



Logix InfoSecurity Pvt. Ltd.

SOC 2 Type II Report

February 2026





DISCLAIMER: This report for Email Hosting Services, Firewall Implementation & Support, and O-365 Product Support & Services is intended solely for the information and use of Management of Logix InfoSecurity Pvt. Ltd., user entities, and relevant stakeholders. In this circumstance, you may distribute this SOC 2 report to current and prospective clients. You must provide recipients of this SOC 2 report with written documentation of the functions Logix InfoSecurity Pvt. Ltd. offers related to your services. You must keep a complete and accurate record of entities and the personnel of such entities to whom this SOC 2 report is provided. Logix InfoSecurity Pvt. Ltd. must promptly provide copies of such records to ShieldByte Infosec Pvt. Ltd. upon request.

EXECUTIVE SUMMARY

Scope	▪ Email Hosting Service ▪ Firewall Implementation & Support and ▪ O-365 Product Support & Services
Applicable Control Objective	▪ Security, ▪ Confidentiality, ▪ Availability and ▪ Processing Integrity
Reporting Period	1 st December 2024 to 30 th November 2025
Locations	Navi Mumbai, India
Audit Report Reference	SIPL/SOC/001178

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
SECTION – I	5
INDEPENDENT SERVICE AUDITOR'S REPORT	5
INDEPENDENT SERVICE AUDITOR'S REPORT	6
SERVICE ORGANIZATION'S RESPONSIBILITIES.....	6
SERVICE AUDITOR'S RESPONSIBILITIES	7
INHERENT LIMITATIONS	7
OPINION	7
RESTRICTED USE	8
SECTION – II	9
LOGIX'S MANAGEMENT ASSERTION	9
LOGIX'S MANAGEMENT ASSERTION	10
SECTION – III	12
DESCRIPTION OF CONTROLS PROVIDED BY LOGIX.....	12
DESCRIPTION OF CONTROLS PROVIDED BY LOGIX.....	13
SERVICES PROVIDED.....	13
BACKGROUND AND OVERVIEW OF SERVICE	13
SUBSERVICE ORGANIZATIONS.....	13
BOUNDARIES OF THE SYSTEM	13
DESCRIPTION OF CONTROL ENVIRONMENT, CONTROL ACTIVITIES, RISK ASSESSMENT, MONITORING, & INFORMATION AND COMMUNICATION	14
COMPLEMENTARY SUB-SERVICE ORGANIZATION CONTROL OR CONTROL OVER SUB- SERVICE ORGANIZATION	23
NON-APPLICABILITY OF ANY CONTROL OBJECTIVES	23
SECTION – IV.....	24
DESCRIPTION AND EVALUATION OF CONTROLS TO ACHIEVE THE APPLICABLE CONTROL OBJECTIVES AND CONTROLS, AND THE RESULTS THEREOF.....	24
INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR.....	25
ASSESSMENT OF CONTROLS.....	25
TRUST SERVICES CRITERIA 2022	26
END OF DOCUMENT	89



SECTION – I

INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

Logix InfoSecurity Pvt. Ltd.

Location: Navi Mumbai, India

SCOPE

We have examined the attached Logix InfoSecurity Pvt. Ltd.'s (Logix) description of the system titled "Email Hosting Services, Firewall Implementation & Support, and O-365 Product Support & Services" for the period 1st December 2024 to 30th November 2025, included in Section 3, based on the criteria outlined in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) and suitability of the design and operating effectiveness of the controls included in the description for the period 1st December 2024 to 30th November 2025 to meet the principles outlined in TSP Section 100A Principles and Criteria, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria, 2022). Logix has determined that Privacy principles do not apply to the services provided to its clients and are therefore not included in the description.

The description indicates that certain applicable Trust Services Criteria can be achieved only if complementary user entity controls contemplated in the design of Logix's controls are appropriately designed, along with related controls at the service organization. Our examination did not extend to such complementary user-entity controls, and we have not evaluated their suitability. Their controls at Sub-Service Organizations are out of scope.

The description includes only those control criteria and related controls of Logix in Navi Mumbai, India.

SERVICE ORGANIZATION'S RESPONSIBILITIES

Logix has provided the accompanying assertion titled "Logix's Management Assertion." Logix is responsible for

1. Preparing the description and the assertion;
2. The completeness, accuracy, and method of presentation of both the description and assertion;
3. Providing the services covered by the description;
4. Specifying the controls that meet the applicable control objectives and stating them in the description; and
5. Designing, implementing, and documenting controls to meet applicable control objectives for Security, Confidentiality, Availability, and Process Integrity.



SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion on

- The fairness of the presentation of the description, and
- Based on our examination, the suitability of the design and operating effectiveness of controls throughout the period to meet the applicable control objectives.

We conducted our examination in accordance with the attestation standard SSAE-22, established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance, in all material respects.

- The description is fairly presented and
- The controls were suitably designed and operated effectively throughout the period from 1st December 2024 to 30th November 2025.

Our examination involved performing procedures to obtain evidence on the fairness of the description's presentation against the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable control objectives. Our procedures included assessing the risks that the description is not fairly presented, and the controls were not suitably designed or operated effectively to meet the applicable control objectives. Our procedures also included examining the fairness of the presentation of the service organization's system and the suitability of the controls design for the period 1st December 2024 to 30th November 2025. We believe that the evidence obtained is enough and appropriate to provide a reasonable basis for our opinion.

INHERENT LIMITATIONS

Because of inherent limitations, controls at a service organization may not continuously operate effectively to meet the applicable trust services criteria. Also, any future projection of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable control objectives is subject to risks that the system may change or that controls at a service organization may become inadequate or fail.

OPINION

In our opinion, in all material respects, based on the description criteria identified in Logix's assertion and the applicable control objectives covering the Security, Confidentiality, Availability, and Processing Integrity aspects:

- The description fairly presents the controls that were designed and implemented, and

Independent Service Auditors' Report

- The controls stated in the description were suitably designed to ensure that the applicable control objectives operated effectively, from 1st December 2024 to 30th November 2025.
- The controls tested are operating effectively and were necessary to provide reasonable assurance that the applicable control objectives were met and managed effectively from 1st December 2024 to 30th November 2025.

RESTRICTED USE

This report and the description of controls are envisioned solely for the information and use of Logix user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service offered by the service organization (Logix).
- How the service organization's system interacts with user entities or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable control objectives.
- The applicable control objectives.
- The risks that may threaten the achievement of the applicable control objectives and how controls address those risks.

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

For House of CPA

HOUSE
OF CPA

Digitally signed by
HOUSE OF CPA
Date: 2026.02.27
21:18:20 +05'30'



K P Krishna Kumar | Certified Public Accountant
License No.: 5793 | Date: 27th February 2026

SECTION – II

LOGIX’S MANAGEMENT ASSERTION

LOGIX'S MANAGEMENT ASSERTION

LOGIX INFOSECURITY PVT. LTD.

Unit No. 127, Bldg. 2(A-3), Sector -1, Millenium Business Park,
Mahape, Navi Mumbai 400 710
Tel.: (+91-22) 4102 4545
CIN : U72100MH1999PTC121303



Logix's Management Assertion

We have prepared the attached description of Logix InfoSecurity Pvt. Ltd.(Logix) for controls about its "Email Hosting Service, Firewall Implementation & Support and O-365 Product Support & Services" from 1st December 2024 to 30th November 2025, based on the criteria in items (A) – (B) below, which are the criteria for a description of a service organization's system in AICPA Guide Reporting on Controls at a Service Organization relevant to Security, Confidentiality, Availability, Processing Integrity, and Privacy (Trust Services Criteria 2022). These criteria are founded for the user entities, their auditors who audit and report on such user entities' internal control and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the associated risks.

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

- A. The description fairly presents the Email Hosting Service, Firewall Implementation & Support and O-365 Product Support & Services made available to user entities of the system from 1st December 2024 to 30th November 2025, for processing their data or information as it relates to controls that are likely to be relevant to testing the design and operating effectiveness of service organization's controls. The Trust Services Criteria we used in making this assertion were that the description
 - a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
 - 1. the types of services provided.
 - 2. the procedures, within both automated and manual systems, by which those services are provided.
 - 3. the information used in the performance of the procedures.
 - 4. how the system captures and addresses significant events and conditions.
 - 5. The process is used to prepare reports and other information for user entities.
 - 6. services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used concerning them.

LOGIX INFOSECURITY PVT. LTD.

Unit No. 127, Bldg. 2(A-3), Sector -1, Millenium Business Park,
Mahape, Navi Mumbai 400 710
Tel.: (+91-22) 4102 4545
CIN : U72100MH1999PTC121303

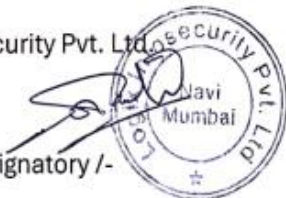


7. The specified control objectives and controls designed to achieve those objectives include, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 8. Other aspects of our control environment, risk assessment process, information, and communication (including the related business processes), control activities, and monitoring activities relevant to the services provided.
- b. It includes relevant details of changes to the service organization's system during the period covered by the description.
- c. It doesn't 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 defined contribution record-keeping system that each user entity of the system and its auditor may consider important in its particular environment.
- B. The controls related to the control objectives stated in the description were suitably designed and operating effectively from 1st December 2024 to 30th November 2025, to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of Logix controls from 1st December 2024 to 30th November 2025. The Trust Services Criteria we used in making this assertion were that
- a. The risks that threaten the achievement of the control objectives stated in the description have been identified by the management of the service organization.
 - b. 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.
 - c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Logix InfoSecurity Pvt. Ltd.

Sign.

