System and Organization Control (SOC 1) Type II Report

Cyfuture India Pvt. Ltd

Independent Service Auditors' Report on a Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability, Process Integrity & Privacy and the Suitability of the Design and Operating Effectiveness of Controls

From 1st July 2025 to 28th February 2026

Statement of Confidentiality

This report, including the Description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to relevant Security for the period from 1st July 2025 to 28th February 2026, 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. Any unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

Table Of Contents

Section 1 Assertion of Cyfuture India Pvt. Ltd. -Service Organization Management 6

1.1 Assertation Cyfuture India Pvt. Ltd., Service Organization Management 7

Section 2 Independent Service Auditor's Report 10

2.1 Scope 11

2.2 Cyfuture India Pvt. Ltd., Responsibilities 11

2.3 Service Auditors' Responsibilities 12

2.4 Service Auditor's Independence and Quality Control 12

2.5 Inherent Limitations 13

2.6 Description of Test Controls 13

2.7 Opinion 13

2.8 Restricted Use 13

Section 3 Description of System 15

3.1 Background and Overview of Cyfuture India Pvt. Ltd. 16

3.1.1 Board of Directors 16

3.1.2 Management's Philosophy and Operating Style 16

3.2 Overview of the services provided (Boundaries of the system) 17

3.3 Control Environment 17

3.3.1 Human Resources 18

3.3.1.1 Organization Structure 18

3.3.1.2 Organization Chart 19

3.3.1.3 Roles & Responsibilities 20

3.3.1.4 Human Resources Policies & Procedures 26
3.3.1.5 New Hire Procedures 27
3.3.1.6 Training & Awareness 27
3.3.1.7 Employee Terminations 27
3.3.1.8 Code of Conduct and Disciplinary Action 27
3.3.2 Risk Management & Assessment 28
3.3.3 Network Security 28
3.3.3.1 Firewall 29
3.3.3.2 Network and Endpoint Protection 30
3.3.3.3 Monitoring 30
3.3.4 Physical and Environmental Security 30
3.3.4.1 Server Room 30
3.3.4.2 Physical Access 30
3.3.4.3 Access to Server Room 31
3.3.4.4 Power Backup and Environmental Security 31
3.3.5 Vendor Management 31
3.3.6 Information & Communication 32
3.3.7 Electronic Mail (e-Mail) 32
3.3.8 Capacity Management 32
3.3.9 Vulnerability Scans & Security Audits 32
3.3.10 Patch Management 32
3.3.11 Help Desk 33
3.3.12 Change Management 33

3.3.13 Incident Response and Management 33
3.3.14 Logical Access 34
3.3.14.1 Security Authorization and Administration 34
3.3.14.2 Security Configuration 34
3.3.14.3 Administrative Level Access 34
3.3.15 Media Disposal 34
3.3.16 Backup and Recovery of Data 35
3.4 Control Objectives and Related Control Activities 35
3.4.1 Selection and Development of Control Activities 35
3.5 Complimentary Controls at user entities 37
3.5.1 Access Control Management 37
3.5.2 Data Encryption 37
3.5.3 Incident response 38
3.5.4 Contractual Arrangements 38
3.5.5 Other Controls 38
Section 4 Testing Matrices 39
4.1 Tests of Operating Effectiveness and Results of Tests 40
4.2 Independent Service Auditor's Description of Tests of Controls and Results 41

Section 1 Assertion of Cyfuture India Pvt. Limited-Service Organization Management

1.1 Assertation Cyfuture India Pvt. Ltd., Service Organization Management

cyfuture
Thinking Future. Moving Ahead.

CMMI. DEV/SVC APPRAISED
1,2,3 COMPLIANT
PCI DSS
ISO 9001:2015
ISO 27001:2022
ISO/IEC TS 20000-11:2021
ISO 22301:2019
ISO 14001:2015
Great Place To Work. Certified

Date: 02-04-2026

Management of Cyfuture India Pvt. Ltd. Assertion

We have prepared the accompanying description of **Cyfuture India Pvt. Ltd** for **"Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services"** throughout the period 1st July 2025 to 28th February 2026 ("the description"), for user entities of the system during all of the period 1st July 2025 to 28th February 2026 and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls, implemented by user entities themselves, when assessing the risks of material misstatement of user entities financial statements.

Cyfuture does not use any subservice organization.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Cyfuture's controls are suitably designed and operating effectively, along with related controls at Cyfuture. The description does not extend to controls of the user entities.

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

a) The description fairly presents the system made available to user entities of the system as during some or all from 1st July 2025 to 28th February 2026 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over "Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services". The criteria we used in making this assertion were that the description:

i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, as applicable

1. The types of services provided including, as appropriate, the classes of transactions processed
2. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
3. The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
4. How the system captures and addresses significant events and conditions other than transactions.
5. The process used to prepare reports and other information for user entities.
6. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the Cyfuture's controls.

7. Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. Includes relevant details of changes to the service organization's system during the period covered by the description.

iii. 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 user entities of the system and their user auditors, and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the description were suitably designed and operating effectively from 1st July 2025 to 28th February 2026 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of controls from 1st July 2025 to 28th February 2026. The criteria we used in making this assertion were that

i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of Cyfuture.

ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

c) The controls stated in the description operated effectively 1st July 2025 to 28th February 2026 to provide reasonable assurance that Cyfuture's service commitments and system requirement were achieved based on the applicable trust services criteria.

For Cyfuture India Pvt. Ltd

Name: Ajai Rai

Title: Chief Technology Officer

Date: 02-04-2026

Signature:

Cyfuture India Pvt. Ltd. NOIDA

Section 2 Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To management of Cyfuture India Pvt. Ltd.

2.1 Scope

We have examined the accompanying description titled "Cyfuture India Pvt. Ltd-Service Organization's Description of the Cyfuture India Pvt. Ltd. Processing System" (the "Description") for the period from **1st July 2025 to 28th February 2026**. Our examination was conducted in accordance with the AICPA's Statement on Standards for Attestation Engagements (SSAE) No. 18, which defines the criteria for a SOC 1 Type 2 engagement, and designed to evaluate the internal controls over financial reporting relevant to the services provided by Cyfuture India Pvt. Ltd. The controls and control objectives included in the Description are those that the management of Cyfuture believes are relevant to user entities' internal controls over financial reporting. The Description specifically excludes aspects of the system that are not deemed relevant to user entities' internal control over financial reporting.

The Description indicates that certain control objectives can only be achieved if complementary user entity controls, assumed in the design of Cyfuture's controls, are suitably designed and operating effectively, alongside the controls implemented by Cyfuture. Our examination did not extend to these complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. Our examination was limited to the controls described in the Description and related to the service organization's operations.

Cyfuture India Pvt. Ltd. does not use any subservice organization to host the Cyfuture Processing System. The description indicates that controls at Cyfuture are suitably designed and operating effectively to achieve Cyfuture's service commitments and system requirements based on the applicable trust services criteria. The description presents Cyfuture's controls, the applicable trust services criteria assumed in the design of Cyfuture's controls.

2.2 Cyfuture India Pvt. Ltd., Responsibilities

In section 1, Cyfuture has provided its assertion titled "Assertion of Cyfuture India Pvt. Ltd.-Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated in the description. Cyfuture is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description ; identifying the risks that threaten the achievement of control objectives; selecting the criteria stated in the assertion, and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

2.3 Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period 1st July 2025 to 28th February 2026. 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 involves the following:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

2.4 Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.
We applied the Statements on Quality Control established by the AICPA and, accordingly, maintained a comprehensive system of quality control.

2.5 Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in providing Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center Operations and DC Co-location Services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

2.6 Description of Test Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

2.7 Opinion

In our opinion, in all material respects, based on the criteria described in Cyfuture's assertion in Section 1:

a) The description presents the Cyfuture India Pvt. Ltd. processing system that was designed and implemented throughout the period of 1st July 2025 to 28th February 2026, in accordance with the description criteria;

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1st July 2025 to 28th February 2026, and as applicable user entities applied the complementary controls assumed in the design of Cyfuture controls throughout the period 1st July 2025 to 28th February 2026;

c) The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved stated in the description throughout the period of 1st July 2025 to 28th February 2026. and user entity controls assumed in the design of Cyfuture controls operated effectively throughout the period 1st July 2025 to 28th February 2026.

2.8 Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 (Testing Matrices) is intended solely for the information and use of management of Cyfuture, user entities of the Cyfuture Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center

Operations and DC Co-location Services some or all of the period 1st July 2025 to 28th February 2026; and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Accorp Partners CPA LLC

Accorp Partners CPA LLC
PAC-FIRM-LIC-47383
Kalispell, Montana
April 02, 2026

Section 3 Description of System

3.1 Background and Overview of Cyfuture India Pvt. Ltd.

Cyfuture India Pvt. Ltd. is a leading provider of comprehensive IT infrastructure and support services. The company offers a wide range of solutions, including Data Center and Co-Location services, Security Services, Dedicated and VPS Hosting, and Cloud Hosting tailored to meet diverse business needs. In addition to hosting services, Cyfuture excels in delivering exceptional Customer Support, Remote Technical Support, and Managed Services, ensuring seamless operations for its clients. These services are supported by robust IT, HR, Administration, and Legal frameworks, enabling Cyfuture to maintain high-quality standards and compliance across its offerings. With a focus on reliability, security, and innovation, Cyfuture empowers businesses to scale effectively and achieve operational excellence.

Cyfuture requires Directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the Company and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. CYFUTURE promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

3.1.1 Board of Directors

1. Mr. Anuj Bairathi – Founder & CEO
2. Mr. Gary Barlow – Director UK Operations
3. Mrs. Shilpi Agarwal – Chief Strategy Officer
4. Mr. Rana Ray – Chief Business Officer
5. Mr. Ravish Sharma – Chief Operating Officer
6. Mr. Munish Mahajan- Chief Human Resources Officer
7. Mr. Ajai Rai – Chief Technology Officer

3.1.2 Management's Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team to interact with operating management on a daily basis.

Confidential

3.2 Overview of the services provided (Boundaries of the system)

The specific products and services and location(s) included in the scope of the report are as below:

Products and Services in scope:
Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services
Geographic Location Scope:
Plot no 197/198 Noida Special Economic Zone Noida Dadri Road, Noida Phase II Noida -201305, Uttar Pradesh, India

3.3 Control Environment

Cyfuture has established an internal controls framework that reflects the overall control environment within the organization and its various processes, the risk assessment procedure, control activities that help in meeting the overall control objectives, information and communication, and monitoring components of internal control.

Cyfuture's governance strategy is designed to generate business value by concentrating on the most critical factors. The key principles driving this approach include:

- Transparency and Accountability
- Compliance
- Efficiency and Effectiveness
- Customer-Centric Approach
- Continuous Improvement
- Trust Integrity

Cyfuture looks at governance from a process perspective and provides regular updates on operational performance. The enhanced governance framework is highlighted below.

