4 Before an employee or a third-party vendor/contractor is engaged by the entity, the third-party personnel undergoes background screening. A background check includes, at a minimum, professional, educational, and employment checks.

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Activities
CA-6 Entity has defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role. CA-11 New employees are required to undergo security training at the time of induction. CA-3 Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter. CA-12 Entity performs annual formal staff evaluation to assess alignment with company principles and objectives. CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis.

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Activities
CA-14 Entity has defined and documented Standard Operating Procedures (SOP) for services provided to the Customers via CCC. CA-15 Entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the Director of IT on an annual basis. CA-16 Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps. CA-17 Cyber essential audits are performed by an external vendor on an annual basis.

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Activities
CA-1 Entity has a documented Information security policy that is available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy is reviewed and approved by the management on an annual basis. CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal. CA-19 Entity has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's) and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements. CA-3 Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter. CA-20 All employees undergo training as per the established process for annual security, confidentiality, and privacy training. CA-21 Incidents are logged by the employees and are assigned severity levels. Reported incidents are assigned to the respective teams for analysis and resolution within the stipulated SLA. CA-22 Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy.

CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Activities
CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal. CA-21 Incidents are logged by the employees and are assigned severity levels. Reported incidents are assigned to the respective teams for analysis and resolution within the stipulated SLA. CA-22 Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy. CA-19 Entity has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's) and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Activities
CA-23 The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management. CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure. CA-17 Cyber essential audits are performed by an external vendor on an annual basis. CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis.

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.

Control Activities
CA-23 The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. CA-26 A master list of the entity's IT system components are maintained, accounting for additions and removals, for management's use. CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management.

Control Activities
CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure.

[Space left blank intentionally]

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Activities
CA-23 The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management. CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure. CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis.

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Activities
CA-23 The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management. CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure. CA-8 Reporting lines and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements. CA-16 Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps.

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Activities
CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis. CA-27 Management and internal audit periodically receive reports summarizing incidents, the root cause of incidents, and corrective action plans. Internal audit monitors for completion of corrective action plans. CA-28 Entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system are raised to the respective team for further resolution. CA-29 Entity has established a process to periodically review user access privileges for appropriateness and access revalidation.

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Activities
CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management. CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure.

CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Activities
CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis. CA-15 Entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the COO of IT on an annual basis. CA-17 Cyber essential audits are performed by an external vendor on an annual basis. CA-16 Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps.

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Activities
CA-1 Entity has a documented Information security policy that is available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy is reviewed and approved by the management on an annual basis.

Control Activities
CA-30 Entity has developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of user access. CA-31 Entity has documented Change Management policy and process which is reviewed and approved by the Director of IT on an annual basis. CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis.

CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Activities
CA-1 Entity has a documented Information security policy that is available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy is reviewed and approved by the management on an annual basis. CA-13 Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis. CA-17 Cyber essential audits are performed by an external vendor on an annual basis.

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Activities
CA-30 Entity has developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of user access. CA-32 Privileged access to sensitive resources is restricted to defined user roles, and logical access to these roles is approved by the Director of IT. CA-33 External access to an entity's environment by employees is permitted only through an encrypted virtual private network (VPN) connection. CA-34 Unique User ID is assigned to individuals to ensure accountability. CA-35 Password parameters for application and infrastructure are defined as per the Password Management Policy which is reviewed on an annual basis.

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Activities
CA-36 User accounts are created in IT systems/applications upon receiving a duly filled user access form along with approvals from relevant stakeholders. CA-37 System security is configured to require users to change their passwords upon their initial system sign-on and thereafter follow the password policy configured within the Organization/within the Application. CA-38 When an employee resigns or transfers out of the Organization or Project, a request to revoke the user's access is initiated to respective teams. The IT team revokes user access based on the request on the last working day of the employee. CA-29 Entity has established a process to periodically review user access privileges for appropriateness and access revalidation.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Activities

CA-30 Entity has developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of user access.

CA-36 User accounts are created in IT systems/applications upon receiving a duly filled user access form along with approvals from relevant stakeholders.

CA-38 When an employee resigns or transfers out of the Organization or Project, a request to revoke the user's access is initiated to respective teams. The IT team revokes user access based on the request on the last working day of the employee.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control Activities
CA-39 Access to the Entity's SOC and CCC are restricted to authorized personnel via a padlock and the combination is known only to appropriate individuals. CA-40 Visitors to the Entity's facility are required to submit details such as visitor's name, contact person within the Entity, and entry and exit time are recorded within the Visitor Register. Visitors are escorted by an employee from the reception at all times during their visit. CA-41 Entry keys are handed over by the human resources department during the joining of the employee and after all required background investigations are completed. Keys are to provide access only to non-sensitive areas within the Organization. CA-42 Entity has established a process that, during the termination process, employees are required to return their entry keys and corresponding assets as part of their exit process.

Control Activities
CA-43 A monitoring process exists to monitor entry or exit points. Measures such as, but not limited to, alarm systems and surveillance cameras. The information (for example, logs, tapes, and so forth) is maintained for an agreed period of time for future reference. CA-44 Unauthorized access attempts are recorded and reviewed on a periodic basis. Appropriate corrective actions are taken against the identified defaulters. CA-45 Physical access to the Entity premises is reviewed periodically to ensure only authorized individuals have access to the facility. CA-46 Entity has established a Data disposal policy which is aligned with Industry best practices for securely disposing of the data.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control Activities
CA-46 Entity has established a Data disposal policy which is aligned with Industry best practices for securely disposing of the data.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Activities
CA-47 Connections to Entity's internal network from External points are protected by a firewall, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices. CA-48 Access to the firewall is provided only to appropriate individuals using AD authentication. CA-28 Entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system are raised to the respective team for further resolution. CA-49 Firewall logs are reviewed on a periodic basis and necessary corrective actions are taken in case any deviations are noted. CA-3 Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Activities
CA-33 External access to an entity's environment by employees is permitted only through an encrypted virtual private network (VPN) connection. CA-50 Entity has established a process to encrypt backups to ensure confidentiality and integrity of the information.