Authorized Signatory /-



Date: 9th December 2025

SECTION – III

DESCRIPTION OF CONTROLS PROVIDED BY LOGIX

DESCRIPTION OF CONTROLS PROVIDED BY LOGIX

SERVICES PROVIDED

Logix is a leading IT company with commanding expertise and a proven track record in providing messaging and collaboration, email security, and cybersecurity solutions to over 2100 businesses, including SMBs, PSUs, BFSIs, government, and large enterprises. As an IT company, Logix focuses on delivering robust services and products while caring for customers—the customers bank on Logix for exceptional, unwavering support.

Logix Cloud is hosted across three Tier 3 IDC facilities in Mumbai, Pune, and Bangalore, on state-of-the-art cloud infrastructure built on Hyperconverged technologies. Maintaining the confidentiality of our customers' data is Logix's utmost priority. Logix adheres to strict SOC 2 Type II guidelines and is SOC 2 Type II compliant.

BACKGROUND AND OVERVIEW OF SERVICE

Logix's Vision & Mission

To be the first choice for customers' IT needs, with complete customer-centricity.

SUBSERVICE ORGANIZATIONS

- Microsoft- Office 365
- Microsoft- Windows Defender
- Synacor- Zimbra
- Fortinet- Firewall
- Cisco- Firewall
- Cisco- IronPort
- Compuage Infocom
- STT Global- Disaster Recovery site
- VMware- Cloud platform
- F-Secure Radar- Vulnerability Scanning and Management
- Zabbix- Threat Management and Security Monitoring

BOUNDARIES OF THE SYSTEM

The following are the services and their descriptions within the scope of the audit.

- IT Infrastructure
- Hosting Platforms
- Desktops/ Laptops
- Network Components

Logix utilizes leased premises for its business operations.

Geographic Locations in Scope	
Office Location	Mahape, Navi Mumbai, India
Address	Unit No 127, Building No 2, Sector 1, Millennium Business Park Mahape, Navi Mumbai 400710, India

DESCRIPTION OF CONTROL ENVIRONMENT, CONTROL ACTIVITIES, RISK ASSESSMENT, MONITORING, & INFORMATION AND COMMUNICATION

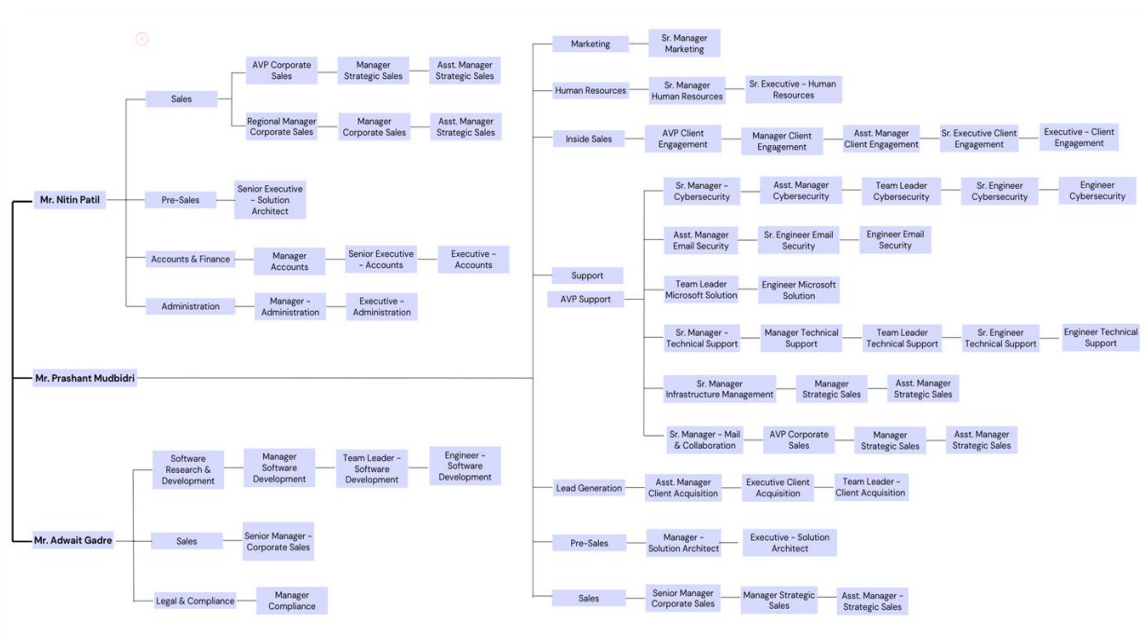
INTEGRITY AND ETHICAL VALUES

Logix is committed to conducting its business with integrity to prevent unethical or unlawful behavior. Logix has defined a 'Code of Conduct and Code of Ethics' that fosters a strong ethical environment for Logix and helps protect the interests and safety of Logix employees. It also describes the corrective actions that may be taken against the employee in case of non-compliance with Logix policies (including disciplinary actions up to termination).

Logix's integrity and ethical values are communicated to employees through induction training. Employees are also required to read and acknowledge that they have understood the clauses in the following documents:

- Confidentiality and Non-Disclosure Agreement
- Code of Conduct and Code of Ethics
- Acceptable Usage Policy

MANAGEMENT TEAM



RISK ASSESSMENT

Risk assessment is conducted when a new business is initiated with a user organization. Risk assessment consists of calculating contingency risks for a project. The Infrastructure Management Team conducts risk analysis to quantify contingency risk and develop a project contingency budget. Risk assessment covers human resources, physical security, logical security, third-party vendors and suppliers, and network security. Risks identified are discussed in a forum consisting of the Infrastructure Management Team and Senior Management. Identified risks are prioritized, and a risk treatment plan is prepared that includes actions to mitigate the risks and timelines for their resolution. The Risk Assessment Methodology and Risk Assessment Matrix are reviewed annually, and controls for high-risk areas are considered for improvement.

INFORMATION SECURITY POLICIES

Logix has developed organization-wide information security policies. The following is the list of information security policies established for various domains within the organization:

- Information Security Policy
- Asset Management Policy
- Acceptable Use Policy
- Technical Vulnerability Management Policy
- Backup and Restoration Policy
- Human Resource Security Policy
- Disciplinary Policy
- Capacity Management Policy
- Change Management Policy
- Business Continuity Policy
- Anti- Malware Policy
- Audit Logging and Monitoring Policy
- Disaster Recovery Policy
- Data Retention and Archival Policy
- Media Handling Policy
- Mobile Device Policy
- Cryptography Policy
- Password Management Policy
- Patch Management Policy
- Monitoring Policy
- Data Classification and Handling Policy
- Access Control Policy
- Information Security Risk Management Policy
- Software Installation Policy
- Whistleblower Policy

- Incident Management Policy
- IT Roles and Responsibility Policy
- Cloud Security Policy

MONITORING

Information Security meetings are conducted between Logix Senior Management and the Infrastructure Management Team to review the effectiveness of Information Security controls. The head of the Infrastructure Management Team prepares the presentation for the Information Security meeting and tracks the status of action items from the meeting. Areas of concern are highlighted, and an action plan is developed based on observations.

INFORMATION AND COMMUNICATION

The following tools are used to support email hosting services:

Sparsh

Sparsh portal is an in-house-developed web-based workflow tool used to manage logical access, customer domain provisioning and de-provisioning, change management, incident management, and the tracking and monitoring of service requests. The Infrastructure Management Team grants access to the required application upon a request from the Human Resource Team.

Control Panel

Control Panel is an in-house-developed tool used for customer domain provisioning/de-provisioning, data segregation, and email monitoring. Access to user organization domains hosted by Logix is also controlled and maintained through the Control Panel. Access to the Control Panel is restricted to members of the Infrastructure Management Team.

VMware

VMware is a virtualization and cloud platform for virtualizing existing hardware infrastructure. Logix provides host-based failover and a single management console to manage all server-based hardware, dynamically allocating resources to virtual servers as needed. VMware is the primary infrastructure tool for a server-based setup.

Cisco IronPort

Cisco IronPort is a third-party anti-spam tool that protects against spam and unsolicited emails. Cisco IronPort serves as a security service in the Logix setup, scanning all incoming and outgoing email to and from the Logix messaging service.

F-Secure Radar

F-Secure Radar is a third-party vulnerability scanning and management tool. Vulnerability scanning and management services help Logix identify and remediate vulnerabilities across any platform or web application.

Zabbix

Zabbix is a third-party tool used for Threat Management and Security Monitoring. It provides real-time analysis of potential security issues for investigation. It may receive events from various devices, such as control panels, servers, firewalls, and CPUs. The tool is monitored on a 24/7 basis. Once an offense/ issue is reported by the Zabbix tool, the responsible group carries out remediation.

Backup Application

An in-house application developed for managing backup and restoration of servers and configurations.

ELECTRONIC MAIL (EMAIL)

Employees are provided with an email for online communication. Incoming and outgoing emails are scanned for known viruses. Important corporate communications are conducted via email. Changes to policies and procedures are communicated via email by the Head of the Infrastructure Management Team.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

INFRASTRUCTURE

Logix has implemented a firewall on Internet Getaway to monitor external traffic and restrict access to authorized users, systems, and services. Rules are enforced on the firewall to 'deny all' with access enabled for specific services as per business requirements.

Logix has deployed a host-based intrusion prevention system on the local area network and Logix infrastructure to monitor network traffic and prevent intrusions. The intrusion prevention system is designed to scan incoming and outgoing network traffic in real-time. The intrusion prevention system is updated with signatures from vendors' websites as they are released.