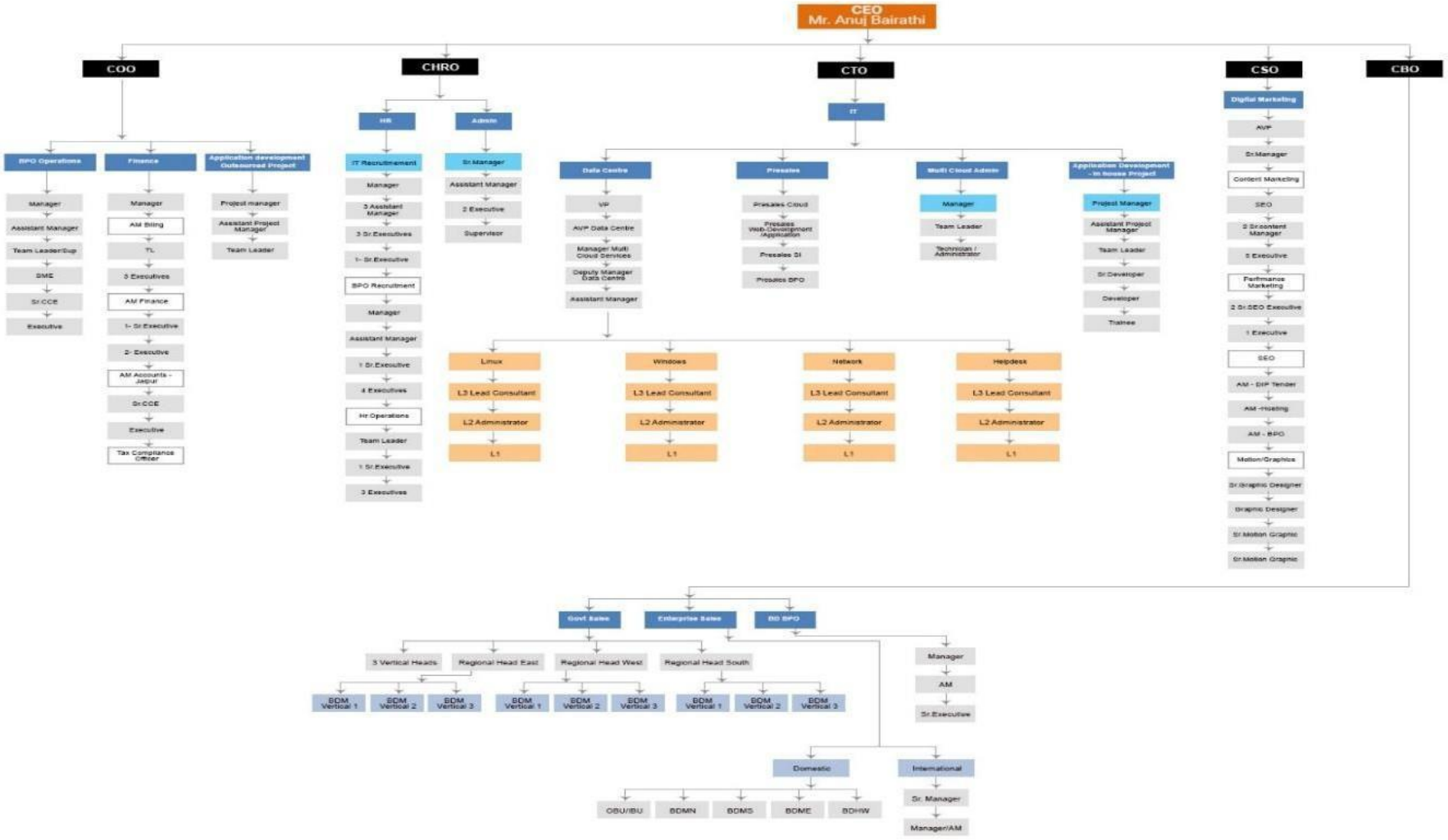
3.3.1 Human Resources

3.3.1.1 Organization Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to their job responsibilities. This approach helps to enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting clients.

The management team meets regularly to review business unit plans and performances. Meetings with the MD and department heads are held to review operational, security and business issues, and plans for the future.

3.3.1.2 Organization Chart



3.3.1.3 Roles & Responsibilities

Management is responsible for the assignment of responsibility and delegation of authority within Cyfuture.
The following are the responsibilities of key roles:

a. Role of IT Infra Head

- Organize management review meetings within stipulated intervals and report the performance of the Information Security System to top management.
- Availability of Infrastructure/Human Resource and Monitoring.
- Impart training on Information Security Systems throughout the Company.
- Initiate action on: Corrective action on non-conformities, Development activities to maintain and improve Information Security systems, to represent the needs of customers in internal functioning,
- Handling all Technical Issues.
- Ensure VAPTs are conducted on a Quarterly basis.

b. Role of CISO

- To work in co-ordination with the Information Security Management Team, issue guidelines, incorporate appropriate procedures, conduct routine internal audit checks to verify the compliance to the Information Security Policies and Procedures and detect incidents.
- Lead the System Administration Team and Information Security Management Team in the information security related activities.
- Prepare security briefs for the Information Security Management Team.
- Maintain Information Security Management System.
- Establish the Security Risk Assessment Process, and Review Risk Assessment Reports and status.
- Establish, support, control and mitigate risk by better the Risk management process for Information systems.
- Maintain the Statement of Applicability.
- Monitor ongoing compliance with security standards.
- Establish and maintain contacts with external security resources.
- Evaluate changes in asset base and resultant security implications.
- Manage the timely resolution of all issues and questions regarding responsibilities for Information security management within that relate to achieving and maintaining full compliance with the Information Security Policies and Procedures.
- Ensure that responsibilities are defined for, and that procedures are in effect, to promptly detect, investigate, report and resolve Information security

incidents within Cyfuture.

- Seek legal guidance in case of illegal activities or hacking related to Cyfuture. Notify such issues to the senior management and to the Information Security Management Team immediately.
- Evaluate and recommend new security products to be implemented across Cyfuture.
- Initiate protective and corrective measures if a security problem is discovered

c. Role of Compliance Head

- Defining the necessary level of knowledge on existing and emerging regulatory compliance requirements across the organization.
- Developing the annual compliance work plan that reflects the organization & unique characteristics.
- Guiding in a productive, professional way, the compliance teams.
- Providing strategic direction to the management team on compliance.
- Preparing and presenting clear and concise compliance reports to the Board.
- Interacting with regulators on compliance issues.
- Coordinating internal compliance review and monitoring activities
- Independently investigating and acting on matters related to compliance.
- Monitoring external review processes.
- Develop and implement company policies and regulation.
- Oversee all business operation relating to compliance including
- Policies and Procedure.
- Design and monitor control system to deal with violations of legal rules and internal policies
- Regularly assess the efficiency of the control system and recommend effective improvement.
- Review and evaluate company procedure and reports to identify hidden risks or common issues.
- Assist in conducting internal and external security audits to assess compliance with regulations and policies.
- Stay informed about industry best practices and security standards, implementing them to enhance the organization's security.
- Identify areas for improvement within the security program and propose enhancements to processes and procedures.

d. Role of Compliance Manager

- Achieve full compliance with all relevant laws, regulations, and standards
- Ensure that all employees are aware of and adhere to compliance requirements

- Identify, assess, and manage compliance risks to protect the organization from legal and financial penalties
- Ensure robust internal controls are in place to safeguard the organization's assets and data.
- Promote a culture of ethics and compliance throughout the organization.
- Ensure accurate and timely reporting of compliance activities and issues to senior management and stakeholders.
- Build and maintain a strong, skilled, and motivated compliance team.
- Effectively manage relationships with regulatory bodies, auditors, and external partners.
- Continuously improve compliance processes and procedures to enhance efficiency and effectiveness.
- Align compliance activities with the organization's strategic goals and support overall business objectives.
- Establish the organization as a leader in compliance and ethical business practices.

e. Role of Compliance Lead

- As per the requirement, design, develop, implement and analyze compliance programs for the Cyfuture Organization.
- Revise compliance programs as necessary to meet changing needs of Cyfuture organization.
- Proactively read through the compliance guidelines, requirements and standards.
- To review & guide against the policies & procedures to compliance executives.
- To coordinate & handle the external audits.
- Develop and implement a compliance program to ensure the organization operates in accordance with regulations.
- Although it led and motivated using leadership skills and qualities, there are the responsible duties for performance.
- Monitor and assess current projects compliance risks for.
- Contribute to the development and delivery of security awareness programs for employees
- Assist in conducting internal and external security audits to assess compliance with regulations and policies
- Monitoring compliance process - start to end.
- Identify areas for improvement within the security program and propose enhancements to processes and procedures
- Monitor the response to actual or suspected breaches in the confidentiality, integrity or availability of information assets**.**

f. Compliance Specialist

- Design, develop, implement and analyze compliance programs for the company.
- Revise compliance programs as necessary to meet changing needs of company.
- Proactively read through the compliance guidelines, requirements and standards.

- Compile and analyze both internal and external information to prepare compliance audit data & another checklist.
- Collect and coordinate internal compliance data with other departments to support said departments.
- Implement policies, procedures and systems to provide administrative support to departments.
- Answer questions regarding regulations to help other members or clients of company better understand.
- Study both existing and new legislation, enforce obedience to policies and advise management on necessary actions to make sure company complies with local, state and country legal requirements.
- Stay current on industry standards by continuing education, reading publications, talking with peers and joining professional groups.
- Explore new, innovative opportunities to add value to your job and the job of everyone in the company.
- Assist compliance manager to administer all processes and procedures and ensure working within regulation framework and develop and implement all policies and recommend ways to minimize risk.
- Educate staff about security risks, best practices, and proper handling of sensitive information
- Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of information assets**.**

g. Head – HR Operations

- Develop corporate plans for a variety of HR matters.
- Overseeing HR initiatives, systems, and tactics.
- Provide proactive and strategic guidance and support for organizational planning and development initiatives that align the human resources agenda in support of key business strategies and initiatives.
- Understand business strategies and how to develop high impact human capital solutions
- Have a data-driven mindset to assess organizational metrics and provide insights into the business
- Consistently measures the effectiveness of HR initiatives and programs to ensure they are delivering desired outcomes
- Help foster a culture of innovation, in an environment that requires high levels of scalability, security, and reliability
- Provide daily support to managers with employee attraction, development, and retention issues which may include: Annual reviews, Leadership coaching, Career pathing, Advanced HR reporting and metrics, Special project assistance
- Closely partner with HR Centers of Excellences and other HRBPs to deliver superior results to the business.
- Act to support the human factor in the company by devising strategies for performance evaluation, compensation, and system. etc.
- Supervise the work of the HR team and provide guidance.
- Deal with grievances and violations invoking disciplinary action when required.
- Report to senior management by analyzing data and using HR metrics.

- Oversee, refine, and execute employee standards and procedures, using and improving HR existing and recommended systems and processes.
- Maintain and enhance employee benefits programs, including compensation, health insurance, expenses, vacation, and other personnel packages.
- Ensure legal compliance by monitoring and implementing applicable HR federal and state requirements, conducting investigations, and maintaining records.
- Identify and recommend areas of improvement to internal standard operating procedures, including team restructuring and morale.
- Support departments in the development and delivery of strategic HR plans to fit with the overall business direction.
- Plan, monitor, and appraise HR activities by scheduling management conferences with employees, hearing and resolving employee grievances, training managers to coach and discipline employees, and counseling employees and supervisors.
- Champion the HR process, ensuring the process is up to date and of high quality, providing clarity and connection for all employees and their role in the overall vision.
- Maintain management guidelines by preparing, updating, and recommending human resource policies and procedures.
- Build strong relationships with external suppliers, fostering trust and promoting collaboration.
- Drive an effective client-service HR team that instils company-wide trust and value for the HR function
- Have executive presence and strong communication skills to partner with senior levels of management
- Strong collaboration skills within and outside of HR
- Serve as a role model, thought leader on Human Capital issues, and coaches other HRBPs in their development.
- Handle confidential matters with discretion.
- Knowledge of ISMS Required.

h. Purchase Head

- Overall responsibility for Purchasing and Cost Estimating activities across the business.
- Create and implement best practice purchasing vision, strategy, policies, processes and procedures to aid and improve business performance.
- Take ownership of the purchasing policy, guidelines and any associated documents.
- Approved / verify Purchase orders, invoices and other purchase documents to ensure value for money, quality standards and delivery terms with technical and operational after input from stakeholders where appropriate.
- Assist or provide inputs to finance for vendor payments and cash flow management.
- Provide / Approve / Verify input costing to the sales team for various projects.
- Initiate and develop creative and innovative purchase processes (CRM).
- Provide leadership to departments under control. Coach, mentor and develop direct reports and manage a high performing team that delivers

continuous improvement, benefit and cost reductions.