[Space left blank intentionally]

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Activities
CA-51 The ability to install applications on systems/servers is restricted to system administration personnel only. CA-52 Antivirus software is installed on all the workstations, laptops, and servers supporting such software to protect them against malware. Antivirus software/agents are configured to receive an updated virus signature at least daily.

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify

(1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Activities
CA-53 Entity has established Patch Management and Vulnerability management procedures to detect known vulnerabilities and monitor the systems. The policy and procedure are made available to the employees through the Intranet portal. CA-16 Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps. CA-54 Security patches are regularly applied to employee workstations so that workstations stay up to date with an operating system version that is current, next most current, or without critical security gaps

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control Activities
CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal.

Control Activities
CA-16 Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Activities
CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal. CA-21 Incidents are logged by the employees and are assigned severity levels. Reported incidents are assigned to the respective teams for analysis and resolution within the stipulated SLA. CA-22 Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Activities
CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal. CA-22 Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy. CA-55 Basis the root cause analysis of the reported Incidents, the Change Management process is invoked by raising a change request for the events that require permanent fixes.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Activities
CA-18 Entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal. CA-22 Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy. CA-55 Basis the root cause analysis of the reported Incidents, the Change Management process is invoked by raising a change request for the events that require permanent fixes.

Control Activities
CA-15 Entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the COO of IT on an annual basis.

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Activities
CA-31 Entity has documented Change Management policy and process which is reviewed and approved by the Director of IT on an annual basis. CA-56 System change requests are reviewed and approved by the owner of the infrastructure/software or COO of IT, prior to work commencing on the requested change. Separate personnel is responsible to authorize changes and implementing the changes. CA-57 System Changes are tested by appropriate individuals. Testing report is documented and deviations from planned results are analyzed and remediated. CA-58 Separate environments are used for testing the change prior to implementation in production. CA-59 System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality commitments, and system requirements throughout the change management process. CA-60 Entity has established a process for automated patching of Windows machines (servers/desktops/laptops), which do not require separate change tickets raised for the same. Testing results are required to be documented and preserved for future reference for the same. Deviations are investigated and necessary corrective actions are taken.

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Activities
CA-23 The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. CA-24 Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management. CA-25 The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

Control Activities
CA-61 Entity has a documented Vendor Management policy that guides personnel when performing the third-party risk assessment process. The policy is reviewed and approved by the COO of IT on an annual basis. CA-62 Entity performs an annual vendor assessment based on its Vendor Management Policy. CA-3 Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter.

3.2.2 Additional Criteria for Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control Activities
CA-19 Entity has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements. CA-63 Capacity management processes are defined and documented which is reviewed and approved by the COO of IT on an annual basis. CA-64 Critical infrastructure components are periodically reviewed for criticality classification and assignment of a minimum level of redundancy. CA-65 Forecasts reports are reviewed and approved by Senior Management to monitor and evaluate current processing capacity and use of system components. Change requests are initiated if required and directed by the Senior Management based on approved forecasts.

A1.2: The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.

Control Activities
CA-66 Entity has established a process for Physical and Environmental Security and has installed the following to ensure system availability: • Cooling systems • Backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers

Control Activities
CA-15 Entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the COO of IT on an annual basis. CA-67 Daily incremental backups are performed using an automated system. CA-68 Backups are monitored for failure and the incident management process is invoked whenever applicable to ensure timely resolution of issues and availability of the backup system.

[Space left blank intentionally]

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Control Activities
CA-15 Entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the Director of IT on an annual basis. CA-69 Backup restoration testing is performed on an annual basis by the IT team. CA-70 Fire drills are carried out by Local Authorities on an annual basis. Local authorities review the Fire extinguishers and other physical and environmental security mechanisms and report about their adequacy.

3.2.3 Additional Criteria for Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Control Activities
CA-71 The entity establishes written policies related to retention periods for the confidential information it maintains. The entity • has processes in place to delete confidential information in accordance with specific retention requirements. • deletes backup information in accordance with a defined schedule. • requires approval for confidential information to be retained beyond its retention period and specifically marks such information for retention. • reviews annually information marked for retention.

C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Control Activities
CA-46 Entity has established a Data disposal policy which is aligned with Industry best practices for securely disposing off the data.

[Space left blank intentionally]

3.2.4 Additional Criteria for Processing Integrity

PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

Control Activities
CA-57 System Changes are tested by appropriate individuals. Testing report is documented and deviations from planned results are analyzed and remediated. CA-72 System alerts are analyzed on a semi-annual basis to co-relate them. Further, the problem management process is invoked basis the result of investigation and correlation. CA-73 Monthly trend reports are reviewed by the respective lead for unusual trends and problems are created basis the result of the review (if any). CA-67 Daily incremental backups are performed using an automated system. CA-74 Processing capacity is monitored on a monthly basis and forecasted to meet the business requirement. CA-75 Logical access to stored data is restricted only to the appropriate administrators.

PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

Control Activities
CA-76 A mirror image of critical data files is replicated periodically and stored on the second system for use in recovery and restoration in the event of system disruption or outage. CA-33 External access to an entity's environment by employees is permitted only through an encrypted virtual private network (VPN) connection.

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

Control Activities
CA-57 System Changes are tested by appropriate individuals. Testing report is documented and deviations from planned results are analyzed and remediated. CA-72 System alerts are analyzed on a semi-annual basis to co-relate them. Further, the problem management process is invoked basis the result of investigation and correlation.