Network Access

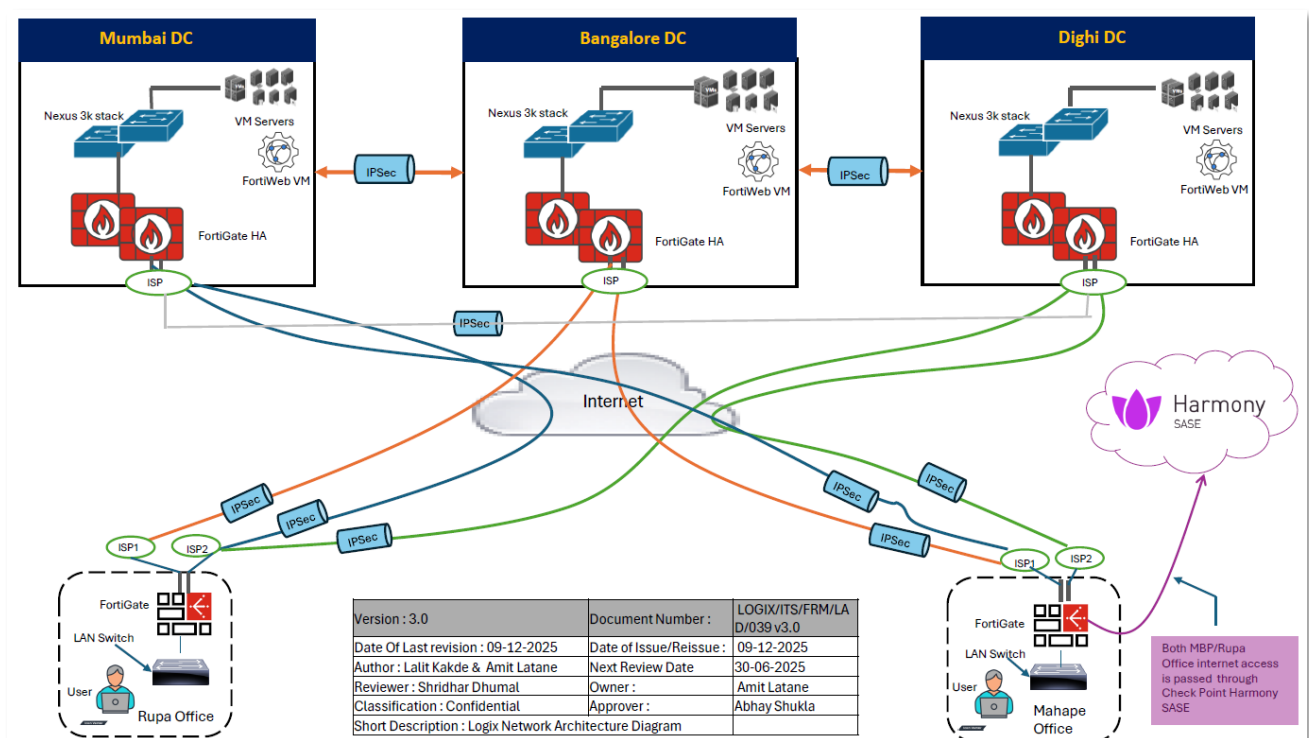
Logix network security controls are designed to provide reasonable assurance that unauthorized access (internally and externally) to the network is prevented and detected. Network components (such as firewalls, routers, and switches) and monitoring tools are in

place to protect the Logix network. The Infrastructure Management Team maintains the network security diagram.

Access to network components is integrated with a secure version of Lightweight Directory Access Protocol (LDAP) that logs commands and access attempts. These logs are pulled back to the logger server, enabling the Infrastructure Management Team to account for all access to network components, including the commands and access attempts.

These logs are pulled back to the logger server, enabling the Infrastructure Management Team to account for all access to network components, including executed commands.

Administrative privileges on the network components are restricted to authorized personnel from the Infrastructure Management Team.



Emergency Backup

Logix has installed an Uninterruptible Power Supply (UPS) to operate in failover mode. This ensures that critical infrastructure supporting devices continue to function until the primary supply is restored. UPS maintenance is performed at set intervals by a third-party vendor.

MONITORING

Logix has implemented Zabbix as a security threat monitoring tool for monitoring the availability of servers and network components. Zabbix is the central repository for storing and interpreting logs and events generated by servers and network components. Zabbix monitors parameters such as:

- Bandwidth utilization
- CPU utilization
- Memory utilization
- Disk utilization
- Link availability
- Performance monitoring, etc.

The Zabbix tool is configured to automatically alert the Infrastructure Management Team when performance or availability drops below defined thresholds and to flag security threats. The Infrastructure Management Team monitors Zabbix in real time and investigates the causes of increased offenses. Depending on the severity/ category of the offense, the Infrastructure Management Team takes corrective actions, if needed, and tracks it to closure. The Infrastructure Management Team performs capacity monitoring for networks and servers as a part of the system availability monitoring process. The Infrastructure Management Team analyses and reviews typical trends in Zabbix alerts and sends a daily summary report to the Head of the Infrastructure Management Team.

SOFTWARE

- **Sparsh-** In-house developed a web-based workflow tool to manage logical access, customer domain provisioning and de-provisioning, change management, incident management, and tracking and monitoring service requests.
- **Control Panel-** In-house developed tool for customer domain provisioning and de-provisioning, data segregation, and email monitoring.
- **VMware-** A virtual and cloud platform to virtualize existing hardware infrastructure.
- **Cisco IronPort** is a third-party anti-spam tool that protects against spam and unsolicited emails.
- **F-Secure Radar-** Third-party vulnerability scanning and management tool.
- **Zabbix** is a third-party tool used for threat management and security monitoring.
- **Backup Application-** In-house application developed for managing backup and restoration of servers and configurations.

PEOPLE

A. Commitment to Competence

Department heads are responsible for identifying and communicating their resource requirements and the minimum required skill sets to the Human Resource Team. Candidates

must undergo human resources and technical interview sessions before appointment to ensure that skill sets match job requirements. Employees are provided with domain knowledge (an overview of the system) for their roles, such as Technical Support, Technical Consultants, and Sales. New hires shadow regular employees till they are provided access to Logix systems.

B. New Hire Procedure

New hires sign the following documents at the time of joining to acknowledge acceptance of Information Security practices at Logix-

- Confidentiality and Non-Disclosure Agreement- agreeing to maintain confidentiality of Logix and User Organization information
- Code of Conduct and Code of Ethics- agreeing to abide by Information Security Policy and describing corrective actions that may be taken against an employee in case of non-compliance with Logix policies (including disciplinary actions, up to termination) and
- Acceptable Usage Policy

Logix's Information Security commitments are communicated to new hires during induction training. During induction training, new hires are informed about information security, passwords, physical security, and email and internet usage policies. Updates or changes to Logix's policies are communicated to employees via periodic mailers from Logix Management. Posters displaying do's and don'ts, along with the corresponding information security practices, are also posted in work areas to raise employee awareness.

C. Training and Development

Employees must complete Information Security Awareness web-based training every 12 months, covering the safeguarding of customers' confidential information.

D. Employee Exit Procedures

Upon an employee's resignation, the Human Resources team updates the employee's last working day in the Sparsh portal. The Human Resources Team sends an email notification to the Infrastructure Management Team to deactivate physical access. Based on email notification, the Infrastructure Management team deactivates physical access to the work area and updates the Sparsh portal.

PROCEDURES

A. Change Management

Logix has defined a formal procedure for describing the infrastructure change management process. The process document details the responsibilities and accountabilities for system

changes, maintenance, and the testing, evaluation, and authorization of system components before implementing changes.

The change request is initiated for a new implementation, a performance issue reported in the infrastructure, infrastructure changes to add a new process, or the resolution of an incident requiring infrastructure changes. Requests for infrastructure changes are submitted through the Sparsh portal for firewall policy additions, switch and device configurations, server operating system upgrades, backup generator maintenance, etc.

The Infrastructure Management team updates the change initiator, description, and reason for the change on the Sparsh portal. The Infrastructure Management Team raises change requests and documents change descriptions within the Sparsh portal. The change request is then forwarded to the Head of the Infrastructure Management Team for authorization. Based on authorization from the Head of the Infrastructure Management Team, impact analysis and testing of the change on the quality server are conducted, where applicable, and the results are updated on the Sparsh portal. The change request is forwarded to the Business Unit Operations Head for approval. Upon approval, the Infrastructure Management Team implements the change and closes the ticket in the Sparsh portal.

B. Vulnerability and Patch Management

On a six-monthly basis, the Infrastructure Management Team conducts an internal Vulnerability Assessment to meet ongoing and evolving commitments and system requirements. The Infrastructure Management Team performs vulnerability scans on critical systems, including servers and network components. These scans confirm that the systems are securely configured for service use, password policies, port access, security patches, and related controls. High- and medium-risk vulnerabilities are addressed and tracked to closure by the Infrastructure Management Team.

C. Incident Reporting and Resolution

Logix has defined a formal procedure for reporting and managing security breaches. Employees are made aware that they must report any violation of system security for Logix information assets to the Infrastructure Management Team. Employees log information security incidents/ breaches by emailing or calling the Infrastructure Management Team. Statement of Work (SoW) or Technical Instruction (TI) documents the process to be followed for the notification of incidents or potential threats identified by Logix, or any change in policies or procedures that might affect each other.

An Infrastructure Management Team member raises a ticket in the Sparsh portal, which provides details of security incidents/breaches, security violations, and employee/group responsibility, and analyzes the impact on the security of information or systems. The Infrastructure Management Team assesses incident details, collects and analyzes related

information, and resolves the incident. Upon resolution, the Infrastructure Management Team updates the Sparsh portal with a brief description of the resolution.

D. Logical Access

1. Security Authorization and Administration

Users at Logix log in to the Sparsh portal to access various utilities at Logix. A centralized directory, implemented using LDAP, stores user permissions. Logix does not have any access to User Organization-specific data. Data is hosted on servers in the data center.

When an employee joins, the Human Resources team updates the new hire's details in the Sparsh portal, which automatically generates and assigns a User ID. Passwords must be changed every 15 days. Based on the user's role or department, the Human Resources Team grants access to specific pages within the Sparsh portal. Creating a user ID in the Sparsh portal is restricted to the Human Resources Team. Access to the Sparsh portal is integrated with LDAP.

2. Administrative Level Access

Administrative privileges on the Sparsh portal and Control Panel are restricted to authorized personnel, subject to approval from the Infrastructure Management Lead. Users are not granted administrative privileges at local workstations.