- Complete regular performance reviews, manage attendance, holidays, disciplinary issues and procedures as appropriate.
- Set department objectives and monitor ongoing progress and performance.
- Ensure strong communication between teams under leadership to facilitate exchange of information and in order to implement change and improvements.
- Input and hold responsibility for Purchasing and cost estimating budgets.

i. Purchase Executive

- Keep a track of Purchase Orders in the database.
- Tracking invoices received against purchase order issued.
- Verify purchase order details with respect to invoices received and other terms & conditions.
- Coordination with vendors regarding invoice related clarifications/issues.
- Get the credit notes where applicable especially ISP (Internet Service Provider) related invoices with SLA breach/service issue as far as up time are considered.
- Taking acceptance from the requestor/end user regarding services/material received against purchase order.
- Timely tax Invoice submission in accounts team.

j. Admin Specialist

- Manage relationships with vendors to ensure timely delivery of goods and services.
- Negotiate contracts and agreements to achieve cost-effective solutions.
- Supervise the upkeep and maintenance of office facilities, including HVAC, electrical, and other systems.
- Liaise with maintenance staff and contractors to address any issues promptly.
- Ensure all departmental administrative activities comply with company policies and local regulations.
- Plan and execute departmental events, meetings, and workshops.
- Handle event logistics, including venue selection, catering, and equipment setup.
- Monitor and manage departmental budgets for administrative activities.
- Optimize resource allocation to enhance operational efficiency.
- Identify inefficiencies in administrative processes and propose improvements.
- Implement best practices for effective office operations.

k. Admin General Manager

- Formulate and execute a comprehensive global administrative strategy aligned with corporate objectives.
- Identify opportunities for innovation and implement cutting-edge practices to enhance efficiency.
- Oversee administrative operations across multiple regions, ensuring consistency and best practices.
- Lead cross-regional teams to deliver high-quality administrative support and services.
- Develop and implement global SOPs to ensure standardized processes across all locations.
- Monitor compliance and regularly review practices to maintain consistency and efficiency.
- Provide visionary leadership to regional and global administrative teams.
- Build leadership pipelines by mentoring and developing future leaders within the administrative function.
- Drive the adoption of advanced global facility management tools and technologies.
- Lead digital transformation initiatives to modernize administrative operations.
- Manage and negotiate global vendor contracts, ensuring optimal cost efficiency and quality.
- Establish and monitor global vendor performance metrics.
- Oversee and manage global administrative budgets, ensuring efficient resource utilization.
- Identify cost-saving opportunities through strategic planning and innovative practices.
- Ensure adherence to global regulatory requirements and corporate policies.
- Develop and implement risk mitigation strategies for global administrative functions.
- Collaborate with corporate executives to align administrative strategies with overall organizational goals.
- Act as a trusted advisor to senior leadership on administrative operations.

3.3.1.4 Human Resources Policies & Procedures

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

The Human Resources department reviews these policies and procedures on a periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring during Induction. Personnel policies and procedures are documented in the Human Resources Policy on intranet.

3.3.1.5 New Hire Procedures

New employees are required to read and accept HR corporate policies and procedures and are provided online access to these policies along with an HR manual. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.
Reference checks are completed for prospective employees. Employees are required to sign Employee Confidentiality Agreement which forms an integral part of the employee file. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

3.3.1.6 Training & Awareness

Appropriate training enables employees & contractors to comply with their responsibilities as it relates to the Information Security Policy. All Cyfuture employees (including contractors) are subject to mandatory Security Awareness training upon onboarding and on monthly basis as refresher trainings. This training is managed and tracked to ensure organization-wide completion.
The HR Team maintains the records of such training programs.

3.3.1.7 Employee Terminations

Termination or change in employment is processed as per extant HR related procedures. There are clearly identified and assigned responsibilities regarding termination or change in employment. All employees, contractors and third-party personnel are required to return physical and digital Identification/access tokens provided to them by or its clients on their termination of employment or contract.
Access privileges are revoked upon termination of employment, contract or agreement. In case of change of employment/role, rights associated with prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

3.3.1.8 Code of Conduct and Disciplinary Action

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

3.3.2 Risk Management & Assessment

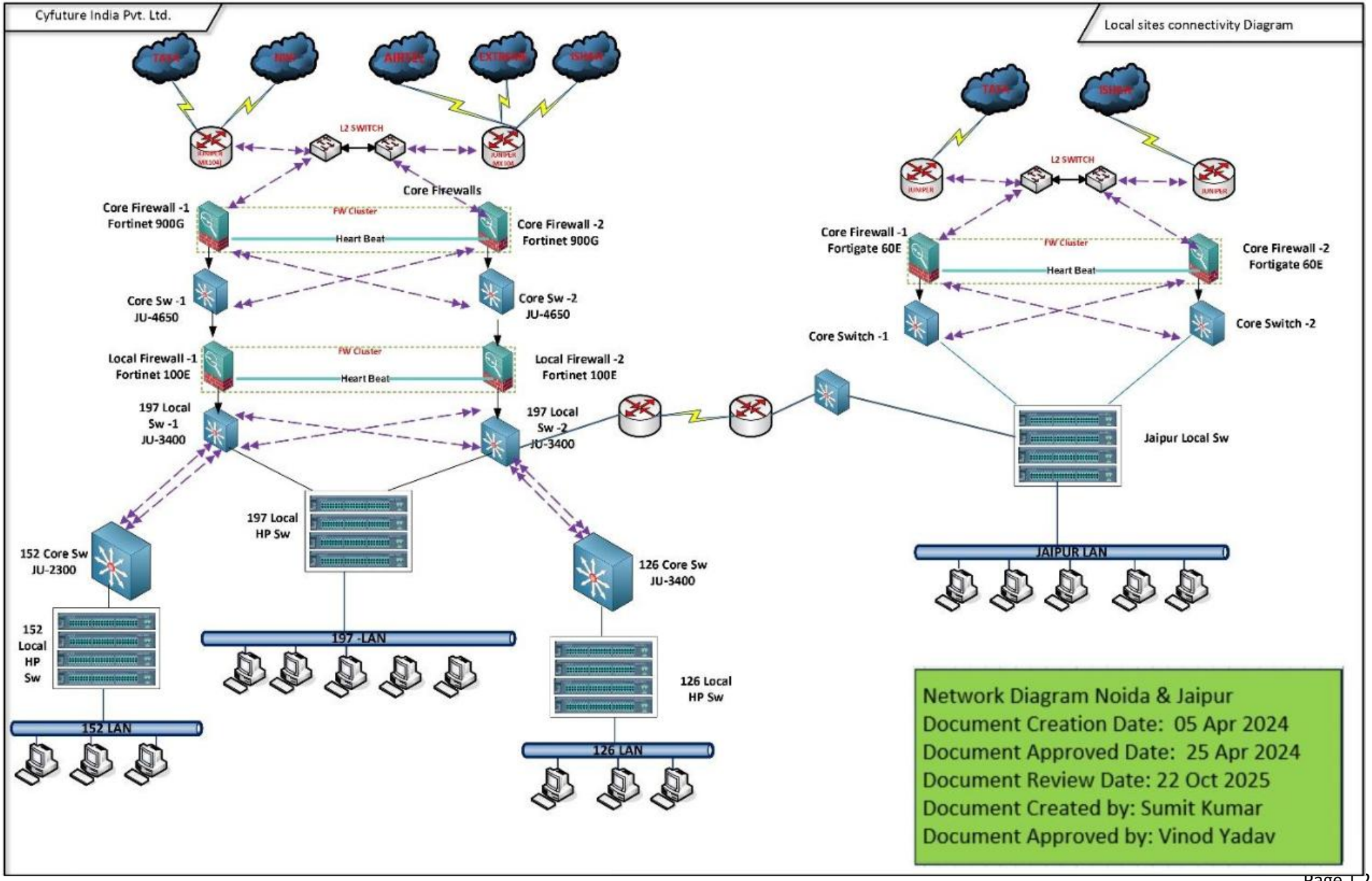
Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to Cyfuture. As part of this process, security threats are identified and the risk from these threats is formally assessed.
Cyfuture has operationalized a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of an Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.
Following steps are involved in performing risk assessments

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

Risk assessment comprises calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk and also to identify the areas where an organization needs to focus over information security. Apart from the asset-based risk assessment, the Company has also conducted organization-based risk assessment which is based on internal as well as external issues, needs and expectations of interested parties etc. The threats, vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

3.3.3 Network Security

Cyfuture has established a well-defined Network Security Policy, supported by an approved and up-to-date network diagram. The policy outlines clear guidelines for securing the network infrastructure, ensuring alignment with industry best practices. The network diagram provides a comprehensive view of the network's architecture, facilitating effective monitoring, management, and troubleshooting. These measures demonstrate Cyfuture commitment to maintaining a secure and resilient network environment, safeguarding its information assets against potential threats.


Cyfuture India Pvt. Ltd.
Local sites connectivity Diagram
L2 SWITCH
Core Firewalls
Core Firewall -1
Fortinet 900G
FW Cluster
Heart Beat
Core Firewall -2
Fortinet 900G
Core Sw -1
JU-4650
Core Sw -2
JU-4650
Local Firewall -1
Fortinet 100E
FW Cluster
Heart Beat
Local Firewall -2
Fortinet 100E
197 Local
Sw -1
JU-3400
197 Local
Sw -2
JU-3400
197 Local
HP Sw
197 -LAN
152 Core Sw
JU-2300
152
Local
HP
Sw
152 LAN
126 Core Sw
JU-3400
126 Local
HP Sw
126 LAN
L2 SWITCH
Core Firewall -1
Fortigate 60E
FW Cluster
Heart Beat
Core Firewall -2
Fortigate 60E
Core Switch -1
Core Switch -2
Jaipur Local Sw
JAIPUR LAN
Network Diagram Noida & Jaipur
Document Creation Date: 05 Apr 2024
Document Approved Date: 25 Apr 2024
Document Review Date: 22 Oct 2025
Document Created by: Sumit Kumar
Document Approved by: Vinod Yadav

3.3.3.1 Firewall

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

3.3.3.2 Network and Endpoint Protection

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

3.3.3.3 Monitoring

Cyfuture has implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

3.3.4 Physical and Environmental Security

3.3.4.1 Server Room

Cyfuture local servers including Domain Controller, Antivirus Server, AD Server, WSUS Server, and Tally Server with Backup server are hosted at the Cyfuture India server room. The server room offers multi- layered security that ensures compliance control for sensitive information. The server room is equipped with industry-standard controls for Physical Security including Temperature Control, Water and Temperature sensing alarm, Pest and rodent control, Fire suppression system. Access to the server room is controlled through biometric access. The entry and exit to the server room are monitored using CCTV Camera.

3.3.4.2 Physical Access

The entrance is secured with a security person, access control and CCTV surveillance. Physical and Environmental Security is controlled and governed by physical security policies forming part of the IS Policy. Entry to the Office premises is restricted to authorized personnel by a biometric access control system. These cards open the door lock. Attendance is recorded through biometric a system. All visitors have to sign the visitors register and are given inactive visitor

cards. Employees are subjected to show their ID cards at the Security entrance and swipe in/thumb print the access management system. Employees are granted access only to those areas which they are required to access. Some members of the IT Support Team & Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to wear their access cards/employee identification cards at all times while within the facility. CCTV is implemented to monitor the activities in the server room and main entrance and other secure zones. Admin Team monitors the CCTV recordings. Logs are generated and communicated to the management periodically. ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR sends an e-mail to IT the department requesting the IT team to issue an access card to the new employee. The IT team ensures that the access card/biometric controls configured with the appropriate access rights, and then issues the same to the employee. On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked.

Visitor Management System is implemented for entry to outsiders visiting the premises for any purpose. All visitors have to get approval prior to visit and make entry in the visitors register and are given a controlled visitor access card. Security guards control visitor access at all entrance points. Surveillance cameras have been installed at various critical points within & around the facility. Backup of recordings is stored for one month. Access by visitors, contractors and/or third-party support service personnel's both entry and exit are monitored by security personnel. Photography, video, audio or other recording equipment, are not allowed inside secure premises, unless specifically authorized. Such accesses are recorded, authorized and monitored. Visitor, contract and/or third-party service personnel to sensitive areas such as data centers are strictly on "need to have" basis and subject to the principle of least privileges, escorted, under video surveillance and supervised. Appropriate displays at the key entry points inform visitors of their responsibilities.

3.3.4.3 Access to Server Room

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

3.3.4.4 Power Backup and Environmental Security

Cyfuture's Offices power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises, UPS units and backup generators supply power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. Generators and UPS are under AMC for preventive maintenance. Fire extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked and AMC is entered on completion of Warranty. Periodic fire drills are conducted in coordination with Admin and HR personnel. The fire drills reports are collected and analysis made upon it.

3.3.5 Vendor Management

Cyfuture has a formal vendor assessment process in place to evaluate vendor security controls and processes governed by Cyfuture Vendor Management policy. During vendor onboarding and on a periodic basis, vendor's security controls are assessed, managed, and monitored to ensure an appropriate control environment consistent with Cyfuture security, availability, Processing Integrity, Privacy commitments.

Risk assessment procedures implemented by Cyfuture evaluate policies, processes, personnel, systems, and effectiveness of internal controls. The risk assessment is performed at least annually.

3.3.6 Information & Communication

Cyfuture has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures as part of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. Manager Service Delivery and Sr. Manager Operational Excellence are the focal points for communication regarding the service activity. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Cyfuture's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with employees.