[Space left blank intentionally]

PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

Control Activities
CA-67 Daily incremental backups are performed using an automated system.

PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.

Control Activities
CA-76 A mirror image of critical data files is replicated periodically and stored on the second system for use in recovery and restoration in the event of system disruption or outage. CA-67 Daily incremental backups are performed using an automated system. CA-68 Backups are monitored for failure and the incident management process is invoked whenever applicable to ensure timely resolution of issues and availability of the backup system.

[Space left blank intentionally]

3.3 Complementary User Entity Controls (CUECs)

In designing its systems, Cyfuture has contemplated that certain complementary controls would be implemented by the clients to achieve the criteria relevant to Security, confidentiality, processing integrity and Availability included in this report. Clients may use custom solutions using tools and processes developed, owned, and facilitated by either their employees or Cyfuture dedicated employees. These solutions, processes and tools are not included in the scope of this report. The complementary user entity controls are listed below.

Control Criteria	CUEC No.	CUEC Description
Common Criteria for Change Management & Incident Management	**1**	Raising a request to Cyfuture to submit a change, if required.
	2	Performing UAT and providing sign offs, if required.
	3	Providing approvals in timely manner to Cyfuture for submitted changes.
	4	Timely remediation of notified incidents by Cyfuture team.
	5	Performing updates/re-configuration of their own environment as a resolution of notified incidents.
Common Criteria Related to Logical and Physical Access Controls	6	Providing specifications/changes to specifications for configuring the SOC and CCC applications.
	7	Designing, implementing and monitoring appropriate security controls over their operating systems, databases, applications and other infrastructure components.
	8	Approving and providing users with access to their network and applications on request from Cyfuture.
	9	Revoking user access from their network and applications on request from Cyfuture.
	10	Performing vulnerability assessments and penetration tests on their own environment if done separately from SOC and CCC services.

Common Criteria Related to Communication	11	Approving and signing the MSA entered between Cyfuture and their Clients.
	12	Reviewing and agreeing to amendments to the MSA.
	13	Providing Standard Operating Procedures to Cyfuture team, if required to follow Client's procedures.

3.4 Principle Service Commitments and System Requirements

Cyfuture makes service commitments to its user organizations and has established system requirements as a part of its services. Some of these commitments are principal to the performance of the services and related to applicable trust service criteria.

Cyfuture is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Cyfuture's service commitments and system requirements are achieved.

Service commitments are documented and communicated in Master Service Agreement and any other agreements as agreed by Cyfuture and user organizations.

Principal Commitments and Requirements	Related Controls
Cyfuture has made commitments related to securing customer data through measures such as encryption, authentication mechanisms, and other security controls.	Incidents are logged by the employees and are assigned severity levels. Reported incidents are assigned to respective teams for analysis and resolution within stipulated SLA. **CA-21** Security incidents are reported, resolved as per the defined SLA and security incident report policy. **CA-22** Connections to Entity's internal network from External points are protected by a firewall, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices. **CA-47**
Cyfuture has made commitments to maintain and develop the skills and experience of Personnel by training and development, work experience, and otherwise as appropriate and in accordance with Good Industry Practice.	New employees are required to undergo security training at the time of induction. **CA-11** All employees undergo training as per the established process for annual security, confidentiality, and privacy training. **CA-20**
Cyfuture has made commitments to implement appropriate security and integrity procedures and practices for Personnel, including conducting background checks for, at a minimum, BPSS clearance or equivalent, subject to a written agreement with the Customer.	Before an employee or a third-party vendor/contractor is engaged by the entity, the third-party personnel undergo background screening. A background check includes, at a minimum, professional, educational, and employment checks. **CA-4**

Cyfuture will perform the services with due care, skill, and diligence in accordance with the standard practice in the IT industry and comply with any lawful and reasonable instructions of the user organization.	The entity has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements. **CA-19**

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR: TEST OF CONTROLS

Information Provided by Service Auditor Except for Applicable Trust Services Criteria and Controls

4.1 Objective of Our Examination

This report is intended to provide interested parties with information about the controls at Cyfuture that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the controls that were tested.

Our testing of Cyfuture's controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, Cyfuture's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Cyfuture our procedures included tests of the following relevant elements of the Cyfuture control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Cyfuture activities and operations, an inspection of Cyfuture documents and records, and re-performance of the application of Cyfuture controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine the Cyfuture description of the system related to Cyfuture as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period of 1st January 2023 to 31st July, 2023.

In selecting particular tests of the operational effectiveness of controls, we considered the (a) nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved and (d) the expected efficiency and effectiveness of the test.

Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Cyfuture. Our tests of controls were performed on controls as they existed during the period of 1st January 2023 to 31st July, 2023, and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the reporting period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the reporting period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicate the performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

4.4 Testing Procedures Performed By Independent Service Auditor

In addition to the tests listed below for each control specified by Cyfuture, ascertained through inquiry with management and the controlling owner that each control activity listed below operated as described throughout the period.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC1.1 CC2.2 CC5.2 CC5.3	CA-1	The entity has a documented Information security policy that is available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy is reviewed and approved by the management on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had a documented Information security policy that was available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy was reviewed and approved by the management on an annual basis. Inspected, Information security policy document to ascertain whether the entity had a documented Information security policy that was available at a centralized place to all employees. Information security policy clearly communicates the responsibilities of all employees. The policy was reviewed and approved by VP-IT on an annual basis.	No exception noted.