COMPLEMENTARY USER ENTITY CONTROLS

This section describes controls that User Organizations are responsible for implementing in addition to those at Logix. Following user control considerations should not be regarded as a comprehensive list of all controls that User Organizations should deploy. Additional appropriate controls for user organizations may not be defined in this report.

Sr. No.	Complementary User Organization Controls	Trust Criteria No.
1	User organizations should ensure Logix is updated with any changes to the user organization's policies and procedures that Logix is expected to comply with.	CC 2.3
2	User organizations should ensure they have appropriate controls to manage the upgrading and general maintenance of their infrastructure, and any applications, operating systems, databases, and other software hosted on their infrastructure.	CC 2.5

3	User organizations should ensure they have appropriate controls to manage logical access to their infrastructure.	CC 5.2
4	User Organizations should ensure they have appropriate controls to back up data held on their infrastructure.	CC 5.7

COMPLEMENTARY SUB-SERVICE ORGANIZATION CONTROL OR CONTROL OVER SUB-SERVICE ORGANIZATION

In designing its system, Logix has considered that subservice organizations would implement controls to meet security and availability criteria.

This section describes additional controls that should be in place at subservice organizations to align with the controls at Logix. The following controls should not be considered a comprehensive list of all controls that subservice organizations should deploy. There may be additional appropriate controls for sub-services not specified in this report.

Serial No.	Subservice Organization Controls	Trust Criteria No.
1	Physical security, restrictions, security personnel, access provisioning/ de-provisioning, identification and authentication of persons accessing server room.	CC5.5

NON-APPLICABILITY OF ANY CONTROL OBJECTIVES

Logix Infosecurity has not included Privacy controls in its description because they are not relevant to the current requirement.

SECTION – IV

DESCRIPTION AND EVALUATION OF CONTROLS TO ACHIEVE THE APPLICABLE CONTROL OBJECTIVES AND CONTROLS, AND THE RESULTS THEREOF

INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

This section presents the following information provided by Logix:

- Logix's management specifies the control objectives.
- The controls established and specified by Logix are to achieve the specified control objectives.

Also included in this section is the following information provided by the service auditors:

- A description of the tests performed by the service auditors to determine whether the service organization's controls were operating effectively to achieve specified control objectives. The service auditor determined the nature, timing, and extent of the testing.
- The results of the service auditor's test of controls.

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in determining Logix's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively.

ASSESSMENT OF CONTROLS

Our tests of the controls' design covered a detailed set of transactions and procedures for the period 1st December 2024 to 30TH November 2025 for the controls listed in this section, which are designed by management to achieve the specified control objectives. In selecting a test of controls, the following were considered:

- The nature of the items being tested,
- The types and competency of available evidential matter,
- The nature of the audit objectives to be achieved,
- The assessed level of control risk and
- The expected efficiency and effectiveness of the test.
- The sampling method was risk-based.

The following information pertains to the suitability of the design examined by the independent auditor. The specific, applicable control objective for each trust principle is identified in the table below.

TRUST SERVICES CRITERIA 2022

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
1	ORGANIZATION AND MANAGEMENT		
CC 1.1	COSO Principle 1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the system's design, development, implementation, operation, maintenance, and monitoring, enabling it to meet its commitments and system requirements as they relate to and are addressed by the engagement.		
CC 1.1A	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behaviour the importance of integrity and ethical values to support the functioning of the system of internal control.	Logix has defined and documented its Information Security Policy and Organization Structure to uphold ethical standards and integrity, thereby supporting the robustness of internal control systems.	No exceptions noted.
CC 1.1B	Establishes Standards of Conduct— The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	Logix has established a formal Code of Conduct that outlines management's expectations, integrity and ethical behaviour and ensure that these standards are effectively communicated and understood across all levels of the organization.	No exceptions noted.
CC 1.1C	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	Verified that performance evaluation of employees is carried out periodically ensuring their adherence with the established standards and management's expectations from them.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 1.1D	Addresses Deviations promptly— Deviations from the entity's expected standards of conduct are identified and remedied promptly and consistently.	Logix has established Disciplinary Policy to address deviations from expected code of ethical values, ensuring that such instances are identified, addressed, and resolved in a timely and consistent manner across the entity.	No exceptions noted.
CC 1.1E	Considers Contractors and Vendor Employees in Demonstrating Its Commitment —Management and the board of directors consider the use of contractors and vendor employees in its processes to establish standards of conduct, evaluate adherence to those standards, and promptly address deviations.	Service Agreements are mutually executed with the external parties obtaining their commitments and adherence towards Logix's established standards. Processes are in place to address any deviations if identified.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC 1.2A	Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities concerning established requirements and expectations.	Management has established oversight mechanisms through periodic review meetings of business practices and internal processes, to ensure adherence with governance standards and operational integrity.	No exceptions noted.
CC 1.2B	Applies Relevant Expertise —The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to	Verified that Logix has established Competence matrix and conducts periodic evaluation of employee	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	enable them to ask probing questions of senior management and take commensurate action.	performance. Trainings are conducted to upskill employees in required domain.	
CC 1.2C	Operates Independently— The board of directors has sufficient members who are independent of management and objective in evaluations and decision-making.	Department head and designated authorities at Logix play key role in decision making and evaluations.	No exceptions noted.
CC 1.2D	Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, using a subcommittee or consultants.	Observed that the Management has taken measures to strengthen the Logix's security posture by establishing internal committee to monitor, assess and enhance expertise in areas critical to Information Security and by engaging external consultants.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC 1.3A	Considers All Structures of the Entity— Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	Observed that Logix has identified and have engaged with necessary sub-service providers to support and achieve its business objectives.	No exceptions noted.
CC 1.3B	Establishes Reporting Lines— Management designs and evaluates lines of reporting for each entity structure to	Verified that Logix has established clear reporting lines for effective execution of responsibilities and authority.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	enable execution of authorities and responsibilities and flow of information to manage the entity's activities.		
CC 1.3C	Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of director's delegate authority, define responsibilities and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	Verified that Logix has established and defined specific responsibilities to personnel, ensuring effective segregation of duties and implementation of appropriate access controls.	No exceptions noted.
CC 1.3D	Addresses Specific Requirements When Defining Authorities and Responsibilities — When defining authorities and responsibilities, management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy.	Verified that Logix has defined roles and responsibilities for each department, thereby ensuring appropriate authority and respective access to mitigate risks and enhance internal security controls.	No exceptions noted.
CC 1.3E	Considers Interactions with External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities — Management and the board of directors consider the need for the entity to interact with and monitor the activities	Logix has formalized reporting structures and clearly defined roles and responsibilities for third-party entities, which is communicated during their onboarding.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	of external parties when establishing structures, reporting lines, authorities, and responsibilities.		
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC 1.4A	Establishes Policies and Practices — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	Observed that Logix has documented key policies, procedures and operational practices to ensure alignment with and support its strategic and operational objectives.	No exceptions noted.
CC 1.4B	Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in outsourced service providers concerning established policies and practices and act as necessary to address shortcomings.	Logix has established a formal process to regularly assess employees and vendor competencies and systematically address any skill gaps or deficiencies identified.	No exceptions noted
CC 1.4C	Attracts, Develops, and Retains Individuals— The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	Verified that Logix provides training to employees to develop and retain sufficient and competent personnel for supporting the achievement of business objectives.	No exceptions noted.
CC 1.4D	Plans and Prepares for Succession— Senior management and the board of directors develop contingency plans for	Logix has established contingency strategies to ensure effective risk	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	responsibility assignments important for internal control.	management, business continuity, and disaster recovery.	
CC 1.4E	Considers the Background of Individuals – The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Logix performs a comprehensive Background Verification of its employees from an external party.	No exceptions noted.
CC 1.4F	Considers the Technical Competency of Individuals – The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Observed that the hiring process of Logix considers the technical competency of potential and existing personnel to determine whether to employ and retain the individuals.	No exceptions noted.
CC 1.4G	Provides Training to Maintain Technical Competencies – The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	Verified that Logix has processes in place for imparting training and performance monitoring to upskill the employees and their technical competencies.	No exceptions noted.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC 1.5A	Enforces Accountability Through Structures, Authorities, and	Logix signs appointment letter with employees that serve as a formal	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for the performance of internal control responsibilities across the entity and implement corrective action as necessary.	documentation of accountability and clearly delineate roles specific responsibilities thereby supporting transparency and alignment with organizational objectives.	
CC 1.5B	Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	Logix conducts performance evaluations of its employee on annual basis. Additionally, incentives and appraisals are provided based on the ratings provided during evaluation.	No exceptions noted.
CC 1.5C	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance— Management and the board of directors align incentives and rewards with the fulfilment of internal control responsibilities in the achievement of objectives.	Verified that Logic conducts annual performance evaluation of employees and provides incentives in the form of appraisals based on the successful completion of responsibilities and the achievement of its objectives.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 1.5D	Considers Excessive Pressures – Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	Logix actively monitors and evaluates performance related pressure, making necessary adjustments in line with defined roles and responsibilities to ensure alignment with strategic objectives and timely achievement of targets.	No exceptions noted.
CC 1.5E	Evaluates Performance and Rewards or Disciplines Individuals –Management and the board of directors evaluate the performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action as appropriate.	Verified that Logix conducts performance evaluations to ensure employees adhere to their assigned responsibilities and the established code of conduct. Based on the performance evaluation outcomes, appropriate actions such as rewards for satisfactory performance or disciplinary measures for non-compliances are taken.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
2	COMMUNICATION AND INFORMATION		
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC 2.1A	Identifies Information Requirements – A process is in place to identify the information required and expected to support the functioning of the other	Logix has established an Information Security Policy that outlines the process for identification and classification of information necessary to achieve business objectives.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	components of internal control and the achievement of the entity's objectives.		
CC 2.1B	Captures Internal and External Sources of Data —Information systems capture internal and external data sources.	Logix has processes in place to assess and determine the information required for the achievement of the business objectives.	No exceptions noted.
CC 2.1C	Processes Relevant Data into Information —Information systems process and transform relevant data into information.	Logix leverages information systems and processes to transform relevant data into actionable insights, supporting informed decision-making.	No exceptions noted.
CC 2.1D	Maintains Quality Throughout Processing —Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	Logix maintains quality and accuracy of information throughout the information processing by enforcing structured procedures.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC 2.2A	Communicates Internal Control Information— A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	Verified that internal communication is done through teams and dedicated exclusively to authorized personnel to facilitate the execution of their responsibilities.	No exceptions noted.
CC 2.2B	Communicates With the Board of Directors— Communication exists	Verified that review meetings are conducted with the Senior and Executive	No exceptions noted