3.3.7 Electronic Mail (e-Mail)

Communication to Customer organizations and project teams are done through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements. Cyfuture requires two factor authentications from employees to access their e- mails.

3.3.8 Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain Cyfuture's resources to ensure system performance meets the expected service levels and minimize the risk of systems failure and capacity related issues. Addition of new information systems and facilities, upgrades, new versions and changes are subject to formal system analysis, testing and approval prior to acceptance.

3.3.9 Vulnerability Scans & Security Audits

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

Confidential

3.3.10 Patch Management

The respective vertical team of Windows/Network team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. The patch management activity is done regularly or as and when any critical event occurs and required updates or patches are installed to ensure efficient working of the servers, desktops and critical network devices. Operating system patches related and marked critical and security are managed and applied as they become available, windows systems are managed through the patch management system and the network devices OS patching is managed automatically while renewed.

3.3.11 Help Desk

Cyfuture has put in place an IT helpdesk function to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to business and ensures that changes to any component of Cyfuture's information assets and infrastructure are controlled and managed in a structured manner.

3.3.12 Change Management

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

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

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

3.3.13 Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk or through email. For Network incidents, IT teams receive incident tickets via email and are resolved by them. The IT team operates 24X7 for all support functions. The help desk personnel or IT team study and escalate all security incidents to the designated team for further escalation/resolution. All security incidents are reviewed and monitored by the IT Team. Corrective and preventive actions are completed for incidents.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in

Confidential

accordance with defined policies and procedures and the actions proposed are approved by CSP Head.

3.3.14 Logical Access

3.3.14.1 Security Authorization and Administration

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

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles.
Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to IT teams and authorized users. Access to storage, backup data, systems, and media is limited to the IT team through the use of physical and logical access controls.

3.3.14.2 Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated with the associated password. Remote access to critical resources is not permitted to any employee. Passwords are controlled through Password policy of the domain controller and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.

3.3.14.3 Administrative Level Access

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

3.3.15 Media Disposal

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

Confidential

3.3.16 Backup and Recovery of Data

Cyfuture has developed formal policies and procedures relating to backup and recovery. Backup is defined in the Backup Policy. Suitable backups are taken and maintained. The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the "Backup_&_Backup_Encryption_Policy".

3.4 Control Objectives and Related Control Activities

3.4.1 Selection and Development of Control Activities

Control activities are a part of the process by which strives to achieve its business objectives. Cyfuture has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Cyfuture evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Cyfuture personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

Cyfuture control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Control Objective#	Control Area	Description
Control Objective 1	Organization and Management	Control activities provide reasonable assurance that senior management provides planning and oversight of the organization's activities
Control Objective 2	Personnel Security Procedures	Controls provide reasonable assurances that people related risks are mitigated and that all hiring, continued employment, transfers, and separation from employment are carried out by defined policies and procedures.
Control Objective 3	System Description and Communication	Controls provide reasonable assurance that system components are defined and communicated
Control Objective 4	Risk Management	Controls provide reasonable assurance that key risks are identified, and assessment and mitigation strategies are implemented promptly.
Control Objective 5	Network Security	Controls provide reasonable assurance that network systems are secured and available as per requirement.
Control Objective 6	Physical Security	Controls provide reasonable assurance that physical access to the work area, computer equipment, storage media, and customer-provided documentation is restricted to authorized individuals.
Control Objective 7	Incident Management	Controls provide reasonable assurance that security related incidents are reported, evaluated, and resolved promptly
Control Objective 8	Change Management	Controls provide reasonable assurance that security related incidents are reported, evaluated, and resolved promptly
Control Objective 9	System Availability	Controls provide reasonable assurance that systems are available as per defined SLA.
Control Objective 10	Environmental Safeguards	Controls provide reasonable assurance that adequate environmental safeguards have been enforced.
Control Objective 11	Third-Party Service Provider Security	Controls provide reasonable assurance that Third Party Service Providers are selected based on Vendor Selection Process, their roles and responsibilities, and performance requirements are formally defined and documented, and they are evaluated periodically.
Control Objective 12	Cloud Operations	Control activities provide reasonable assurance that cloud operations and client onboarding activities are comprehensive and as per defined onboarding processes.

3.5 Complimentary Controls at user entities

Cyfuture “Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center Operations and DC Co-location Services**”** system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to Cyfuture Services system to be solely achieved by Cyfuture control activities. Accordingly, user entities, in conjunction with the Cyfuture system, should establish their own internal controls or procedures to complement those of Cyfuture.

Examples in Practice:

If Cyfuture provides “Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center Operations and DC Co-location Services, they may implement encryption and firewalls as part of their controls to protect overall cloud infrastructure. However, they expect their clients/customers to manage their own user access to the platform sourced by them on Protean Cloud, through strong authentication controls. These client-side controls (CUECs) are necessary to complement the security measures taken by Protean Cloud and ensure a complete and effective security framework to protect client’s assets.

Here are some examples of Complementary User Entity Controls (CUECs), which are controls that a service organization (Cyfuture) expects from its user entities (clients/customers) to implement to complement the service organization's controls and help achieve control objectives:

3.5.1 Access Control Management

Client Responsibility: The user entity is responsible for managing its users' access to the Cloud Services system, ensuring that access rights are granted only to authorized individuals.

Example: The client should implement strong password policies, enforce multi-factor authentication (MFA), and conduct regular reviews of user access privileges.

3.5.2 Data Encryption

Client Responsibility: While the service organization may provide encryption for data in transit or at rest, the client is responsible for ensuring sensitive data are properly classified and encrypted before that are uploaded or transferred to the service provider.

Example: Clients should ensure encryption keys are securely managed, and that their own sensitive data are encrypted before transmission to the service organization.

3.5.3 Incident response

Client Responsibility: The user entity must have its own incident response procedures in place to detect, respond to, and mitigate potential security incidents related to its use of the service.
Example: A client should monitor logs for suspicious activity, maintain internal response plans, and coordinate with the service provider in case of a security breach.

3.5.4 Contractual Arrangements

User organizations are responsible for understanding and complying with their contractual obligations to such as providing input information, review and approval of processed output and releasing any instructions.

3.5.5 Other Controls

- User Organizations are responsible for ensuring end customer privacy.
- User Organizations are responsible for ensuring that complete, accurate and timely information is provided for processing.
- User Organizations are responsible for their network security policy and access management for their networks, application & data.
- User Organizations are responsible for working with to jointly establish service levels and revise the same based on changes in business conditions.

Section 4 Testing Matrices

4.1 Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to the providing Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center Operations and DC Co-location Services provided by Cyfuture. The scope of the testing was restricted to providing Data Center activities including Claims Provider Solutions, Claims Payer Solutions, Predictive Analysis, and SOC as a service, Customer Support, Remote technical support, Managed services, Cloud Services, Backup as a service and DR as a service, Data Center Operations and DC Co-location Services considered to be relevant to the internal control over financial reporting of respective user entities. Accorp Partners, conducted the examination testing over the period 1st July 2025 to 28th February 2026.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies

	and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Accorp Partners LLC, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the “Complementary Controls at User Entities” within Section 3.

Ref No	Control Area	Test Procedures	Test Results
1.	**Organization and Management** Control Objective: Control activities provide reasonable assurance that senior management provides planning and oversight of the organization's activities		
1.1	How does the company maintain its information security-related policies and procedures that describe information security processes, practices, and organization?	During the audit of Cyfuture, it was observed that the company has effectively maintained a well-defined Information Security Management System (ISMS) policy. This demonstrates the organization's commitment to ensuring the confidentiality, integrity, and availability of its information assets by implementing a structured approach to managing information security risks and ensuring compliance with industry standards and best practices. Verified DOC-CYF-ISMS-POL-014-ISMS Policy version 7.0 dated 22.10.2025	No exceptions noted
1.2	All new employees are required to attend induction training. They are also required to have their joining/appointment letter and the Code of Conduct. New employees must sign off to confirm that they have read this document.	During the audit of Cyfuture, it was observed that the company has provided the induction feedback form, offer letter, and training attendance sheet. This demonstrates the organization's commitment to maintaining proper documentation of employee onboarding, training, and feedback processes, ensuring compliance with internal policies and fostering a structured approach to employee development and engagement. Verified Offer Letter of Ms. Apoorva Saxena, join as Flutter Developer dated 09.09.2025 Verified Appointment Letter & NDA Signed by Ms. Apoorva Saxena dated 10.09.2025 Verified Appointment Letter & NDA of Ms. Nandini Kansal as Billing & Customer Executive dated 10.12.2025	No exceptions noted

		Verified Induction Feedback Form of Mr. Atul Ranjan Jha dated 12.09.2025 Verified Induction Feedback Form of Ms. Ms. Apoorva Saxena dated 12.09.2025	
1.3	Is the Non-Disclosure Agreement (NDA) included as part of the Code of Conduct and Data Protection Policy that all new joiners are required to sign upon joining?	During the audit of Cyfuture, it was observed that the company has effectively maintained a Non-Disclosure Agreement (NDA). This demonstrates the organization's commitment to safeguarding sensitive and confidential information by ensuring that appropriate legal protections are in place for employees, contractors, and third parties. Verified Appointment Letter & NDA Signed by Ms. Apoorva Saxena dated 10.09.2025 Verified Appointment Letter & NDA of Ms. Nandini Kansal as Billing & Customer Executive dated 10.12.2025	No exceptions noted
1.4	As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of all policies and procedures, which includes the Acceptable Use Policy (AUP).	During the audit, it was observed that the company has effectively maintained the Employee Acceptable Use Agreement Form and offer letter. This demonstrates the organization's commitment to clearly defining acceptable use of company resources and ensuring proper documentation of employee agreements, thereby promoting a secure and compliant work environment. Verified Employee Acceptable Use policy version 1.0 dated 22.10.2025.	No exceptions noted

1.5	Provides the Certification of Entity	During the audit of Cyfuture, it was observed that the company has maintained certifications on their website. This demonstrates the organization's commitment to transparency and compliance by making relevant certifications publicly available, showcasing their adherence to industry standards and best practices. Verified Certification of Cyfuture: - ISO 27001:2022 ISO 9001:2015 ISO 14001:2015 ISO 20000-1:2018 ISO 27017:2015 PCI-DSS-2025-COC QSA CGA-Cyfuture- 20000-9:2015 ISO 27701:2019 ISO 45001:2018 etc.	No exceptions noted
1.6	Vendor agreements, including any security, availability, and confidentiality commitments, are required by appropriate entity management during the procurement process.	During the audit of Cyfuture, it was observed that the company has effectively maintained the SLAs, Supplier Re-evaluation form. This demonstrates the organization's commitment to regularly assessing and ensuring the continued reliability and compliance of its suppliers, thereby supporting effective risk management, and maintaining high standards in the supply chain. Verified- Vendor agreements & Supplier Re-evaluation Forms 2025	No exceptions noted

1.7	Management review meetings, headed by the CISO, are required to be held every year to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.	During the audit of Cyfuture, it was observed that the company has provided the management MRM (Management Review Meeting) documentation. This demonstrates the organization's commitment to regularly evaluating and improving its management system, ensuring alignment with business objectives and compliance with relevant standards and regulations. Verified CYF-ISMS-PRO-006-Management Review Meeting Procedure version 7.0 dated 22.10.2025 Verified Management review meeting (MRM) for April & October 2025	No exceptions noted
1.8	The management team is required to meet quarterly to discuss both business and operational issues.	During the audit of Cyfuture, it was observed that the company has provided the management MRM (Management Review Meeting) documentation. This demonstrates the organization's commitment to regularly evaluating and improving its management system, ensuring alignment with business objectives and compliance with relevant standards and regulations. Verified Management review meeting (MRM) for April & October 2025.	No exceptions noted

1.9	An organizational chart is required to depict authority, reporting roles, and responsibilities for the management of its information systems. These charts need to be communicated to employees and updated as needed when agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities.	During the audit of Cyfuture, it was observed that the company has provided evidence of roles and responsibilities and included the organization chart. This demonstrates the organization's commitment to clearly defining and communicating roles and responsibilities within the company, ensuring effective governance and alignment with operational and strategic objectives. Verified Organization Hierarchy & CYF- ISMS-MGT-002-CFT Roles responsibilities version 4.0 dated 22.10.2025	No exceptions noted
1.10	The company requires information security-related policies and procedures that describe information security processes, practices, and organization.	During the audit of Cyfuture, it was observed that the company has effectively maintained a well-defined Information Security Management System (ISMS) policy. This demonstrates the organization's commitment to ensuring the confidentiality, integrity, and availability of its information assets by implementing a structured approach to managing information security risks and ensuring compliance with industry standards and best practices. Verified DOC-CYF-ISMS-POL-014-ISMS Policy version 7.0 dated 22.10.2025	No exceptions noted