Information Provided by Service Auditor

CC1.1	CA-2	The entity has policies and procedures in place to establish acceptable use of information assets.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had policies and procedures in place to establish acceptable use of information assets. Inspected, acceptable usage policy to ascertain whether the entity had policies and procedures in place to establish acceptable use of information assets. The policy was reviewed and approved by VP-IT on an annual basis.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC1.1 CC1.5 CC2.2 CC6.6 CC9.2	CA-3	Employees and contractors are required to read and accept a Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether employees and contractors were required to read and accept Non-disclosure agreement to ensure confidentiality and follow privacy policy practices upon their hire and to formally reaffirm them annually thereafter. Inspected, acknowledged Non-Disclosure agreement to ascertain whether sample new joiners accepted the Non-Disclosure agreement upon their joining.	No exception noted.
CC1.1 CC1.4	CA-4	Before an employee or a third-party vendor/contractor is engaged by the entity, the third-party personnel undergo background screening. A background check includes, at a minimum, professional, educational, and employment checks.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether before an employee or a third party vendor/contractor was engaged by the entity, the third-party personnel undergo background screening. A background check includes, at a minimum, professional, educational, and employment checks. Inspected, for sample new joiners, background verification reports to ascertain whether before an employee or a third party vendor/contractor was engaged by the entity, the third-party personnel undergo background screening. A background check includes, at a minimum, professional, educational and employment checks.	No exception noted.

Information Provided by Service Auditor

CC1.1	CA-5	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties or subcontractors.	Confirmed via corroborative inquiry with Director of IT and Manager IT whether agreements were established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties or subcontractors. Inspected, sample agreement to ascertain whether agreements were established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties or subcontractors.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC1.2 CC1.3 CC1.4 CC1.5	CA-6	Entities have defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role. Inspected roles and responsibilities document to ascertain whether the entity had defined roles and responsibilities for each job role, which sets the boundaries for allowable activities within the designated role.	No exception noted.
CC1.2	CA-7	The entity has defined organizational structures, reporting lines, authorities, and responsibilities within the organization to meet its commitments and requirements as they relate to security, availability, confidentiality, and processing integrity.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had defined organizational structures, reporting lines, authorities, and responsibilities for the within the Organization to meet its commitments and requirements as they relate to security, availability, confidentiality, and processing integrity. Inspected organization chart to ascertain whether the entity had defined organizational structures, reporting lines, authorities, and responsibilities for the within the Organization to meet its commitments and requirements as they relate to security, availability, confidentiality and processing integrity.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC1.2 CC1.3 CC3.4	CA-8	Reporting lines and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether reporting lines and organizational structures were reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements. Inspected organization chart to ascertain whether reporting lines and organizational structures were reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	No exception noted.
CC1.4	CA-9	The entity has defined processes for hiring, training, and performance appraisal to enable that person to fulfill their responsibilities which are documented within the HR Policies. HR policies and procedures relating to recruitment and termination are maintained within the intranet portal.	Confirmed via corroborative inquiry with COO of IT and HR Manager whether the entity had defined processes for hiring, training, and performance appraisal to enable that person to fulfill their responsibilities which were documented within the HR Policies. HR policies and procedures relating to recruitment and termination were maintained within the intranet portal. Inspected HR policy and procedure document to ascertain whether the entity had defined processes for hiring, training, and performance appraisal to enable that person fulfill their responsibilities which were documented within the HR Policies. HR policies and procedures relating to recruitment and termination were maintained within the intranet portal.	No exception noted.
CC1.4	CA-10	The experience, competence and training of candidates for employment or assignment are evaluated before they assume the responsibilities of their position.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the experience, competence, and training of candidates for employment or assignment	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
			were evaluated before they assume the responsibilities of their position. Inspected sample new joiners inspected the candidate evaluation forms to ascertain whether the experience, competence, and training of candidates for employment or assignment were evaluated before they assume the responsibilities of their position.	
CC1.4 CC1.5	CA-11	New employees are required to undergo security training at the time of induction.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether new employees were required to undergo security training at the time of induction. Inspected sample new joiners inspected the training records to ascertain whether new employees were required to undergo security training at the time of induction.	No exception noted.
CC1.5	CA-12	Entity performs annual formal staff evaluation to assess alignment with company principles and objectives.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity performs annual formal staff evaluation to assess alignment with company principles and objectives. Inspected annual evaluation records to ascertain whether the entity performs annual formal staff evaluation to assess alignment with company principles and objectives.	No exception noted.
CC1.5 CC3.1 CC3.3 CC4.1 CC5.1 CC5.2 CC5.3	CA-13	Internal audits are performed annually and corrective plans are formulated based on recommendations. The audit report is shared with Senior Management on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether internal audits were performed annually and corrective plans were formulated based on recommendations. The audit report was shared with Senior Management on an annual basis. Inspected internal audit report to ascertain whether internal audits were performed annually and corrective plans were formulated based on recommendations. The audit report was shared with Senior Management on an annual basis.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC2.1	CA-14	The entity has defined and documented Standard Operating Procedures (SOP) for services provided to the Customers via SOC and CCC.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether the entity had defined and documented Standard Operating Procedures (SOP) for services provided to the Customers via CCC.	No exception noted.
A1.2 A1.3 CC2.1 CC5.1 CC7.5	CA-15	The entity has established Business continuity and disaster recovery plans and is tested annually. Business Continuity and disaster recovery plans are adjusted to accommodate any changes suggested basis the test results. BCP/DR plans are reviewed by the Director of IT on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had established Business continuity and disaster recovery plans and was tested annually. Inspected BCP/ DR policy to ascertain whether the entity had established Business continuity and disaster recovery plans and were tested annually.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC2.1 CC3.4 CC5.1 CC7.1 CC7.2	CA-16	Vulnerability scans and penetration testing are performed on an annual basis. Risks are identified are documented in the risk register along with the mitigation steps.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Vulnerability scans and penetration testing were performed on an annual basis. Risks were identified were documented in the risk register along with the mitigation steps. Inspected VA/PT report to ascertain whether Vulnerability scans and penetration testing were performed on an annual basis. Risks were identified were documented in the risk register along with the mitigation steps.	No exception noted.
CC2.1 CC3.1 CC5.1 CC5.3	CA-17	Cyber Essential audits are performed by an external vendor on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Cyber Essential audits were performed by an external vendor on an annual basis. Inspected Cyber Essential audit report to ascertain whether Cyber Essential audits was performed by an external vendor on an annual basis.	No exception noted.