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	between management and the board of directors so that both have the information needed to fulfil their roles with respect to the entity's objectives.	Management to support business objectives and uphold organizational integrity.	
CC 2.2C	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Logix has utilized Email and teams as its primary communication channels with external and internal stakeholders. Additionally, mobile communication can be utilized as an alternative when primary communication channels are inoperative.	No exceptions noted.
CC 2.2D	Selects Relevant Method of Communication— The method of communication considers the timing, audience, and nature of the information.	Logix utilizes Email and teams as its primary communication channels to facilitate clear and efficient communication of information.	No exceptions noted.
CC 2.2E	Communicates Responsibilities — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	Management appropriately communicates the allocation, and any modifications of responsibilities related to information system controls to the relevant personnel.	No exceptions noted.
CC 2.2F	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters —Entity personnel are provided	Logix has established an Incident Management Process, outlining clear procedures for reporting system	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	failures, incidents and related concerns to designated personnel.	
CC 2.2G	Communicates Objectives and Changes to Objectives — The entity promptly communicates its objectives and changes to those objectives to personnel.	Logix communicates the Information Security objectives and changes to objectives with authorized personnel ensuring awareness and alignment with established standards.	No exceptions noted.
CC 2.2H	Communicates Information to Improve Security Knowledge and Awareness — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviours to personnel through a security awareness training program.	Logix delivers comprehensive information security awareness training to their employees periodically to ensure enhancement in the security knowledge and awareness.	No exceptions noted.
CC 2.2I	Communicates Information About System Operation and Boundaries— The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	Logix communicates the design, operational procedures, and system boundaries to relevant personnel to ensure alignment with their responsibilities.	No exceptions noted.
CC 2.2J	Communicates System Objectives — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	Logix ensures timely communication of system changes impacting responsibilities or organizational objectives to designated personnel in timely manner.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 2.2K	Communicates System Changes— System changes that affect responsibilities or the achievement of the entity's objectives are communicated promptly.	Logix ensures timely communication of system changes impacting responsibilities or organizational objectives to designated personnel in timely manner.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC 2.3A	Communicates to External Parties — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	Logix uses communication channel such as email to share relevant information with external parties in a timely and structured manner.	No exceptions noted.
CC 2.3B	Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	Logix utilizes email as the primary communication channel for vendors, customers and relevant external stakeholders for streamlined formal communication.	No exceptions noted.
CC 2.3C	Communicates With the Board of Directors— Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.	Logix communicates external assessment outcomes to Senior Management during review meetings or as deemed necessary.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 2.3D	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Logix has utilized Email and teams as its primary communication channels with external and internal stakeholders. Additionally, mobile communication can be utilized as an alternative when primary communication channels are inoperative.	No exceptions noted.
CC 2.3E	Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	Logix relies on email to transmit relevant information to appropriate parties.	No exceptions noted.
CC 2.3F	Communicates Objectives Related to Confidentiality and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives, and changes to objectives related to confidentiality.	Agreements executed with external parties outlines the communication of system objectives and changes to objectives related to confidentiality.	No exceptions noted.
CC 2.3G	Communicates Objectives Related to Privacy and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of	Logix does not communicate its system objectives related to privacy to appropriate clients/vendors. Thus, Not Applicable.	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	the system, objectives related to privacy and changes to those objectives.		
CC 2.3H	Communicates Information About System Operation and Boundaries— The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	Service Agreements are executed with external parties communicating the information about system operations and boundaries.	No exceptions noted.
CC 2.3I	Communicates System Objectives — The entity communicates its system objectives to appropriate external users.	Logix communicates its system objectives to appropriate external parties through executed agreements to ensure mutual understanding and alignment.	No exceptions noted.
CC 2.3J	Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.	Verified that development, design and monitoring of system control activities is performed in house by Logix.	No exceptions noted.
CC 2.3K	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents,	A structured process has been implemented effectively and communicated to external entities for the reporting of system-related issues, incidents and grievances.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	concerns, and other complaints to appropriate personnel.		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
3	RISK ASSESSMENT		
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to identify and assess risks relating to objectives.		
CC 3.1A	Reflects Management's Choices — Operations objectives reflect management's choices about structure, industry considerations, and entity performance.	Logix has aligned its business objectives in accordance with the industry considerations and performance of the organizations.	No exceptions noted.
CC 3.1B	Considers Tolerances for Risk— Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Logix has established Information Security Risk Management Policy and process to systematically assess risk levels and prioritize them based on their potential impact.	No exceptions noted.
CC 3.1C	Includes Operations and Financial Performance Goals— The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	Logix has processes in place to analyse its operational and financial performance against established objectives to ensure alignment with the organization's desired outcomes.	No exceptions noted.
CC 3.1D	Forms a Basis for Committing of Resources— Management uses operations objectives to allocate resources needed to attain desired operations and financial performance.	Logix conducts reviews of its information resource requirements to ensure alignment with established operational objectives and expected performance.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 3.1E	Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate for the circumstances.	Logix's financial reporting objectives are appropriately aligned with established accounting principles and standards.	No exceptions noted.
CC 3.1F	Considers Materiality— Management considers materiality in financial statement presentation.	Logix reviews its financial frameworks including strategy, objectives, and budgeting processes to ensure they are aligned with established materiality thresholds and audit compliance requirements.	No exceptions noted.
CC 3.1G	Reflects Entity Activities —External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.	Corroborative inquiry with the Management confirms that the financial strategies and objectives are aligned and reviewed periodically.	No exceptions noted.
CC 3.1H	Complies With Externally Established Frameworks —Management establishes objectives consistent with laws and regulations, standards, and frameworks of recognized external organizations.	Observed that Logix adheres to externally recognized compliance frameworks such as ISO 27001-2022 and ISO 9001-2015.	No exceptions noted.
CC 3.1I	Considers the Required Level of Precision— Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	Management ensures key operational reports are accurate to meet end user requirements.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 3.1J	Reflects Entity Activities —External reporting reflects the underlying transactions and events within a range of acceptable limits.	Corroborative inquiry with the Management conforms external reporting are in line with the objectives, reviewed periodically and are devoid of any manipulations.	No exceptions noted.
CC 3.1K	Reflects Management's Choices —Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.	Organizational objectives are clearly articulated across all functional levels. Management engages in scheduled review meetings to assess strategic alignment and operational performance metrics	No exceptions noted.
CC 3.1L	Considers the Required Level of Precision— Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	Logix maintains the required level of precision and accuracy in its service delivery, supporting both financial and non-financial reporting objectives aligned with requirements and materiality thresholds with financial reporting.	No exceptions noted.
CC 3.1M	Reflects Entity Activities —Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	Logix's internal reporting mechanisms effectively capture and reflect underlying transactions and events within acceptable parameters, and actively report, evaluate, and address risks or threats arising from within the business environment.	No exceptions noted.
CC 3.1N	Reflects External Laws and Regulations — Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	Observed that Logix aligns with externally mandated legal and regulatory frameworks, such as ISO 27001-2022 and ISO 9001-2015.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 3.1O	Considers Tolerances for Risk— Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Logix has established Information Security Risk Management Policy and Process designed to assess, categorize, and prioritize risks based on their potential impact on operations and business.	No exceptions noted.
CC 3.1P	Establishes Sub-objectives to Support Objectives — Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's reporting, operations, and compliance objectives.	Management conforms that Logix utilizes and implements controls to achieve and maintain its compliance objectives.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks to determine how the risks should be managed.		
CC 3.2A	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to achieving objectives.	Information Security Risk Management Policy and Process are established and designed to identify and evaluate risks across various levels in the organization.	No exceptions noted.
CC 3.2B	Analyzes Internal and External Factors — Risk identification considers internal and external factors and their impact on achieving objectives.	Logix has established Information Security Risk Management Policy and maintains the Risk register to document the outcomes of risk assessments comprising of both internal and external sources.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 3.2C	Involves Appropriate Levels of Management — The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.	Logix has established Information Security Management Policy that defines the effective risk assessment mechanism involving appropriate levels of management to monitor and manage identified risks effectively.	No exceptions noted.
CC 3.2D	Estimates Significance of Risks Identified — Identified risks are analysed through a process that includes estimating the potential significance of the risk.	Logix maintains Risk register that appropriately reflects the potential significance and impact of the identified risks as per the Information security risk management process.	No exceptions noted.
CC 3.2E	Determines How to Respond to Risks— Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	Logix has established Risk Assessment Process within Information Security Risk Management Policy that defines the procedure to manage and respond to the identified risks.	No exceptions noted.
CC 3.2F	Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities — The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets;	Logix has implemented a structured Information Security Risk Assessment Policy to identify threats and vulnerabilities to its information system and assets. Findings are documented and tracked through risk register with assigned risk owners.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	(3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.		
CC 3.2G	Analyses Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	Reviewed the Information Security Risk Management Process and observed that it defines a structured process for identifying, analyzing, and prioritizing risks associated with third parties, business partners and other relevant parties.	No exceptions noted.
CC 3.2H	Considers the Significance of the Risk — The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with	Logix has established the Information Security Risk Management Policy that outlines the process for identifying and mitigating threats; and documents identified risks associated with the business operations and its resources based on their criticality, threat impact, and likelihood in the risk register.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	assets based on asset criticality, threat impact, and likelihood.		