1.11	Information Security policies and procedures related to HR policies are required to be approved by management at least annually.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Human Resource Security Policy. This demonstrates the organization's commitment to safeguarding its information assets by ensuring proper security measures are in place throughout the employee lifecycle, from recruitment to termination, in accordance with best practices and regulatory requirements. Verified CYF-ISMS-POL-010-Human Resource Security Policy version 5.0 dated 22.10.2025	No exceptions noted

2	**Personnel security procedures:** Controls provide reasonable assurances that people related risks are mitigated and that all hiring, continued employment, transfers and separation from employment are carried out in accordance with defined policies and procedures.		
2 A	**New Hire Procedures**		
2A.1	The company requires documented HR policies and procedures, including recruitment, training, and exit procedures.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Human Resource Security Policy and Exit Interview form. This demonstrates the organization's commitment to ensuring security throughout the employee lifecycle, from onboarding to exit, by implementing necessary policies and procedures to manage human resource-related security risks effectively. Verified CYF-ISMS-POL-010-Human Resource Security Policy version 5.0 dated 22.10.2025.	No exceptions noted
2A.2	Job requirements must be documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Job Descriptions (JD). This demonstrates the organization's commitment to clearly defining roles and responsibilities, ensuring alignment with business objectives, and promoting transparency in employee expectations and organizational structure. Verified Job Description (JD) of Content Writer & BID Manager and Interview Invitations Verified JD communication of IT Manager with internal team dated 28.02 2026	No exceptions noted

2A.3	New employees are required to sign their offer letters, indicating their agreement and acceptance of the broad terms of employment, including a brief description of the position and other terms.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Job Descriptions (JD). This demonstrates the organization's commitment to clearly defining roles and responsibilities, ensuring alignment with business objectives, and promoting transparency in employee expectations and organizational structure. Verified Offer Letter of Ms. Apoorva Saxena, join as Flutter Developer dated 09.09.2025 Verified Appointment Letter & NDA Signed by Ms. Apoorva Saxena dated 10.09.2025 Verified Appointment Letter & NDA of Ms. Nandini Kansal as Billing & Customer Executive dated 10.12.2025	No exceptions noted
2A.4	How are internal HR reference checks conducted by the HR team or the hiring manager, through document verification and reference checks with former colleagues or managers provided in the resume?	During the audit of Cyfuture, it was observed that the company has provided the background verification report. This demonstrates the organization's commitment to ensuring the integrity and trustworthiness of its employees by conducting thorough background checks as part of its recruitment process. Verified Background verification report of Mr. Ramesh Kumar Meena dated 10th June 2025, Report Status- Green Verified Background verification report of Mr. Sushanta Debbarma dated 3rd Jan 2025, Report Status- Green	No exceptions noted

2A.5	How are background verification checks conducted for new hires by the internal HR team? This includes verification of education qualifications and employment history. If a negative background verification report is found, the offer is revoked.	During the audit of Cyfuture, it was observed that the company has provided the background verification report. This demonstrates the organization's commitment to ensuring the integrity and trustworthiness of its employees by conducting thorough background checks as part of its recruitment process. Verified Background verification report of Mr. Ramesh Kumar Meena dated 10th June 2025, Report Status- Green Verified Background verification report of Mr. Sushanta Debbarma dated 3rd Jan 2025, Report Status- Green	No exceptions noted
2A.6	Does the company have any contract employees working on existing projects?	Not Applicable	No exceptions noted

2 B	Training and Competency		
2B.1	Newly hired personnel are required to undergo sufficient training before assuming the responsibilities of their new position.	During the audit of Cyfuture, it was observed that the company has provided the training calendar, employee handbook, and master list of HR policies. This demonstrates the organization's commitment to employee development, clear communication of workplace expectations, and ensuring that comprehensive HR policies are in place to support a well-structured and compliant work environment. Training Attendance sheet of Java Script for Full Stack Developer Jan 2025-26 Verified Induction Feedback Form of Mr. Atul Ranjan Jha dated 12.09.2025 Verified Induction Feedback Form of Ms. Ms. Apoorva Saxena dated 12.09.2025 Verified CFI/IV/HRM/FT/25 -Training calendar 2025	No exceptions noted
2B.2	The induction training provided by HR includes information security training. This training must cover HR policies, physical access policies, and security policies.	During the audit of Cyfuture, it was observed that the company conducts induction training for employees. This demonstrates the organization's commitment to effectively onboarding new employees, ensuring they are well-informed about company policies, procedures, and their roles, thus promoting a smooth integration into the organization. Verified CFI/IV/HRM/FT/25 -Training calendar 2025 & Training Invite	No exceptions noted

2B.3	An awareness refresher training is required to be provided to all employees. It is conducted quarterly to ensure that all employees are covered at least once a year.	During the audit of Cyfuture, it was observed that the company conducts awareness training for employees. This demonstrates the organization's commitment to fostering a culture of security and compliance by ensuring that employees are regularly educated on relevant policies, procedures, and best practices to mitigate risks and support organizational objectives. Verified CFI/IV/HRM/FT/25 -Training calendar 2025 & Training Invite Verified Induction Feedback Forms 2025 Verified Induction Feedback Form of Mr. Atul Ranjan Jha dated 12.09.2025 Verified Induction Feedback Form of Ms. Ms. Apoorva Saxena dated 12.09.2025 Cyber Security Best Practices for Web dated 21.03.2025. CMMI training conducted dated 31.12.2025	No exceptions noted
2B.4	The HR team is required to maintain training calendars. They circulate an email to all employees informing them about scheduled trainings for the particular month, including ISMS awareness sessions.	During the audit of Cyfuture, it was observed that the company has provided the training calendar. This demonstrates the organization's commitment to structured and planned employee development by scheduling training sessions that align with organizational goals and compliance requirements. Verified CFI/IV/HRM/FT/25 -Training calendar 2025 & Training Invite. & ISMS Presentation Cyfuture. Cyber Security Best Practices for Web dated 21.03.2025. CMMI training conducted dated 31.12.2025	No exceptions noted

2B.5	Roles and responsibilities are required to be defined in written job descriptions and communicated to employees and their managers.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Job Descriptions (JD). This demonstrates the organization's commitment to clearly defining roles and responsibilities, ensuring alignment with business objectives, and promoting transparency in employee expectations and organizational structure. Verified Job Description (JD) of Content Writer & BID Manager and Interview Invitations. Verified JD communication of IT Manager with internal team dated 28.02 2026	No exceptions noted
2B.6	Job descriptions are required to be reviewed by entity management on an annual basis as part of performance appraisals.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Job Descriptions (JD). This demonstrates the organization's commitment to clearly defining roles and responsibilities, ensuring alignment with business objectives, and promoting transparency in employee expectations and organizational structure. Verified Job Description (JD) of Content Writer & BID Manager and Interview Invitations. Verified JD communication of IT Manager with internal team dated 28.02 2026	No exceptions noted

2B.7	How are internal audits performed in the company, and how are the results communicated and corrective actions monitored?	During the audit of Cyfuture, it was observed that the company has maintained the Internal Audit Policy. This demonstrates the organization's commitment to ensuring regular, systematic evaluations of its internal processes and controls to identify areas for improvement and ensure compliance with relevant standards and regulations. DOC- CYF-ISMS-POL-016-Internal Audit Policy version 7.0 dated 22.10.2025 CYF-ISMS-REC-001-Internal Audit Plan 2025 CYF-ISMS-REP-001-CYF Internal Audit Assessment Record conducted dated 18.04.2025 and 24.10.2025.	No exceptions noted
2B.8	A meeting is required to be carried out quarterly to hold department discussions and provide status updates.	During the audit of Cyfuture, it was observed that the company conducts internal departmental meetings. This demonstrates the organization's commitment to fostering communication, collaboration, and alignment across departments, ensuring that operational objectives are met and any challenges are addressed in a timely manner. Verified Management review meeting (MRM) for April & October 2025 DC DR & Cybersecurity Meeting – 11 Nov 2025	No exceptions noted

3	**System Description and Communication:** Controls provide reasonable assurance that system components are defined and communicated		
3.1	System boundaries, both logical and physical, are required to be documented. Network diagrams must be in place. System boundaries should be shared with customers when required.	During the audit of Cyfuture, it was observed that the company has provided the network diagram. This demonstrates the organization's commitment to maintaining a clear and comprehensive representation of its network infrastructure, which supports effective security management, risk assessment, and overall system reliability. Verified Cyfuture DC DR Network diagram dated 22.10.2025	No exceptions noted
3.2	Customer responsibilities and appropriate system descriptions are provided in client contracts-MSA.	During the audit of Cyfuture, it was observed that the company customer responsibilities and the relevant system descriptions are outlined in the Service Agreement provided to clients. Verified SLA Signed with Clients 2025. SLA Signed with Cyfuture Smriti Bank Final & Webmyne. ASD Service Agreement dated 01.11.2025	No exceptions noted
3.3	External Client communication is carried out on a timely manner by the Project Manager / IT Head using a standard client specific escalation matrix.	During the audit of Cyfuture, it was observed that the company has established escalation matrix is shared with clients, detailing the designated company's points of contact for various levels of support. This structured framework facilitates clear and efficient communication, allowing clients to escalate issues appropriately based on their urgency or nature, thereby ensuring prompt and effective resolution. Verified Escalation Matrix.	No exceptions noted

3.4	How should HR communicate the hiring of new employees at senior levels to stakeholders via email?	During the audit of Cyfuture, it was observed that the company communicates with senior managers when hiring senior-level employees. This demonstrates the organization's commitment to involving key stakeholders in the recruitment process, ensuring that hiring decisions align with organizational goals and leadership requirements. Verified NOC and SOC Team Member 2025-26 Verified Entry-exit tracker.	No exceptions noted
3.5	The company's security, availability, and confidentiality commitments regarding the system must be included in the client contracts / SOW.	During the audit of Cyfuture, it was observed that the company has maintained the Service Level Agreement (SLA). This demonstrates the organization's commitment to clearly defining expectations and responsibilities regarding service delivery, ensuring that both parties understand the agreed-upon terms for performance, quality, and timelines. Verified MP CSP SOW_R1_310524 & SLA Signed with Clients.	No exceptions noted
3.6	How should the security policies be communicated to all employees?	During the audit, it was observed that Cyfuture effectively communicated its policies to all employees. The policies were made accessible through an internal system and employees were required to acknowledge and accept them. Verified Awareness ISMS Awareness & Protection Against Spam Emails – Best Practices 2025	No exceptions noted

3.7	Customer specific SLA are monitored on monthly basis. These are shared with customers based on the customer requirements.	During the audit of Cyfuture, it was observed that the company's customer-specific Service Level Agreements (SLAs) are monitored on a monthly basis to ensure performance meets agreed standards. SLA reports are shared with customers according to their specific requirements, providing transparency and accountability in service delivery. Verified email invite of Request to Share Monthly Cloud System Availability Reports. Verified SLA Signed with Cyfuture Smriti Bank Final & Webmyne. ASD Service Agreement dated 01.11.2025	No exceptions noted
3.8	Customer responsibilities are described in client contracts - MSA	During the audit, it was observed that the company's customer responsibilities and the relevant system descriptions are outlined in the Service Agreement provided to clients. Verified MSA Agreement- CRM doc 6-RFP & SLA Signed with Clients. Verified SLA Signed with Cyfuture Smriti Bank Final & Webmyne. ASD Service Agreement dated 01.11.2025	No exceptions noted
3.9	How do customers provide their issues, complaints, or feedback to business heads? Employees must raise their complaints and grievances with HR.	During the audit, it was observed that Cyfuture has maintained a comprehensive Employee Grievance Handling Policy. The policy outlines clear procedures for employees to report grievances, ensuring that any concerns are addressed in a timely and effective manner. Verified Grievance Handling Policy Verified Ticket Portal, Ticket responses Verified Employees Complaint & Grievance process mail & Warning Letter.	No exceptions noted