CC2.2 CC2.3 CC7.2 CC7.3 CC7.4 CC7.5	CA-18	The entity has defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure are made available to the employees through the Intranet portal.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure were made available to the employees through the Intranet portal. Inspected Incident management policy to ascertain whether the entity had defined and documented the policies and procedures related to Incident management and problem management processes. The policy and procedure were made available to the employees through the Intranet portal.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
A1.1 CC2.2 CC2.3	CA-19	The entity has defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements. Inspected Master Service Agreement for sample client to ascertain whether the entity had defined and documented Service Level Agreements, Master Service Agreement, and Statement of Work with respect to clients in order to perform service responsibilities. The entity's availability, processing integrity (via SLA's), and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exception noted.

Information Provided by Service Auditor

CC2.2	CA-20	All employees undergo training as per the established process for annual security, confidentiality, and privacy training.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether all employees undergo training as per the established process for annual security, confidentiality, and privacy training. Inspected security training records to ascertain whether all employees undergo training as per the established process for annual security, confidentiality, and privacy training.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC2.2 CC2.3 CC7.3	CA-21	Incidents are logged by the employees and are assigned severity levels. Reported incidents are assigned to the respective teams for analysis and resolution within the stipulated SLA.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether incidents were logged by the employees and were assigned severity levels. Reported incidents were assigned to the respective teams for analysis and resolution within the stipulated SLA. Inspected, for sample incidents, incident records to ascertain whether incidents were logged by the employees and were assigned severity levels. Reported incidents were assigned to the respective teams for analysis and resolution within the stipulated SLA.	No exception noted.
CC2.2 CC2.3 CC7.3 CC7.4 CC7.5	CA-22	Security incidents are reported, resolved, and monitored as per the defined SLA and security incident reporting policy.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether security incidents were reported, resolved, and monitored as per the defined SLA and security incident reporting policy. Inspected, for sample security incidents, incident records to ascertain whether security incidents were reported, resolved, and monitored as per the defined SLA and security incident reporting policy.	No exception noted.

Information Provided by Service Auditor

CC3.1 CC3.2 CC3.3 CC3.4 CC9.1	CA-23	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether the entity had defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Inspected risk management policy to ascertain whether the entity had defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC3.1 CC3.2 CC3.3 CC3.4 CC4.2 CC9.1	CA-24	Identified risks within the entity are rated using a risk evaluation process and ratings are reviewed by the management.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Identified risks within the entity were rated using a risk evaluation process and ratings were reviewed by the management. Inspected risk register to ascertain whether Identified risks within the entity were rated using a risk evaluation process and ratings were reviewed by the management.	No exception noted.
CC3.1 CC3.2 CC3.3 CC3.4 CC4.2 CC9.1	CA-25	The risk response strategy is reviewed and approved by senior management. An owner is assigned for each remediation plan and is tracked for closure.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether risk response strategy was reviewed and approved by senior management. An owner is assigned for each remediation plan and were tracked for closure. Inspected risk register to ascertain whether risk response strategy was reviewed and approved by senior management. An owner is assigned for each remediation plan and were tracked for closure.	No exception noted.

CC3.2	CA-26	A master list of the entity's IT system components is maintained, accounting for additions and removals, for management's use.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the master list of the entity's IT system components was maintained, accounting for additions and removals, for management's use. Inspected asset register to ascertain whether the master list of the entity's IT system components was maintained, accounting for additions and removals, for management's use.	No exception noted.
CC4.1	CA-27	Management and internal audits periodically receive reports summarizing incidents, the root cause of incidents, and corrective action plans. Internal audit monitors for completion of corrective action plans.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether management and internal audit periodically receive reports summarizing incidents, the root cause of incidents, and corrective action plans. Internal audit monitors for completion of corrective action plans. Inspected internal audit report to ascertain whether management and internal audit periodically receive reports summarizing incidents, the root cause of incidents, and corrective action plans. Internal audit monitors for completion of corrective action plans.	No exception noted.
Criteria Reference	**Control No.**	**Control Activities**	**Testing Performed**	**Results of Tests**
CC4.1 CC6.6	CA-28	Entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system are raised to the respective team for further resolution.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system were raised to the respective team for further resolution. Inspected quarterly logging report to ascertain whether the entity performs logging of all network devices (routers, Switches, and Firewall) and servers via SIEM solution. Alerts from the system were raised to the respective team for further resolution.	No exception noted.

CC4.1 CC6.2	CA-29	The entity has established a process to annually review user access privileges for appropriateness and access revalidation.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether the entity had established a process to annually review user access privileges for appropriateness and access revalidation. Inspected user access review to ascertain whether the entity had established a process to annually review user access privileges for appropriateness and access revalidation.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC5.2 CC6.1 CC6.3	CA-30	The entity has developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of user access.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether the entity had developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of the user access. Inspected access management policy to ascertain whether the entity had developed and implemented logical access security policies and procedures to control access to system resources for provisioning, de-provisioning, and modification of the user access.	No exception noted.
CC5.2 CC8.1	CA-31	The entity has documented Change Management policy and process which is reviewed and approved by the Director of IT on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had documented Change Management policy and process which is reviewed and approved by COO of IT on an annual basis. Inspected Change Management policy to ascertain whether the entity had documented Change Management policy and process which is reviewed and approved by COO of IT on an annual basis.	No exception noted.