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC 3.3A	Considers Various Types of Fraud — The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Logix has established Information Security Risk Management Policy and Process that outlines the procedures to conduct periodic risk assessments of processes and technology to detect and report risks that possess potential threat to business objectives.	No exceptions noted.
CC 3.3B	Assesses Incentives and Pressures — The assessment of fraud risks considers incentives and pressures.	Logix has processes in place to assess risk factors related to incentives and pressures as part of its risk management.	No exceptions noted.
CC 3.3C	Assesses Opportunities — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	Risk assessments are conducted periodically to evaluate threats possessing from unauthorized access and potential fraud involving Logix's assets and sensitive information.	No exceptions noted.
CC 3.3D	Assesses Attitudes and Rationalizations — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.	Logix has established Disciplinary Policy outlining both formal and informal measures to address instances of misconduct and deviation from established standards that might possess threat to business function.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 3.3E	Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes considering threats and vulnerabilities that arise specifically from IT and access to information.	Logix conducts periodic access reviews and Vulnerability Assessment and Penetration Testing (VAPT) of applications, ensuring that potential risks related to system access and information security are proactively identified and mitigated.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the internal control system.		
CC 3.4A	Assesses Changes in the External Environment — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	Logix has established an Information Security Risk Management Policy and Process that outlines the methodology for identifying risks arising from changes in the business environment or operational functions.	No exceptions noted.
CC 3.4B	Assesses Changes in the Business Model — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	Logix has processes in place to conduct risk assessment to identify potential impact of new business lines or changes in business environment.	No exceptions noted.
CC 3.4C	Assesses Changes in Leadership — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.	Logix has established procedures to analyse and evaluate changes in leadership and internal roles and determine their potential impact on	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
		operational efficiency and control effectiveness.	
CC 3.4D	Assesses Changes in Systems and Technology — The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	Modifications to information systems, applications, technologies, and tools are periodically assessed ensuring alignment with the information security risk management process.	No exceptions noted.
CC 3.4E	Assesses Changes in Vendor and Vendor Relationships — The risk identification process considers changes in vendor relationships.	Logix assesses the change in vendor, vendor relationship and business partners as a part of risk assessment process.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
4	MONITORING ACTIVITIES		
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC 4.1A	Considers a Mix of Ongoing and Separate Evaluations— Management includes a balance of ongoing and separate evaluations.	Observed that business and application processes are aligned to support ongoing evaluations, with specific individuals assigned responsibilities for conducting periodic evaluation.	No exceptions noted.
CC 4.1B	Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	Logix has implemented a formalized mechanism for the periodic review of processes, which includes the assessment of changes in business operations to ensure continued alignment with	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
		organizational objectives and compliance requirements.	
CC 4.1C	Establishes Baseline Understanding — An internal control system's design and current state are used to establish a baseline for ongoing and separate evaluations.	Current state of internal control system design is utilized as a baseline for ongoing and separate evaluation.	No exceptions noted.
CC 4.1D	Uses Knowledgeable Personnel— Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	Observed that designated personnel with required skills and expertise are appointed to perform the ongoing and separate evaluations.	No exceptions noted.
CC 4.1E	Integrates With Business Processes — Ongoing evaluations are built into the business processes and adjust to changing conditions.	Ongoing evaluations are conducted in alignment with defined policies, and their periodic assessment supports continuous improvement in response to dynamic operational conditions.	No exceptions noted.
CC 4.1F	Adjusts Scope and Frequency — Management varies the scope and frequency of separate evaluations depending on risk.	Logix has process in place to assess the scope and frequency of evaluations and adjust them based on the criticality of identified risk.	No exceptions noted.
CC 4.1G	Objectively Evaluates — Separate evaluations are performed periodically to provide objective feedback.	Verified that controls and processes are periodically evaluated, and the outcome from evaluations are reviewed to identify and implement necessary enhancements.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 4.1H	Considers Different Types of Ongoing and Separate Evaluations — Management uses various types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	Logix undertakes various compliances for its business and process by leveraging different types of ongoing and separate evaluations. Additionally, Logix conduct periodic VAPT of its applications and is ISO/IEC 27001 as well as ISO/IEC 9001 certified.	No exceptions noted.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC 4.2A	Assesses Results — As appropriate, management and the board of directors assess the results of ongoing and separate evaluations.	Management reviews the outcomes of both ongoing and separate evaluations to identify deviations and initiate corrective actions as required.	No exceptions noted.
CC 4.2B	Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	Logix has established processes to ensure system deficiencies are promptly escalated to designated personnel, who are responsible for initiating and executing corrective actions.	No exceptions noted.
CC 4.2C	Monitors Corrective Action — Management tracks whether deficiencies are remedied promptly.	Management conducts regular review meetings to ensure oversight on the corrective actions and timely remediation of deficiencies.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
5	CONTROL ACTIVITIES		
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to mitigating risks and achieving objectives to acceptable levels.		
CC 5.1A	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Logix has processes in place to implement control activities to mitigate any identified risks, ensuring the security of its operations and strategic objectives.	No exceptions noted.
CC 5.1B	Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Controls are developed and implemented as per the criticality of operations and specified requirements for the service.	No exceptions noted.
CC 5.1C	Determines Relevant Business Processes —Management determines which relevant business processes require control activities.	Logix has established control activities for key business processes related to application development, deployment, and maintenance.	No exceptions noted.
CC 5.1D	Evaluates a Mix of Control Activity Types — Control activities include various controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls and preventive and detective controls.	Logix has implemented both automated and manual detective as well as preventive controls to identify and mitigate risks that possess threat to information system. Microsoft Intune and Windows Defender are used for regular scanning of end devices. FortiGate firewall is utilized for securing network, CrowdStrike as a SOC/SIEM monitoring solution for servers, also	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
5	CONTROL ACTIVITIES		
		various compliance and incident management mechanisms are enforced for securing Information system.	
CC 5.1E	Considers at What Level Activities Are Applied — Management considers control activities at various levels in the entity.	Logix incorporates risk considerations across different organizational levels and has process in place to apply corresponding controls based on the criticality to ensure effective governance and operational oversight.	No exceptions noted.
CC 5.1F	Addresses Segregation of Duties — Management segregates incompatible duties and selects and develops alternative control activities where such segregation is not practical.	Logix categorizes and addresses the identified risks based on criticality, impact and likelihood of occurrence and documents them in a Risk register. Roles and responsibilities are defined for reporting risks, assigning ownership and accountability for remediation plan within the Information Security Risk Management Policy.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC 5.2A	Determines dependency Between the Use of Technology in Business Processes and Technology General Controls — Management understands and defines the dependency and linkage between business processes, automated control activities, and general technology controls.	Logix has conducted a comprehensive assessment of technology integration across its business processes and platforms and has deployed appropriate tools and controls to support operational efficiency and alignment with strategic objectives.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
5	CONTROL ACTIVITIES		
CC 5.2B	Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Logix has instituted robust control measures to govern the use of technical tools, ensuring that their outputs are consistently accurate, complete, and reliable. These measures provide assurance that the tools function as intended and that the integrity of the resulting information is maintained.	No exceptions noted.
CC 5.2C	Establishes Relevant Security Management Process Controls Activities — Management selects and develops control activities designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and protect the entity's assets from external threats.	Logix has implemented role-based access controls to ensure that employees are granted access strictly based on authorization levels with formal approvals from relevant personnel.	No exceptions noted.
CC 5.2D	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities — Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	Observed that Management has established and maintains control activities related to acquisition, development, and maintenance of technology and its infrastructure to support the achievement of organizational objectives.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
5	CONTROL ACTIVITIES		
CC 5.3A	Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Logix has established formal Policies and Procedures wherein management has clearly defined employee responsibilities and corresponding control activities to ensure accountability and operational consistency.	No exceptions noted.
CC 5.3B	Establishes Responsibility and Accountability for Executing Policies and Procedures — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	Logix has established responsibilities for control activities to designated risk owners within relevant business units to ensure accountability where risks reside.	No exceptions noted.
CC 5.3C	Performs promptly — Responsible personnel perform control activities promptly as defined by the policies and procedures.	Logix has established Roles and Responsibilities Matrix ensuring responsibility and accountability of designated personnel are defined for executing control activities in a timely manner.	No exceptions noted.
CC 5.3D	Takes Corrective Action — Responsible personnel investigates and acts on matters identified because of executing control activities.	Logix has designated individuals with the authority to implement corrective measures in accordance with the established control activities.	No exceptions noted.
CC 5.3E	Performs Using Competent Personnel — Competent personnel with sufficient	Logix hires and appoints qualified and competent personnel to perform	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
5	CONTROL ACTIVITIES		
	authority perform control activities with diligence and continuing focus.	control activities. Periodic performance evaluation is conducted to ensure competent individuals are retained.	
CC 5.3F	Reassesses Policies and Procedures— Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	Logix communicated that periodic reviews of its established policies and procedures are conducted and updated either annually or as necessitated by operational requirements.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
6	LOGICAL AND PHYSICAL CONTROLS		
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC 6.1A	Identifies and Manages the Inventory of Information Assets — The entity identifies, inventories, classifies, and manages information assets.	Logix maintains an Inventory of information assets while classifying them based on their categories and criticalities.	No exceptions noted.
CC 6.1B	Restricts Logical Access — Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components, is restricted using access control software and rule sets.	Logix has implemented role-based access control mechanisms, multifactor authentication through SAML and FortiClient VPN to ensure secure access and connections to the information system and information assets.	No exceptions noted.
CC 6.1C	Identifies and Authenticates Users — Persons, infrastructure, and software	Logix assesses and authenticates authorized users before granting access	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	are identified and authenticated before accessing information assets, whether locally or remotely.	to information and information systems both locally and remotely.	
CC 6.1D	Considers Network Segmentation — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	Logix has process in place to segregate its network, ensuring security and manageability of the network.	No exceptions noted.