4	**Risk Management:** Controls provide reasonable assurance that key risks are identified, assessment and mitigation strategies implemented in a timely manner.		
4.1	Policies and procedures related to risk management are required to be developed, implemented, and communicated to personnel.	During the audit, it was observed that Cyfuture has maintained a well-defined Risk Management Procedure. The procedure outlines the process for identifying, assessing, and mitigating risks, ensuring that potential threats to the organization are effectively managed. DOC- CYF-ISMS-PRO-005-Risk Management Procedure version 7.0 dated 22.10.2025	No exceptions noted
4.2	A risk assessment should be performed annually or whenever there are changes in the security posture.	During the audit, it was observed that Cyfuture has maintained a well-defined Risk Management Procedure. The procedure outlines the process for identifying, assessing, and mitigating risks, ensuring that potential threats to the organization are effectively managed. DOC- CYF-ISMS-PRO-005-Risk Management Procedure version 7.0 dated 22.10.2025 Risk register version 8.0 dated 22.11.2025	No exceptions noted
4.3	Identified risks should be rated and prioritized based on their likelihood, impact, detection, and the effectiveness of existing control measures.	During the audit, it was observed that Cyfuture has maintained a well-defined Risk Management Procedure. The procedure outlines the process for identifying, assessing, and mitigating risks, ensuring that potential threats to the organization are effectively managed. DOC- CYF-ISMS-PRO-005-Risk Management Procedure version 7.0 dated 22.10.2025 Risk register version 8.0 dated 22.11.2025	No exceptions noted
4.4	How are information assets identified?	During the audit, it was observed that Cyfuture has maintained an Asset Classification Policy and an up-to-date Asset Register. The policy provides clear guidelines for classifying and handling assets based on their sensitivity and	No exceptions noted

		value, while the asset register effectively tracks and manages the company's assets. CYF-ISMS-POL-015- Asset Classification version 1.0 dated 22.10.2025 CYF-ISMS-POL-003-Asset Management Policy version 1.0 dated 22.11.2025 Asset Register version 13.0 dated 22.10.2025	
4.5	How does the company conduct vulnerability assessments and penetration tests annually?	During the audit, it was observed that Cyfuture conducts regular vulnerability assessments. These assessments are performed systematically to identify and address potential security vulnerabilities, ensuring that the company's systems and infrastructure are adequately protected against threats. CYF-ISMS-POL-028- Vulnerability Management Policy version 7.0 dated 22.10.2025 Verified Cyfuture Internal VAPT Report September-2025_	No exceptions noted
4.6	How does the company maintain a list of all hardware assets?	During the audit, it was observed that Cyfuture has maintained an Asset Classification Policy and an up-to-date Asset Register. The policy provides clear guidelines for classifying and handling assets based on their sensitivity and value, while the asset register effectively tracks and manages the company's assets. CYF-ISMS-POL-015- Asset Classification version 1.0 dated 22.10.2025 CYF-ISMS-POL-003-Asset Management Policy version 1.0 dated 22.11.2025 Asset Register version 13.0 dated 22.10.2025	No exceptions noted

4.7	Management should evaluate the effectiveness of controls and mitigation strategies in addressing identified risks and recommend changes based on its evaluation.	During the audit, it was observed that Cyfuture evaluates the effectiveness of its controls and mitigation strategies in addressing identified risks. The company conducts regular assessments to ensure that the implemented controls remain effective in managing risks. Verified Management review meeting (MRM) for April & October 2025 DC DR & Cybersecurity Meeting – 11.11.2025	No exceptions noted

5	**Network Security:** Controls provide reasonable assurance that network systems are secured and available as per requirement.		
5.1	The company must have documented procedures for logical access controls.	During the audit, it was observed that Cyfuture has maintained a comprehensive Access Control Policy. The policy outlines clear guidelines for granting, reviewing, and revoking access to the organization's systems and data based on role and responsibility. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-001-Access Control Policy version 1.0 dated 22.10.2025	No exceptions noted
5.2	Access should be granted on a least privileges basis by default.	During the audit, it was observed that Cyfuture has maintained an Access Control Policy that ensures access is granted based on the principle of least privilege. The policy defines clear guidelines for granting and managing user access to systems and resources, ensuring that individuals have only the minimum level of access necessary to perform their job functions. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-001-Access Control Policy version 1.0 dated 22.10.2025 Access Types and Review Records version 13.0 dated 22.10.2025	No exceptions noted
5.3	Physical and logical diagrams of networking devices for the office network must include routers, firewalls, switches, servers (including wireless devices), and be documented.	During the audit of Cyfuture, it was observed that the company has provided the network diagram. This demonstrates the organization's commitment to maintaining a clear and comprehensive representation of its network infrastructure, which supports effective security management, risk assessment, and overall system reliability. Verified Cyfuture DC DR Network diagram dated	No exceptions noted

		22.10.2025	
5.4	The company should not allow customers or external users to access its systems.	During the audit, it was observed that Cyfuture has maintained an Access Control Policy that ensures access is granted based on the principle of least privilege. The policy defines clear guidelines for granting and managing user access to systems and resources, ensuring that individuals have only the minimum level of access necessary to perform their job functions. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025	No exceptions noted
5.5	The company should maintain a VPN/remote working policy that requires external access to be granted on a need basis.	During the audit, it was observed that Cyfuture has maintained an VPN setup process that requires external access to be granted on a need basis. Verified VPN_server_client_setup	No exceptions noted
5.6	The IT department should maintain an up-to-date list of all software.	During the audit, it was observed that Cyfuture has provided a comprehensive list of software in use across the organization. This list includes all authorized and licensed software, ensuring that the company maintains proper software management and complies with licensing agreements. Verified List of Approved Software's version 1.0 dated 04.02.2025	No exceptions noted

5.7	All assets should be assigned to owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed.	During the audit, it was observed that Cyfuture has maintained an Asset Classification Policy and an up-to-date Asset Register. The policy provides clear guidelines for classifying and handling assets based on their sensitivity and value, while the asset register effectively tracks and manages the company's assets. Asset Register version 13.0 dated 22.10.2025	No exceptions noted
5.8	Privileged access to sensitive resources should be restricted to defined user roles, and access to these roles must be approved by management.	During the audit, it was observed that Cyfuture has maintained an Access Control Policy that ensures access is granted based on the principle of least privilege. The policy defines clear guidelines for granting and managing user access to systems and resources, ensuring that individuals have only the minimum level of access necessary to perform their job functions. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025 Access Types and Review Records version 13.0 dated 22.10.2025. Verified access provisioning email sent for access of all cloud VPN and background Infra Access dated 06.02.2026	No exceptions noted
5.9	The password parameters must be in place for active directory: - length of 8-character length - complexity is enabled - password expires in 30 days password history is set at 5	During the audit, it was observed that Cyfuture has maintained a robust Password Policy, along with supporting evidence of password configuration. The policy outlines the requirements for creating, managing, and securing passwords, ensuring that strong authentication measures are in place. Verified CYF-ISMS-POL-019-Password Policy version 1.0 dated 22.10.2025 Verified Passwords Configuration Screenshot	No exceptions noted

5.10	When an employee leaves the organization, the employee's manager should initiate the 'Exit Process'. HR must inform respective teams/IT team within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist should be used to ensure compliance with termination procedures.	During the audit of Cyfuture, it was observed that the company has effectively maintained the Human Resource Security Policy. This demonstrates the organization's commitment to safeguarding its information assets by ensuring proper security measures are in place throughout the employee lifecycle, from recruitment to termination, in accordance with best practices and regulatory requirements. Verified CYF-ISMS-POL-010-Human Resource Security Policy version 5.0 dated 22.10.2025 Verified Employee Entry Exit Tracker & Employees Exit Process 2025	No exceptions noted
5.11	A role-based security process should be set up in Active Directory with groups and roles based on job requirements.	During the audit, it was observed that Cyfuture has maintained an Access Control Policy that ensures access is granted based on the principle of least privilege. The policy defines clear guidelines for granting and managing user access to systems and resources, ensuring that individuals have only the minimum level of access necessary to perform their job functions. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-001-Access Control Policy version 1.0 dated 22.10.2025 Verified AD policy & Access Types and Review Records version 13.0 dated 22.10.2025	No exceptions noted

5 A	Network Security (Firewall)		
5A.1	External points of connectivity at office network must be protected by firewall.	During the audit, it was observed that Cyfuture has maintained comprehensive firewall configuration evidence. The configurations demonstrate that the company has implemented appropriate firewall rules and security measures to protect its network from unauthorized access and potential threats. Verified Firewall policy CYF-ISMS-POL-018-Network Security Policy version 1.0 dated 22.10.2025	No exceptions noted
5A.2	Incoming connection must be accepted from only whitelisted IPs in the firewall.	During the audit, it was observed that Cyfuture has maintained comprehensive firewall configuration evidence. The configurations demonstrate that the company has implemented appropriate firewall rules and security measures to protect its network from unauthorized access and potential threats. Verified Firewall policy & Whitelisted IP's	No exceptions noted
5A.3	Are customer responsibilities outlined and described within client contracts, Master Service Agreements (MSAs), or Service Level Agreements (SLAs)	During the audit of Cyfuture, it was observed that the company has maintained the Service Level Agreement (SLA). This demonstrates the organization's commitment to clearly defining expectations and responsibilities regarding service delivery, ensuring that both parties understand the agreed-upon terms for performance, quality, and timelines. Verified SLA signed with Tata Teleservices dated 25.06.2025	No exceptions noted

5A.4	Users should be informed of the process for reporting complaints and security Breaches during induction Security Training.	During the audit, it was observed that Cyfuture ensures users are informed of the process for reporting complaints and security breaches during their induction security training. Verified CYF-ISMS-PRO-007-Incident Management Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-011-Incident Management Policy version 7.0 dated 22.10.2025	No exceptions noted
5A.5	How does the company implement a content filtering system through the firewall that blocks access to certain sites, such as personal emails and storage?	During the audit, it was observed that Cyfuture implements web filtering as part of its security measures. This proactive control helps restrict access to potentially harmful or inappropriate websites, enhancing the protection of the organization's network and systems from online threats. Verified Firewall policy and CYF-ISMS-POL- 018-Network Security Policy version 1.0 dated 22.10.2025	No exceptions noted
5A.6	Access to modify firewall rules should be restricted by management.	During the audit, it was observed that Cyfuture has maintained an Access Control Policy that ensures access is granted based on the principle of least privilege. The policy defines clear guidelines for granting and managing user access to systems and resources, ensuring that individuals have only the minimum level of access necessary to perform their job functions. CYF-ISMS-POL-018-Network Security Policy version 1.0 dated 22.10.2025 CYF-ISMS-POL-001-Access Control Policy version 1.0 dated 22.10.2025 Access Types and Review Records version 13.0 dated 22.10.2025, Firewall Policy and worksheet Review conducted in 2025-26.	No exceptions noted

5 B	Network Security (Encryption)		
5B.1	Entity policies should prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	During the audit, it was observed that Cyfuture has maintained a comprehensive Network Security and Encryption Policy. The policy outlines clear guidelines for securing the organization's network infrastructure and ensuring the protection of sensitive data through encryption techniques. Verified DOC- CYF-ISMS-POL-018-Network Security, Encryption & information Transfer Policy version 1.0 dated 22.10.2025	No exceptions noted
5B.2	How external users access applications hosted in the cloud.	During the audit, it was observed that Cyfuture has maintained a comprehensive Network Security and Encryption Policy. The policy outlines clear guidelines for securing the organization's network infrastructure and ensuring the protection of sensitive data through encryption techniques. Verified DOC- CYF-ISMS-POL-018-Network Security, Encryption & information Transfer Policy version 1.0 dated 22.10.2025	No exceptions noted
5B.3	The use of removable media must be prohibited by policy, except when authorized by management.	During the audit, it was observed that Cyfuture has maintained a Secure Media Disposal Policy. The policy outlines the procedures for securely disposing of sensitive media and ensures that all data is effectively destroyed to prevent unauthorized access or data breaches. Verified DOC- CYF-ISMS-POL-037-Cyfuture Secure Media Disposal Policy version 1.0 dated 22.10.2025 Verified Removable-Media-Policy.	No exceptions noted