CC6.1	CA-32	Privileged access to sensitive resources is restricted to defined user roles, and logical access to these roles is approved by the COO of IT.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Privileged access to sensitive resources was restricted to defined user roles, and logical access to these roles was approved by the COO of IT. Inspected list of users having access to privileged rights to ascertain whether Privileged access to sensitive resources was restricted to defined user roles and logical access to these roles was approved by the COO of IT.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.1 CC6.7 PI1.2	CA-33	External access to an entity's environment by employees is permitted only through an encrypted virtual private network (VPN) connection.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether external access to entity's environment by employees was permitted only through an encrypted virtual private network (VPN) connection. Inspected VPN settings to ascertain whether external access to entity's environment by employees was permitted only through an encrypted virtual private network (VPN) connection.	No exception noted.
CC6.1	CA-34	Unique User ID is assigned to individuals to ensure accountability.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether unique user ID was assigned to individuals to ensure accountability. Inspected list of users to ascertain whether unique user ID was assigned to individuals to ensure accountability.	No exception noted.
CC6.1	CA-35	Password parameters for application and infrastructure are defined as per the Password Management Policy which is reviewed on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether password parameters for application and infrastructure were defined as per the Password Management Policy which was reviewed on an annual basis. Inspected password parameter and password policy to ascertain whether password parameters for application and infrastructure were defined	No exception noted.

			as per the Password Management Policy which was reviewed on an annual basis.	
CC6.2 CC6.3	CA-36	User accounts are created in IT systems/applications upon receiving a duly filled user access form along with approvals from relevant stakeholders.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether user accounts were created in IT systems/ applications upon receiving a duly filled user access form along with approvals from relevant stakeholders. Inspected, for sample new joiners, user creation forms to ascertain whether user accounts were created in IT systems/ applications upon receiving a duly filled user access form along with approvals from relevant stakeholders.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.2	CA-37	System security is configured to require users to change their passwords upon their initial system sign-on and thereafter follow the password policy configured within the Organization/within the Application.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether system security was configured to require users to change their passwords upon their initial system sign-on and thereafter following the password policy configured within the Organization/within the Application. Inspected password parameters to ascertain whether system security was configured to require users to change their passwords upon their initial system sign-on and thereafter follow the password policy configured within the Organization/within the Application.	No exception noted.

CC6.2 CC6.3	CA-38	When an employee resigns or transfers out of the Organization or Project, a request to revoke the user's access is initiated to respective teams. The IT team revokes user access based on the request on the last working day of the employee.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether when an employee resigns or transfers out of the Organization or Project, a request to revoke the user's access is initiated to respective teams. The team revokes user access based on the request on the last working day of the employee. Inspected, for sample leavers, exit checklist to ascertain whether when an employee resigns or transfers out of the Organization or Project, a request to revoke the user's access is initiated to respective teams. The team revokes user access based on the request on the last working day of the employee.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.4	CA-39	Access to the Entity's SOC and CCC are restricted to authorized personnel via a padlock and the combination is known only to appropriate individuals.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether access to the Entity's SOC and CCC was restricted to authorized personnel via a padlock and the combination is known only to appropriate individuals.	No exception noted.
CC6.4	CA-40	Visitors to the Entity's facility are required to submit details such as visitor's name, contact person within the Entity, and entry and exit times are recorded within the Visitor Register. Visitors are escorted by an employee from the reception at all times during their visit.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether visitors to the Entity's facility were required to submit details such as visitor's name, contact person within the Entity, and entry and exit time were recorded within the Visitor Register. Visitors were escorted by an employee from the reception at all times during their visit.	No exception noted.
CC6.4	CA-41	Entry keys are handed over by the human resources department during the joining of the employee and after all required background investigations are completed. Keys are to provide access only to non-sensitive areas within the Organization.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether entry keys were handed over by the human resources department during the joining of the employee and after all required background investigations were completed. Keys were to provide access only to non-sensitive areas within the Organization.	No exception noted.

Information Provided by Service Auditor

CC6.4	CA-42	The entity has established a process that, during the termination process, employees are required to return their entry keys and corresponding assets as part of their exit process.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had established a process that, during the termination process, employees were required to return their entry keys and corresponding assets as part of their exit process.	No exception noted.
CC6.4	CA-43	A monitoring process exists to monitor entry or exit points. Measures such as, but not limited to, alarm systems and surveillance cameras. The information (for example, logs, tapes, and so forth) is maintained for an agreed period of time for future reference.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether a monitoring process exists to monitor entry or exit points. Measures such as, but not limited to, alarm systems and surveillance cameras. The information (for example, logs, tapes, and so forth) was maintained for an agreed period of time for future reference.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.4	CA-44	Unauthorized access attempts are recorded and reviewed on a periodic basis. Appropriate corrective actions are taken against the identified defaulters.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether unauthorized access attempts were recorded and reviewed on a periodic basis. Appropriate corrective actions were taken against the identified defaulters.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
CC6.4	CA-45	Physical access to the Entity premises is reviewed periodically to ensure only authorized individuals have access to the facility.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether physical access to the Entity premises was reviewed periodically to ensure only authorized individuals had access to the facility. Inspected, user access review evidence to ascertain whether physical access to the Entity premises was reviewed periodically to ensure only authorized individuals had access to the facility.	No exception noted.

C1.2 CC6.5	CA-46	The entity has established a Data disposal policy which is aligned with Industry best practices for securely disposing off the data.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had established a Data disposal policy that was aligned with Industry best practices for securely disposing of the data. Inspected data disposal policy to ascertain whether the entity had established a Data disposal policy that was aligned with Industry best practices for securely dispose of the data.	No exception noted.
CC6.6	CA-47	Connections to Entity's internal network from External points are protected by a firewall, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether connections to Entity's internal network from External points were protected by a firewall, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices. Inspected firewall configuration to ascertain whether connections to Entity's internal network from External points were protected by a firewall, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.6	CA-48	Access to the firewall is provided only to appropriate individuals using AD authentication.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether access to the firewall was provided only to appropriate individuals using AD authentication. Inspected firewall configuration to ascertain whether access to the firewall was provided only to appropriate individuals using AD authentication.	No exception noted.