CC 6.1E	Manages Points of Access — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each access point are identified, documented, and managed.	Verified that Logix has implemented FortiClient VPN protection and provides role-based access control to ensure that only authorized users can securely access relevant systems and data. Additionally, FortiGate firewall is implemented, Zabbix is used for monitoring activities and Endpoint security solution through CrowdStrike is configured.	No exceptions noted.
CC 6.1F	Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.	Logix has implemented secure VPN Solution with MFA Enabled, role-based access control mechanisms and port restrictions to ensure access to information assets is restricted to authorized users through secure channels.	No exceptions noted.
CC 6.1G	Manages Identification and Authentication — Identification and authentication requirements are established, documented, and managed	Identification and authentication of user access to systems is managed by designated individuals where access is	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	for individuals and systems accessing entity information, infrastructure, and software.	given to users based on their roles and formal authorization.	
CC 6.1H	Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented before being granted access credentials and implemented on the network or access point. Credentials are removed, and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.	Logix has established Access Control Policy that outlines measures to grant access to registered systems and software. Access to information system is revoked or terminated when no longer required.	No exceptions noted.
CC 6.1I	Uses Encryption to Protect Data — The entity uses encryption to supplement other measures used to protect data at rest when such protections are deemed appropriate based on assessed risk.	Logix protects the data at rest using BitLocker Encryption centrally managed by the IT Admin.	No exceptions noted.
CC 6.1J	Protects Encryption Keys — Processes are in place to protect encryption keys during generation, storage, use, and destruction.	Logix has established Cryptography Policy that defines the standards for encrypting data using appropriate encryption mechanisms and secure generation, usage, rotation and destruction of encryption keys. BitLocker Encryption keys used for encrypting data at rest are managed by IT Admin.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 6.2	Before issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC 6.2A	Controls Access Credentials to Protected Assets — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	Logix has established Access Control Policy and has implemented access control for authorized users; access credentials are provisioned after receiving a formal approval.	No exceptions noted.
CC 6.2B	Removes Access to Protected Assets When Appropriate — Processes are in place to remove credential access when an individual no longer requires such access.	Verified that employee access from information assets is revoked on the last day of employment or when no longer required to prevent unauthorized use of company assets and system resources.	No exceptions noted.
CC 6.2C	Reviews Appropriateness of Access Credentials — The appropriateness of access credentials is reviewed periodically for unnecessary and inappropriate individuals with credentials.	Logix has implemented role-based access control with periodic review of access credentials to prevent unauthorized access to sensitive data and critical system.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC 6.3A	Creates or Modifies Access to Protected Information Assets — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Observed that asset owner authorizes the administrative configurations and modifications to protect information assets.	No exceptions noted.
CC 6.3B	Removes Access to Protected Information Assets — Processes are in	Observed that processes are in place for access revocation in a timely manner	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	place to remove access to protected information assets when an individual no longer requires access.	when access is no longer required or when employee exits.	
CC 6.3C	Uses Role-Based Access Controls — Role-based access control is utilized to support the segregation of incompatible functions.	Logix enforces role-based access controls across all business units to ensure that user privileges are appropriately aligned with individual job functions and operational needs.	No exceptions noted.
CC 6.3D	Reviews Access Roles and Rules — The appropriateness of access roles and access rules are reviewed periodically for unnecessary and inappropriate individuals with access, and access rules are modified as appropriate.	Logix has processes in place for conducting periodic access reviews to prevent unauthorized, inappropriate access to its information systems.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC 6.4A	Creates or Modifies Physical Access — Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas based on an authorization from the system's asset owner.	The project scope is limited to the services provided by Logix. Physical access controls are out of scope. Thus, Not Applicable.	Not Applicable.
CC 6.4B	Removes Physical Access — Processes are in place to remove access to physical resources when an individual no longer requires access.	The project scope is limited to the services provided by Logix. Physical access controls are out of scope. Thus, Not Applicable.	Not Applicable.
CC 6.4C	Reviews Physical Access — Processes are in place to periodically review physical	The project scope is limited to the services provided by Logix. Physical	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	access to ensure consistency with job responsibilities.	access controls are out of scope. Thus, Not Applicable.	
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC 6.5A	Identifies Data and Software for Disposal — Procedures are in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.	Logix has processes in place to identify information to dispose and has established Secure Media Disposal Policy for secure disposal of information assets.	No exceptions noted.
CC 6.5B	Removes Data and Software from Entity Control — Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	Logix has formalized a Secure Media Disposal Policy that defines the process to ensure controlled and traceable handling of media assets during secure disposal.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC 6.6A	Restricts Access — The activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Observed that secure communication channel and connection over VPN have been enforced to ensure the confidentiality of sensitive information along with controls to restrict access to only authorized services.	No exceptions noted.
CC 6.6B	Protects Identification and Authentication Credentials — Identification and authentication credentials are protected during	Logix utilizes FortiClient VPN services along with FortiGate firewall protection while working remotely to ensure a secure and private connection during	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	transmission outside its system boundaries.	transmission outside its system boundaries.	
CC 6.6C	Requires Additional Authentication or Credentials — Additional authentication information or credentials are required when accessing the system outside its boundaries.	Logix ensures that access credentials are encrypted and securely transmitted when communicated beyond system boundaries.	No exceptions noted.
CC 6.6D	Implements Boundary Protection Systems — Boundary protection systems (firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	Logix has implemented FortiGate Firewall to protect external access points from unauthorized access, securing external access points against potential threats.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC 6.7A	Restricts the Ability to Perform Transmission — Data loss prevention processes and technologies are used to restrict the ability to authorize and execute transmission, movement, and removal of information.	Logic has implemented Data Loss Prevention mechanisms to restrict unauthorized activities on data.	No exceptions noted.
CC 6.7B	Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect the transmission of data	Observed that data is transmitted using encrypted communication channels to ensure confidentiality and prevent unauthorized access.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	and other communications beyond connectivity access points.		
CC 6.7C	Protects Removal Media — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes) as appropriate.	Verified that FortiGate firewall is implemented to protect critical assets and network along with USB port restrictions. Microsoft Intune and Defender are implemented to enhance endpoint security.	No exceptions noted.
CC 6.7D	Protects Mobile Devices — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.	Logix has established Asset Management Policy and implemented Microsoft Intune along with Windows Defender to protect endpoints to safeguard organizational information assets such as laptops.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
CC 6.8A	Restricts Application and Software Installation — The ability to install applications and software is restricted to authorized individuals.	Logix has established Software Installation Policy that outlines the guidelines and procedures to restrict application installation to authorized personnel. Administrator access is restricted to employees to prevent software installation.	No exceptions noted.
CC 6.8B	Detects Unauthorized Changes to Software and Configuration Parameters — Processes are in place to detect changes to software and configuration parameters that may indicate unauthorized or malicious software.	Logix utilizes Microsoft Intune, Windows Defender and FortiGate Firewall to safeguard against unauthorized changes to software and monitor devices in real-time.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 6.8C	Uses a Defined Change Control Process – A management-defined change control process is used to implement software.	Logix has established Change Management Policy. Verified that all the system changes undergo a structured review and approval process prior to implementation.	No exceptions noted.
CC 6.8D	Uses Antivirus and Anti-Malware Software – Antivirus and anti-malware software is implemented and maintained to provide for the interception, detection, and remediation of malware.	Logix has established Anti Malware Policy that defines process for prevention, early detection and response to malware threats. Antivirus and Antimalware protection are enabled through Microsoft Intune and Windows Defender to regularly scan, detect and address malware threats.	No exceptions noted.
CC 6.8E	Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software – Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected before its implementation on the network.	Logix has established Antivirus and Antimalware protection through Microsoft Intune and Windows Defender to regularly scan, detect and address malware threats and protect information assets from external threats.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
7	SYSTEM OPERATIONS		
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify changes to configurations that result in the introduction of new vulnerabilities, and		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	susceptibilities to newly discovered vulnerabilities.		
CC 7.1A	Uses Defined Configuration Standards – Management has defined configuration standards.	Observed that Logix has defined configuration standards to ensure consistency, security and optimal performance of the system.	No exceptions noted.
CC 7.1B	Monitors Infrastructure and Software – The entity monitors infrastructure and software for non-compliance with the standards, which could threaten the achievement of the entity's objectives.	Logix has implemented Microsoft Intune and Defender for endpoint security and FortiGate firewall to block, protect from unauthorized access to network, Zabbix is used for monitoring activities and CrowdStrike is used as a SOC/SIEM solution to monitor servers.	No exceptions noted.
CC 7.1C	Implements Change-Detection Mechanisms – The IT system includes a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	Logix has implemented detection tools to monitor system in real-time and detect any unauthorized changes and anomalies to critical system and configuration files.	No exceptions noted.
CC 7.1D	Detects Unknown or Unauthorized Components – Procedures are in place to detect the introduction of unknown or unauthorized components.	Logix has enabled Antimalware protection through Windows Defender to actively scan systems and detect as well as prevent, any unauthorized components or activities.	No exceptions noted.
CC 7.1E	Conducts Vulnerability Scans – The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations periodically and after any significant	Logix conducts Vulnerability Assessment and Penetration Testing for its applications, encompassing both application and network-level assessments to identify vulnerabilities	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	change in the environment and takes action to remediate identified deficiencies on a timely basis.	and remediate deficiencies in a timely manner.	
CC 7.2	The entity monitors system components and those components' operation for anomalies indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.		
CC 7.2A	Implements Detection Policies, Procedures, and Tools — Detection policies and procedures are defined and implemented, and detection tools are implemented on infrastructure and software to identify anomalies in operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes the provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	Observed that Logix has defined the processes for detecting and addressing anomalies in the system. Firewall and antivirus solutions are implemented as detection mechanisms for identifying anomalies.	No exceptions noted.