5B.4	Does the company install antivirus software on workstations, laptops, and servers?	During the audit, it was observed that Cyfuture has provided evidence of anti-virus configuration. The configuration details confirm that anti-virus software is actively deployed and properly configured across the organization's systems to detect and prevent potential threats. Verified Antivirus-Signatures & Dashboard	No exceptions noted
5B.5	Signature files should be updated daily, and the antivirus console is required to provide compliance reports about non-updated machines.	During the audit, it was observed that Cyfuture has maintained an Anti-Virus Policy and provided supporting evidence of its anti-virus configuration. Verified Antivirus-Signatures & Dashboard CYF-ISMS-POL-002-Antivirus Policy version 7.0 dated 22.10.2025	No exceptions noted
5B.6	The ability to install software on workstations and laptops must be restricted to IT support personnel through domain policies. Local admin access should be given only when approved by the IT Infrastructure Head, based on demonstrated need.	During the audit, it was observed that Cyfuture has provided evidence of administrative user accounts. This evidence includes a list of authorized admin users, ensuring that access to critical systems and resources is properly controlled and monitored. Verified Firewall policy Verified Approved Software list CYF-ISMS-POL-018-Network Security Policy version 1.0 dated 22.10.2025	No exceptions noted
5B.7	Any viruses discovered should be reported to IT team either by the antivirus system or by the affected employees.	During the audit, it was observed that Cyfuture has maintained an Anti-Virus Policy and provided supporting evidence of its anti-virus configuration. No virus discovered within the period from July to February 2025. Verified Antivirus-Signatures & Dashboard CYF-ISMS-POL-002-Antivirus Policy version 7.0 dated 22.10.2025	No exceptions noted

6	**Physical Security:** Controls provide reasonable assurance that physical access to the work area, computer equipment, storage media, and customer provided documentation is restricted to authorized individuals.		
6.1	The entity needs to implement a strong perimeter at the premises and deploy all security controls, including people, processes, and technological equipment.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025	No exceptions noted
6.2	Physical access to office premises should be monitored through CCTV installed at key points within the premises.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy and provided supporting evidence in the form of CCTV records. The policy outlines the measures in place to safeguard the organization's premises and assets, while the CCTV records demonstrate effective monitoring and incident tracking. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 Verified CCTV Inventory Record	No exceptions noted
6.3	There should be a security desk at the office entry manned by a security guard	During the audit, it was observed that Cyfuture has maintained the presence of a security guard at the office desk and provided the agreement detailing the terms and responsibilities of the security service. Verified - Security Guard Agreement	No exceptions noted
6.4	All visitors are required to enter their details in the visitor register.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats.	No exceptions noted

		Verified DC Entry register 2025 DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025	
6.5	ID cards should include an employee picture which must be worn at all times when accessing or leaving the facility.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 Employee ID Cards.	No exceptions noted
6.6	Physical access should be set up by the HR Department for new joiners after all HR formalities are completed. ID cards do not have access to any of the sensitive areas by default.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 Verified DC-Access Provisioning 2025-2026	No exceptions noted
6.7	Upon the last day of employment, the HR team must send an exit email requesting deactivation of physical access for terminated employees.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 Verified Access Revoke Request.	No exceptions noted

6.8	Employees must be required to return their ID cards on the last day, and all ID badges are to be disabled.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy and provided evidence of administrative clearance processes. This evidence confirms that access to restricted areas is granted only to authorized personnel following proper clearance procedures. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 Verified Priyanshu Sahu & Sumitesh Exit Process & Returned ID Card.	No exceptions noted
6.9	Is the sharing of access badges and tailgating prohibited?	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025	No exceptions noted

7	**Incident Management:** Controls provide reasonable assurance that security related incidents are reported, evaluated and resolved in a timely manner.		
7 A	System Operations		
7A.1	Hardening Policy should be in place for hardening of IT infrastructure/desktops	During the audit, it was observed that Cyfuture has maintained comprehensive hardening guidelines for networks, Windows, and Linux systems. These documents outline the security measures and configurations required to protect the organization's systems from vulnerabilities and unauthorized access. CYF-ISMS-POL-030 Patch Management.doc Malicious Code Prevention Policy version 1.0 dated 22.10.2025 Verified System Hardening Standard version 4.0 dated 22.10.2025 Verified Linux Server Hardening	No exceptions noted
7A.2	How the IT team receive requests to reset user, passwords etc.	During the audit, it was observed that Cyfuture has provided evidence of user password reset processes. This evidence demonstrates that the organization has implemented secure and well-documented procedures for resetting user passwords, ensuring adherence to security best practices and reducing the risk of unauthorized access. Verified CYF-ISMS-POL-019-Password Policy version 1.0 dated 22.10.2025 Verified User Password Reset 2025	No exceptions noted
7A.3	A formal, defined incident management process must be documented in Security Incident Management Policy for evaluating reported events.	During the audit, it was observed that Cyfuture has maintained a comprehensive Incident Management Policy. The policy outlines the processes for identifying, reporting, responding to, and resolving security incidents, ensuring that the organization is prepared to handle potential threats effectively.	No exceptions noted

		Verified CYF-ISMS-PRO-007-Incident Management Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-011-Incident Management Policy version 7.0 dated 22.10.2025	
7A.4	Reported incidents should be logged as tickets and include the following details Severity Data and Time of incident Details Status Root Cause (for urgent & high incidents only)	During the audit, it was observed that Cyfuture has maintained a comprehensive Incident Management Policy and provided evidence of incident response tickets. The policy outlines procedures for identifying, reporting, and managing incidents, while the ticket evidence demonstrates the effective implementation of these procedures. Verified Incident Portal & Incident Tickets. Verified CYF-ISMS-PRO-007-Incident Management Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-011-Incident Management Policy version 7.0 dated 22.10.2025 Verified RCA Incident tickets 2025-26	No exceptions noted
7A.5	Change management requests must be opened for events that require permanent fixes.	During the audit, it was observed that Cyfuture has maintained a robust Change Management process. This process includes well-defined procedures for requesting, reviewing, approving, and implementing changes to systems and processes, ensuring minimal disruption and maintaining security and compliance. Verified Change tracker & Change tickets from 2025 to 2026 CYF-ISMS-POL-004-Change Management Procedure version 7.0 dated 22.10.2025	No exceptions noted

7A.6	All incidents should be evaluated and necessary action taken should be taken to close the threat/vulnerability.	During the audit, it was observed that Cyfuture has maintained a comprehensive Incident Management Policy and provided evidence of incident response tickets. The policy outlines procedures for identifying, reporting, and managing incidents, while the ticket evidence demonstrates the effective implementation of these procedures. Verified Incident Portal & Incident Tickets. Verified CYF-ISMS-PRO-007-Incident Management Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-011-Incident Management Policy version 7.0 dated 22.10.2025	No exceptions noted

8.	**Change Management:** Controls provide reasonable assurance that changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with policies, commitments, and requirements.		
8.1	All change requests should be submitted with implementation and back up plans.	During the audit, it was observed that Cyfuture has maintained a robust Change Management process. This process includes well-defined procedures for requesting, reviewing, approving, and implementing changes to systems and processes, ensuring minimal disruption and maintaining security and compliance. CYF-ISMS-POL-004-Change Management Procedure version 7.0 dated 22.10.2025 Verified Change tracker & Change tickets from 2025 to 2026	No exceptions noted
8.2	Changes should be communicated to the appropriate client and user community if the change has any potential impact on the user base.	During the audit, it was observed that Cyfuture has maintained a robust Change Management process. This process includes well-defined procedures for requesting, reviewing, approving, and implementing changes to systems and processes, ensuring minimal disruption and maintaining security and compliance. CYF-ISMS-POL-004-Change Management Procedure version 7.0 dated 22.10.2025 Verified Change tracker & Change tickets from 2025 to 2026	No exceptions noted

8.3	All change requests should be logged and change request ticket must be created in email. Ticket details change type (Standard, Minor, Major) and priority of action (low, medium, high & mandatory)	During the audit, it was observed that Cyfuture has maintained a robust Change Management process. This process includes well-defined procedures for requesting, reviewing, approving, and implementing changes to systems and processes, ensuring minimal disruption and maintaining security and compliance. CYF-ISMS-POL-004-Change Management Procedure version 7.0 dated 22.10.2025 Verified Change tracker & Change tickets from 2025 to 2026	No exceptions noted
8.4	A process should be existed to manage mandatory changes. Mandatory changes, due to their urgent nature, must be performed without prior review.	During the audit, it was observed that Cyfuture has maintained a robust Change Management process. This process includes well-defined procedures for requesting, reviewing, approving, and implementing changes to systems and processes, ensuring minimal disruption and maintaining security and compliance. CYF-ISMS-POL-004-Change Management Procedure version 7.0 dated 22.10.2025 Verified Change tracker & Change tickets from 2025 to 2026	No exceptions noted

8 A	**Software Development Lifecycle (SDLC)**		
8.A1	Where is the software code is maintained?	Not Applicable	No exceptions noted
8.A2	Are software development changes tested through both unit testing and QA testing, with each of these activities being documented and monitored in change requests? Additionally, are test plans utilized by the QA team for testing	Not Applicable	No exceptions noted
8.A3	Is there a formal release process in place for releasing builds, where release notes specify what is included in the release, and the testing team conducts comprehensive testing of the release	Not Applicable	No exceptions noted
8.A4	What development methodologies are used for development?	Not Applicable	No exceptions noted
8.A5	How often is the application updated or patched?	Not Applicable	No exceptions noted
8.A6	How is the quality of the code maintained (e.g., code reviews, automated testing)?	Not Applicable	No exceptions noted
9	**System Availability:** Controls provide reasonable assurance that systems are available as per defined SLA.		
9.1	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements	During the audit, it was observed that Cyfuture has provided evidence of capacity monitoring and alert mechanisms. The evidence demonstrates that the company actively monitors system capacity and resource utilization, with alerts configured to notify relevant personnel of potential issues. Verified Screenshot Capacity Monitoring and Management-Network Verified CYF-ISMS-POL-031-Audit Log and Monitoring Policy version 7.0 dated 22.10.2025 CYF-ISMS-POL-021-Capacity Management Policy version 7.0 dated 22.10.2025 Inspected Capacity Management Records & Ticket portal 2025-2026.	No exceptions noted

9 A	System Availability (Backup Procedures)		
9A.1	Backup policy should be defined in the information security policies.	During the audit, it was observed that Cyfuture has maintained a comprehensive Data Backup and Restoration Policy. The policy outlines procedures for regularly backing up critical data and ensuring its timely restoration in the event of data loss or system failure. Verified CYF-ISMS-POL-006-Data Backup and Restoration Policy 7.0 dated 22.10.2025 CYF-ISMS-POL-008-Data Backup and Restoration Procedure 7.0 dated 22.10.2025 Verified Backup Screenshots 2025-26	No exceptions noted
9A.2	Manual backup should be done to perform scheduled weekly full backup of production systems	During the audit, it was observed that Cyfuture has maintained a comprehensive Data Backup and Restoration Policy and provided evidence of regular backups. The policy outlines procedures for data backup and restoration, while the evidence demonstrates that Cyfuture conducts frequent backups to ensure data integrity and availability. Verified CYF-ISMS-POL-006-Data Backup and Restoration Policy 7.0 dated 22.10.2025 CYF-ISMS-POL-008-Data Backup and Restoration Procedure 7.0 dated 22.10.2025 Verified Backup Screenshots 2025-26	No exceptions noted

9A.3	Local office backup must be carried out.	During the audit, it was observed that Cyfuture has maintained a comprehensive Data Backup and Restoration Policy and provided evidence of regular backups. The policy outlines procedures for data backup and restoration, while the evidence demonstrates that Cyfuture conducts frequent backups to ensure data integrity and availability. Verified Backup Screenshots 2025-26 Verified CYF-ISMS-POL-006-Data Backup and Restoration Policy 7.0 dated 22.10.2025 CYF-ISMS-POL-008-Data Backup and Restoration Procedure 7.0 dated 22.10.2025	No exceptions noted
9A.4	No backups should be performed on external hard drives or tapes.	During the audit, it was observed that Cyfuture has maintained a comprehensive Data Backup and Restoration Policy and provided evidence of regular backups. The policy outlines procedures for data backup and restoration, while the evidence demonstrates that Cyfuture conducts frequent backups to ensure data integrity and availability. Verified Backup Screenshots 2025-26 Verified CYF-ISMS-POL-006-Data Backup and Restoration Policy 7.0 dated 22.10.2025 CYF-ISMS-POL-008-Data Backup and Restoration Procedure 7.0 dated 22.10.2025	No exceptions noted