CC6.6	CA-49	Firewall logs are reviewed on a periodic basis and necessary corrective actions are taken in case any deviations are noted.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Firewall logs were reviewed on a periodic basis and necessary corrective actions were taken in case any deviations were noted. Inspected logging report to ascertain whether Firewall logs were reviewed on a periodic basis and necessary corrective actions were taken in case any deviations noted.	No exception noted.
CC6.7	CA-50	An entity has established a process to encrypt backups to ensure confidentiality and integrity of the information.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Entity had established a process to encrypt backups to ensure confidentiality and integrity of the information. Inspected backup policy to ascertain whether Entity has established a process to encrypt backups to ensure confidentiality and integrity of the information.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC6.8	CA-51	The ability to install applications on systems/servers is restricted to system administration personnel only.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the ability to install applications on systems/servers was restricted to system administration personnel only.	No exception noted.
CC6.8	CA-52	Antivirus software is installed on all the workstations, laptops, and servers supporting such software to protect them against malware. Antivirus software/agents are configured to receive an updated virus signature at least daily.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Antivirus software was installed on all the workstations, laptops, and servers supporting such software to protect them against malware. Antivirus software/agents were configured to receive an updated virus signature at least daily. Inspected antivirus software installed on sample workstations to ascertain whether Antivirus software was installed on all the workstations, laptops, and servers supporting such software to protect them against malware. Antivirus	No exception noted.

			software/agents were configured to receive an updated virus signature at least daily.	
CC7.1	CA-53	An entity has established Patch Management and Vulnerability management procedures to detect known vulnerabilities and monitor the systems. The policy and procedure are made available to the employees through the Intranet portal.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had established Patch Management and Vulnerability management procedures to detect known vulnerabilities and monitor the systems. The policy and procedure were made available to the employees through the Intranet portal. Inspected Patch Management and Vulnerability management procedures to ascertain whether the entity had established Patch Management and Vulnerability management procedures to detect known vulnerabilities and monitor the systems. The policy and procedure were made available to the employees through the Intranet portal.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC7.1	CA-54	Security patches are regularly applied to employee workstations, so that workstations stay up to date with an operating system version that is current, next most current, or without critical security gaps	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Security patches were regularly applied to employee workstations so that workstations stay up to date with an operating system version that was current, next most current, or without critical security gaps Inspected patching report to ascertain whether Security patches were regularly applied to employee workstations, so that workstations stay up to date with an operating system version that was current, next most current, or without critical security gaps.	No exception noted.

CC7.4 CC7.5	CA-55	Basis the root cause analysis of the reported Incidents, the Change Management process is invoked by raising a change request for the events that require permanent fixes.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the root cause analysis of the reported Incidents, the Change Management process was invoked by raising a change request for the events that require permanent fixes. Inspected, change tickets for sample changes to ascertain whether the root cause analysis of the reported Incidents, the Change Management process was invoked by raising a change request for the events that require permanent fixes.	No exception noted.
CC8.1	CA-56	System change requests are reviewed and approved by the owner of the infrastructure/software or Director of IT, prior to work commencing on the requested change. Separate personnel is responsible to authorize changes and implementing the changes.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether System change requests were reviewed and approved by the owner of the infrastructure/software or Director of IT, prior to work commencing on the requested change. Separate personnel were responsible to authorize changes and implementing the changes. Inspected, change request form for sample changes to ascertain whether System change requests were reviewed and approved by the owner of the infrastructure/software or COO of IT, prior to work commencing on the requested change. Separate personnel was responsible to authorize changes and to implement the changes.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC8.1 PI1.1 PI1.3	CA-57	System Changes are tested by appropriate individuals. Testing report is documented and deviations from planned results are analyzed and remediated.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether System Changes were tested by appropriate individuals. The testing report was documented and deviations from planned results were analyzed and remediated. Inspected, change tickets for sample changes to ascertain whether System Changes were tested by appropriate individuals. The testing report	No exception noted.

			was documented and deviations from planned results were analyzed and remediated.	
CC8.1	CA-58	Separate environments are used for testing the change prior to implementing it in production.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Separate environments were used for testing the change prior to implementation in production. Inspected test and production environment URLs to ascertain whether Separate environments were used for testing the change prior to implementation in production.	No exception noted.
CC8.1	CA-59	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality commitments, and system requirements throughout the change management process.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether System change requests were evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality commitments, and system requirements throughout the change management process. Inspected, change tickets for sample changes to ascertain whether System change requests were evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality commitments, and system requirements throughout the change management process.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC8.1	CA-60	The entity has established a process for automated patching of Windows machines (servers/desktops/laptops), which do not require separate change tickets raised for the same. Testing results are required to be documented and preserved for future reference for the same. Deviations are investigated and necessary corrective actions are taken.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had established a process for automated patching of Windows machines (servers/desktops/laptops), which do not require separate change ticket raised for the same. Testing results were required to be documented and preserved for future reference for the same. Deviations were investigated and necessary	No exception noted.

			corrective actions are taken.	
CC9.2	CA-61	The entity has a documented Vendor Management policy that guides personnel when performing the third-party risk assessment process. The policy is reviewed and approved by the Director of IT on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity had a documented Vendor Management policy that guides personnel when performing the third-party risk assessment process. The policy was reviewed and approved by the COO of IT on an annual basis. Inspected vendor management policy to ascertain whether the entity had a documented Vendor Management policy that guides personnel when performing the third-party risk assessment process. The policy was reviewed and approved by the COO of IT on an annual basis.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
CC9.2	CA-62	Entity performs an annual vendor assessment based on its Vendor Management Policy.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether the entity performs an annual vendor assessment based on its Vendor Management Policy. Inspected annual vendor assessment report to ascertain whether the entity performs an annual vendor assessment based on its Vendor Management Policy.	
A1.1	CA-63	Capacity management process is defined and documented which is reviewed and approved by the Director of IT on an annual basis.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether capacity management process was defined and documented which was reviewed and approved by COO of IT on an annual basis. Inspected capacity management process to ascertain whether capacity management processes were defined and documented which was reviewed and approved by COO of IT on an annual basis.	No exception noted.