9A.5	Disaster recovery and Business Continuity plans and procedures for various disruption scenarios should be documented.	During the audit, it was observed that Cyfuture has maintained a comprehensive Business Continuity Plan. The plan outlines procedures and strategies to ensure the organization can continue operations in the event of a disruption, addressing key areas such as recovery time objectives (RTO), recovery point objectives (RPO), and resource allocation. CYF-ISMS-PLA -001-Business Continuity Policy version 2.0 dated 22.10.2025 Disaster Recovery- AD_DomainController_DR-Drill Test Report – DC to DR 04.10.2025 and DR to DC 04.10.2025.	No exceptions noted

10	**Environmental Safeguards:** Controls provide reasonable assurance that adequate environmental safeguards have been enforced		
10.1	Environmental controls (fire extinguishers, fire sprinklers, and smoke detectors) should be installed to protect the perimeter area. CCTV must be installed at key points for surveillance.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025	No exceptions noted
10.2	Fire drill should be conducted annually.	During the audit, it was observed that Cyfuture conducts regular fire drills. These drills are designed to ensure that employees are familiar with emergency evacuation procedures and can respond effectively in the event of a fire or other emergencies. Inspected Fire Mock Drill & Evacuation Report & Checklist, dated 12th Dec 2025	No exceptions noted
10.3	Uninterruptible power supply (UPS)devices must be in place to secure critical IT equipment against power failures and fluctuations. DG set of sufficient capacity should be provided to supply power during outages.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 & Business Continuity Plan and Maintenance records 2025.	No exceptions noted

10.4	How many ISPs are in place to provide redundancy in case of link failure?	During the audit of Cyfuture, it was observed that the company has provided the network diagram. This demonstrates the organization's commitment to maintaining a clear and comprehensive representation of its network infrastructure, which supports effective security management, risk assessment, and overall system reliability. Verified Cyfuture DC DR Network diagram dated 22.10.2025	No exceptions noted
10.5	Vendor warranty specifications should be complied with and tested to determine if the system is properly configured.	During the audit, it was observed that Cyfuture has provided evidence of vendor warranties for relevant products and services. Verified Agreements signed with vendors.	No exceptions noted
10.6	Facilities and admin personnel should monitor the status of environmental protections on a regular basis. Maintenance checklists must be used where applicable.	During the audit, it was observed that Cyfuture has maintained a comprehensive Physical Security Policy. The policy outlines measures to protect the organization's premises, assets, and personnel from unauthorized access and physical threats. DOC- CYF-ISMS-POL-027- Physical Security Policy version 1.0 dated 22.10.2025 & Maintenance records of 2025	No exceptions noted
11	**Third Party Service Provider Security:** Controls provide reasonable assurance that Third Party Service Providers are selected based on Vendor Selection Process, their roles and responsibilities, and performance requirement are formally defined and documented, and they are evaluated periodically.		

11.1	New Third-Party Service Providers should be selected based on a Vendor Selection Process. Security risk assessment must be a key part of the vendor selection process.	During the audit, it was observed that Cyfuture has provided the vendor contract agreement. This agreement outlines the terms, conditions, and responsibilities between Cyfuture and its vendors, ensuring that all parties are aligned on deliverables, expectations, and compliance requirements. Verified Vendor onboarding verification and payment Manual 2025 Verified CYF-ISMS-GDL-004-Vendor Contact List version 7.0 dated 22.10.2025 Verified Client RFP and SOW NaBFID Third party risk management framework – Cyfuture dated 04.03.225	No exceptions noted
11.2	If certain financial reporting functions are outsourced, what controls are in place to manage these relationships?	During the audit of Cyfuture, it was observed that the company has maintained the Service Level Agreement (SLA). This demonstrates the organization's commitment to clearly defining expectations and responsibilities regarding service delivery, ensuring that both parties understand the agreed-upon terms for performance, quality, and timelines. Verified Vendor onboarding verification and payment Manual 2025 Inspected - SLA Dashboard 2025	No exceptions noted

11.3	How does the organization monitor and evaluate the performance of service providers related to financial reporting?	During the audit of Cyfuture, it was observed that the company has maintained the Service Level Agreement (SLA). This demonstrates the organization's commitment to clearly defining expectations and responsibilities regarding service delivery, ensuring that both parties understand the agreed-upon terms for performance, quality, and timelines. Verified Vendor onboarding verification and payment Manual 2025 Inspected - SLA Dashboard 2025	No exceptions noted

12	**Operations:** Control activities provide reasonable assurance that operations and client onboarding activities are comprehensive and as per defined onboarding processes.		
12A.1	Clients onboard should be provided a client account on application.	During the audit, it was observed that Cyfuture has provided the vendor contract agreement. This agreement outlines the terms, conditions, and responsibilities between Cyfuture and its vendors, ensuring that all parties are aligned on deliverables, expectations, and compliance requirements. Verified Client Onboarding Manual version 1.0 dated 01.06.2025	No exceptions noted
12A.2	Service Delivery team should maintain a client escalation matrix	During the audit, it was observed that Cyfuture has provided an escalation matrix. The matrix outlines the procedures for escalating issues or incidents within the organization, ensuring that matters are addressed at the appropriate level of authority in a timely and efficient manner. Verified Escalation Matrix.	No exceptions noted

13	**Financial**		
13.1	Are new accounts set up completely and accurately in accordance with client and vendor agreements and any applicable regulations?	During the audit, it was observed that Cyfuture has provided the vendor contract agreement. This agreement outlines the terms, conditions, and responsibilities between Cyfuture and its vendors, ensuring that all parties are aligned on deliverables, expectations, and compliance requirements. Verified Client Onboarding Manual version 1.0 dated 01.06.2025 Client RFP and SOW SLA with Webmyne SLA_Cyfuture_Smriti Bank_Final_Updated	No exceptions noted
13.2	Before beginning asset custody operations, what procedures must be taken to guarantee that all client agreements have been completely executed and authorised?	During the audit, it was observed that Cyfuture has provided the vendor contract agreement. This agreement outlines the terms, conditions, and responsibilities between Cyfuture and its vendors, ensuring that all parties are aligned on deliverables, expectations, and compliance requirements. Verified Client RFP and SOW SLA with Webmyne SLA_Cyfuture_Smriti Bank_Final_Updated	No exceptions noted
13.3	How can we verify that investment and foreign exchange transactions are authorised, documented fully, precisely, and on time in accordance with client instructions?	During the audit, it was observed that Cyfuture has established Financial and organizational operation which outlines that investment and foreign exchange transactions are authorised, documented fully, precisely, and on time in accordance with client instructions. Verified Financial and organizational operation IFC dated 01.06.2025 Forex transaction and investment manual dated 01.06.2025	No exceptions noted

13.4	Are financial and organizational operations identified, executed, processed, and recorded in a timely manner?	During the audit, it was observed that Cyfuture has established vendor manual, which outlines financial and organizational operations identified, executed, processed, and recorded in a timely manner. Verified Vendor onboarding verification and payment Manual version 1.0 dated 01.06.2025	No exceptions noted
13.5	Are cash receipts and payments properly authorizing, processed, and documented in a timely manner?	During the audit, it was observed that Cyfuture has established Financial and organizational process which outlines, cash receipts and payments properly authorised, processed, and documented in a timely manner. Verified Financial and organizational operation IFC dated 01.06.2025	No exceptions noted
13.6	Are securities lending programs authorized, and are loan initiation, maintenance, and termination recorded and logged accurately and in a timely manner?	Not Applicable as Cyfuture is not involved in lending business.	No exceptions noted
13. 7	How are loans collateralized in accordance with the lender's agreement, and how is the collateral together with its related income recorded accurately on a timely basis?	Not Applicable as Cyfuture is not involved in lending business.	No exceptions noted
13. 8	How are accounts managed in line with client agreements and all relevant regulations?	During the audit, it was observed that Cyfuture has signed client agreements, which outlines accounts are managed in line with client agreements and all relevant regulations Verified SLA with Webmyne SLA_Cyfuture_Smriti Bank_Final_Updated	No exceptions noted
13.9	Are non-monetary static data changes, such as address changes and allocation instructions, authorised and documented in a timely manner?	Not Applicable	No exceptions noted
13.10	Are investment income and related tax reclaiming collection and recording done accurately and timely?	During the audit, it was observed that Cyfuture has established Procedure for fix deposit, which outlines, investment income and related tax reclaiming collection and recording done	No exceptions noted

		accurately and timely Verified SOP- Fixed deposit dated 01.06.2025	
13.11	Are the accurate recording and regular reconciliation of asset positions for securities held by third parties, such as sub custodians and depositories, ensured?	Not Applicable as Cyfuture is not involved in Fund management.	No exceptions noted
13.12	How are assets held, including investments with depositories, cash, and physically held assets, safeguarded from loss, misappropriation, and unauthorized use?	During the audit, it was observed that Cyfuture's assets held, including investments with depositories, cash, and physically held assets, safeguarded from loss, misappropriation, and unauthorized use. CYF-ISMS-POL-015- Asset Classification version 1.0 dated 22.10.2025 CYF-ISMS-POL-003-Asset Management Policy version 1.0 dated 22.11.2025 Asset Register version 13.0 dated 22.10.2025	No exceptions noted
13.13	Are the assets held by the company accurately registered and documented?	During the audit, it was observed that Cyfuture's assets held by the company accurately registered and documented. Verified Asset Registration Procedures version 3.2 dated 31.12.2025. Asset Register Subledger Extracts dated 31.12.2025. Custodian Registry Statements dated 31.12.2025 Periodic Review Evidence dated 31.01.2025	No exceptions noted
13.14	If any transaction errors have occurred, they must be rectified.	Not Applicable	No exceptions noted
13.15	Is the appointment of subservice organizations, including sub-custodians, approved? Are subservice organizations managed according to the requirements of the client agreement? Are their activities adequately monitored?	Not Applicable	No exceptions noted

13. 16	Is client asset reporting complete, accurate, and delivered within the appropriate timeframes?	Not Applicable	No exceptions noted
13.17	Do asset positions and information of securities lent (including collateral) get reported to interested parties accurately and on time?	Not Applicable	No exceptions noted
13. 18	What policies and procedures are in place to ensure accurate financial reporting?	During the audit, it was observed that Cyfuture has established policies and procedures are in place to ensure accurate financial reporting. Verified Financial and organizational operation IFC dated 01.06.2025	No exceptions noted
13. 19	What systems/software's are used to capture and process financial information?	During the audit, it was observed that Cyfuture has established asset register which outlines, systems/software's are used to capture and process financial information. Verified Asset Register-2025	No exceptions noted
13. 20	Are these systems secure and regularly updated?	During the audit, it was observed that Cyfuture has established Patch management policy which outlines, systems are secure and regularly updated Verified CYF-ISMS-POL-030 Patch Management and Malicious Code Prevention Policy.	No exceptions noted

13. 21	How is information about controls and financial reporting communicated within the organization?	During the audit of Cyfuture, it was observed that the company has provided the management MRM (Management Review Meeting) documentation. This demonstrates the organization's commitment to regularly evaluating and improving its management system, ensuring alignment with business objectives and compliance with relevant standards and regulations. Verified CYF-ISMS-PRO-006-Management Review Meeting Procedure version 7.0 dated 22.10.2025 Verified Management review meeting (MRM) for April & October 2025	No exceptions noted
13. 22	What access controls are in place to protect financial data?	During the audit, it was observed that Cyfuture has implemented Role based access controls are in place to protect financial data. Verified CYF-ISMS-PRO-013-Access Control Procedure version 7.0 dated 22.10.2025 CYF-ISMS-POL-001-Access Control Policy version 1.0 dated 22.10.2025 Access Types and Review Records version 13.0 dated 22.10.2025	No exceptions noted
13. 23	How are transactions recorded, processed, and reported?	During the audit, it was observed that Cyfuture has established IFC process, which outlines transactions recorded, processed, and reported Verified Financial and organizational operation IFC dated 01.06.2025	No exceptions noted
13. 24	How does the organization identify and assess risks related to financial reporting?	During the audit, it was observed that Cyfuture has established IFC process, which outlines the organization identify and assess risks related to financial reporting. Verified Financial and organizational operation IFC dated 01.06.2025	No exceptions noted