Information Provided by Service Auditor

A1.1	CA-64	Critical infrastructure components are periodically reviewed for criticality classification and assignment of a minimum level of redundancy.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether critical infrastructure components were periodically reviewed for criticality classification and assignment of a minimum level of redundancy. Inspected capacity reports to ascertain whether Critical infrastructure components were periodically reviewed for criticality classification and assignment of a minimum level of redundancy.	No exception noted.
A1.1	CA-65	Forecasts reports are reviewed and approved by Senior Management to monitor and evaluate the current processing capacity and use of system components. Change requests are initiated if required and directed by the Senior Management based on approved forecasts.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Forecasts reports were reviewed and approved by Senior Management to monitor and evaluate current processing capacity and use of system components. Change requests were initiated if required and directed by the Senior Management based on approved forecasts. Inspected capacity reports to ascertain whether Forecasts reports were reviewed and approved by Senior Management to monitor and evaluate current processing capacity and use of system components.	

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
A1.2	CA-66	An entity has established a process for Physical and Environmental Security and has installed the following to ensure system availability: • Cooling systems • Backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Entity had established a process for Physical and Environmental Security and had installed the following to ensure system availability: • Cooling systems • Backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers Inspected Physical and Environmental Security to ascertain whether Entity has established a process for Physical and Environmental Security.	No exception noted.

Information Provided by Service Auditor

A1.2 PI1.1 PI1.4 PI1.5	CA-67	Daily incremental backups are performed using an automated system.	Confirmed via corroborative inquiry with the COO of IT and Manager IT whether daily incremental backups were performed using an automated system. Inspected backup logs to ascertain whether daily incremental backups were performed using an automated system.	No exception noted.
A1.2 PI1.5	CA-68	Backups are monitored for failure and the incident management process is invoked whenever applicable to ensure timely resolution of issues and availability of the backup system.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Backups are monitored for failure and the incident management process is invoked whenever applicable to ensure timely	The operating effectiveness of this control activity could not be tested as there was no related activity

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
			resolution of issues and availability of the backup system.	during the audit period.
A1.3	CA-69	Backup restoration testing is performed on an annual basis by the IT team.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether backup restoration testing was performed on an annual basis by the IT team. Inspected backup restoration logs to ascertain whether backup restoration testing was performed on an annual basis by the IT team.	No exception noted.
A1.3	CA-70	Fire drills are carried out by Local Authorities on an annual basis. Local authorities review the Fire extinguishers and other physical and environmental security mechanisms and report about their adequacy.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Fire drills were carried out by Local Authorities on an annual basis. Local authorities review the Fire extinguishers and other physical and environmental security mechanisms and report about their adequacy. Inspected fire drill report backup restoration logs to ascertain whether Fire drills were carried out by Local Authorities on an annual basis. Local authorities review the Fire extinguishers and other physical and environmental security	No exception noted.

			mechanisms and report about their adequacy.	
C1.1	CA-71	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity • has processes in place to delete confidential information in accordance with specific retention requirements. • deletes backup information in accordance with a defined schedule. requires approval for confidential information to be retained beyond its retention period and specifically marks such information for retention. • reviews annually information marked for retention.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether entity established written policies related to retention periods for the confidential information it maintains. Inspected data retention policy to ascertain whether entity established written policies related to retention periods for the confidential information it maintains.	No exception noted.

Criteria Reference	Control No.	Control Activities	Testing Performed	Results of Tests
PI1.1 PI1.3	CA-72	System alerts are analyzed on a semi-annual basis to co-relate them. Further, the problem management process is invoked basis the result of investigation and correlation.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether system alerts were analyzed on a semi-annual basis to co-relate them. Further, the problem management process is invoked basis the result of investigation and correlation.	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
PI1.1	CA-73	Monthly trend reports are reviewed by the respective lead for unusual trends and problems are created basis the result of the review (if any).	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Monthly trend reports were reviewed by the respective lead for unusual trends and problems are created basis the result of review (if any).	The operating effectiveness of this control activity could not be tested as there was no related activity during the audit period.
PI1.1	CA-74	Processing capacity is monitored on a monthly basis and forecasted to meet business requirements.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether processing capacity was monitored on a monthly basis and forecasted to meet the business requirement. Inspected capacity reports to ascertain whether processing capacity was monitored on a monthly basis and forecasted to meet business requirements.	No exception noted.

Information Provided by Service Auditor

PI1.1	CA-75	Logical access to stored data is restricted only to the appropriate administrators.	Confirmed via corroborative inquiry with COO of IT and Manager IT whether Logical access to stored data is restricted only to the appropriate administrators.	No exception noted.
PI1.2 PI1.5	CA-76	A mirror image of critical data files is replicated periodically and stored on the second system for use in recovery and restoration in the event of system disruption or outage.	restoration in the event of system disruption or outage. Inspected backup logs to the secondary system to ascertain whether A mirror image of critical data files are replicated periodically and stored on a second system for use in recovery and restoration in the event of a system disruption or outage.	No exception noted.