CC 7.2B	Designs Detection Measures — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and	Logix utilizes CrowdStrike for monitoring of servers and FortiGate firewall for securing infrastructure, while Vulnerability Assessment and Penetration Testing is conducted on applications. Additionally, Physical and Environment Security Policy is	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	established defining measures to detect physical security events.	
CC 7.2C	Implements Filters to Analyse Anomalies – Management has implemented procedures to filter, summarize, and analyse anomalies to identify security events.	Logix has established Information Security Risk Management Policy, deployed FortiGate firewall, enforced strong access control measures, implemented Microsoft Intune and Defender for endpoint security and CrowdStrike to detect and analyse anomalies associated with servers.	No exceptions noted.
CC 7.2D	Monitors Detection Tools for Effective Operation – Management has implemented processes to monitor the effectiveness of detection tools.	Logix has processes in place to conduct periodic monitoring of logs from different tools to check effectiveness of detection tools.	No exceptions noted.
CC 7.3	The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC 7.3A	Responds to Security Incidents – Procedures are in place for responding to security incidents and periodically evaluating the effectiveness of those policies and procedures.	Logix has established Incident Management Process outlining the procedures for identifying, reporting and mitigating security incidents.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 7.3B	Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program, and actions are taken, if necessary.	Verified that IT Team at Logix is accountable for the continuous detection, analysis and remediation of security events.	No exceptions noted.
CC 7.3C	Develops and Implements Procedures to Analyse Security Incidents — Procedures are in place to analyse security incidents and determine system impact.	The established Incident Management Process defines that all suspected security events are reported immediately to IT operations through ticketing process and notified to relevant individuals through email.	No exceptions noted.
CC 7.3D	Assesses the Impact on Personal Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.	Logix ensures designated personnel is responsible to assess the impact of unauthorized use or disclosure of personal information.	No exceptions noted.
CC 7.3E	Determines Personal Information Used or Disclosed — The affected information is identified when an unauthorized use or disclosure of personal information has occurred.	Verified that Incident Management Process has been established that defines the procedures for addressing unauthorized use or disclosure of personal information, although no such incident has occurred till the date of Audit.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents as appropriate.		
CC 7.4A	Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	Verified that Incident Management Process is established that defines authorized personnel as per designated role is responsible for carrying out tasks related to design, implementation and maintenance of the incident response program.	No exceptions noted.
CC 7.4B	Contains Security Incidents — Procedures are in place to contain security incidents that actively threaten entity objectives.	Logix has established Incident Management Process and implemented procedures, tools and techniques to effectively minimize, impact of security incidents that threaten entity objectives.	No exceptions noted.
CC 7.4C	Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.	Logix has established a formal Incident Management Process that outlines the process for analysing and mitigating identified security incidents. Although, no incidents have been reported till the date of audit.	No exceptions noted.
CC 7.4D	Ends Threats Posed by Security Incidents — Procedures are in place to end the threats posed by security incidents by closing the vulnerability, removing unauthorized access, and other remediation actions.	Logix has established Incident Management Process and Technical Vulnerability Management Policy that defines the procedure for identifying and remediating vulnerabilities to proactively prevent the exploitation of vulnerabilities and potential loss.	No exceptions noted.
CC 7.4E	Restores Operations — Procedures are in place to restore data and business	Logix has established a Backup and Restoration Policy that defines the	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	operations to an interim state that permits the achievement of entity objectives.	procedure for data restoration. Restoration activities are conducted on a quarterly basis to ensure data integrity and recovery readiness.	
CC 7.4F	Develops and Implements Communication Protocols for Security Incidents — Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Email communication is utilized to communicate security incidents and take necessary actions to develop and implement the remediation plan. Additionally, incidents can also be reported by creating ticket from Sparsh Live portal to respective stakeholders.	No exceptions noted.
CC 7.4G	Obtains Understanding of Nature of Incident and Determines Containment Strategy — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	Logix has established an Incident Management Process that outlines the process for identifying, responding, and remediating security incidents. Reported Incidents are evaluated to understand their nature, criticality and impact on the application and business.	No exceptions noted.
CC 7.4H	Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.	Logix has established Technical Vulnerability Management Policy that outlines the vulnerability management practices to proactively remediate the vulnerabilities.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 7.4I	Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.	Logix has documented an Incident Management Process, outlining the steps and remedial actions which is communicated and made available to relevant individual.	No exceptions noted.
CC 7.4J	Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness periodically.	Logix has established processes to monitor and periodically evaluate the effectiveness of its incident response activities, ensuring continuous improvement and alignment with security objectives.	No exceptions noted.
CC 7.4K	Periodically Evaluates Incidents — Periodically, management reviews security, availability, processing integrity, confidentiality, and privacy incidents and identifies the need for system changes based on incident patterns and root causes.	Logix has established Incident Management Process and maintains Incident Register to document any observed incidents. Processes are in place to periodically review reported security incidents and their mitigation strategies by management.	No exceptions noted.
CC 7.4L	Communicates Unauthorized Use and Disclosure — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.	Logix has procedures in place for communicating unauthorized use or disclosure of personal information to affected data subjects through email.	No exceptions noted.
CC 7.4M	Application of Sanctions — The conduct of individuals and organizations operating under the entity's authority and involved in the unauthorized use or disclosure of personal information is	Logix has established Disciplinary Policy describing the procedures for addressing violations related to privacy and security of personal information,	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.	including both formal and informal enforcement of actions.	
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC 7.5A	Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations as needed.	Logix has established Business Continuity Plan that defines the procedures to ensure critical operations are operative during disruptions like natural disasters or incidents. Backup and Restore Policy define the process to restore business operations.	No exceptions noted.
CC 7.5B	Communicates Information About the Event — Communications about the nature of the incident, recovery actions taken, and activities required to prevent future security events are made to management and others as appropriate (internal and external).	Logix has procedures in place to communicate the information about reported incidents including their nature, analysis and remediation plans to management during review meetings and through internal communication channels.	No exceptions noted.
CC 7.5C	Determines Root Cause of the Event — The event's root cause is determined.	Established Incident Management Process includes defined procedures for conducting root cause analysis of reported security incidents, ensuring its effective remediation and prevention as per assessed criticality and impact.	No exceptions noted.
CC 7.5D	Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls, or both, are	Logix has established process to evaluate reported incidents to assess changes required for recurring events; identified changes can be tested,	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	implemented to prevent and detect recurrences on a timely basis.	developed and implemented to prevent future recurrence of events.	
CC 7.5E	Improves Response and Recovery Procedures — Lessons learned are analysed, and the incident-response plan and recovery procedures are improved.	Logix has implemented Incident response plan within Incident Management Process to recover from any incidents, also lesson learnt are documented for future reference.	No exceptions noted.
CC 7.5F	Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performed periodically. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Incident Management Process is established that defines the process for testing incident response capabilities, including procedures for simulating various incident scenarios, validating detection mechanisms, and assessing the effectiveness of containment, eradication and recovery strategies.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
8	CHANGE MANAGEMENT		
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 8.1A	Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.	Logix has documented Change Management Policy to ensure that all changes to systems, processes or services are planned, reviewed, approved and implemented in controlled environment to support availability and processing integrity.	No exceptions noted.
CC 8.1B	Authorizes Changes — A process is established to authorize system changes before development.	Verified that change request raised to designated personnel are reviewed, evaluated and authorized before development by authorized personnel.	No exceptions noted.
CC 8.1C	Designs and Develops Changes — A process is in place to design and develop system changes.	Logix has established Secure Software Development Policy and Change Management Policy that outlines the process for design and development of system changes.	No exceptions noted.
CC 8.1D	Documents Changes — A process is in place to document system changes to support ongoing system maintenance and support system users in performing their responsibilities.	Logix has processes in place to document system changes and support ongoing maintenance of the system. Changes are documented and tracked by authorized personnel.	No exceptions noted.
CC 8.1E	Tracks System Changes — A process is in place to track system changes before implementation.	Verified that changes are tested in development environment and moved to validation environment prior to deployment.	No exceptions noted.
CC 8.1F	Configures Software — A process is in place to select and implement the	Observed that Logix defines and implements appropriate configuration	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	configuration parameters used to control the software's functionality.	parameters to regulate software behaviour and functionality.	
CC 8.1G	Tests System Changes — A process is in place to test system changes before implementation.	Verified that Changes to the application are tested in development and testing environments before implementation.	No exceptions noted.
CC 8.1H	Approves System Changes — System change approval before implementation.	Verified that changes are tested in development environment and moved to validation environment, approval is obtained from management prior to implementation.	No exceptions noted.
CC 8.1I	Deploys System Changes — A process is in place to implement system changes.	Logix has established Change Management Policy and procedures are in place to deploy system changes by relevant personnel.	No exceptions noted.
CC 8.1J	Identifies and Evaluates System Changes — Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.	Logix has implemented Change Management Policy that defines system objectives affected by system changes are identified prior to development and approved by stakeholders to meet objectives throughout the system development lifecycle.	No exceptions noted.
CC 8.1K	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.	Logix has established and documented the procedures to identify changes in infrastructure and operational system in an event of incident to develop required changes and remediate incidents.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 8.1L	Creates Baseline Configuration of IT Technology — A baseline configuration of IT and control systems is created and maintained.	Logix has established process and maintains configuration parameters for IT and control system.	No exceptions noted.
CC 8.1M	Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergencies (that is, changes that need to be implemented in an urgent time frame).	Verified the Change management policy and observed that the procedure outlines the necessary steps for authorizing, designing, testing, approving and implementing necessary emergency changes.	No exceptions noted.
CC 8.1N	Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.	Logix has established Secure Software Development Policy as well as Data protection and Privacy Policy that outlines the measures for protection of personnel information during implementation and change processes to meet entity's objectives related to confidentiality.	No exceptions noted.
CC 8.1O	Protects Personal Information — The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.	Protection of personal information is not in the scope by Logix. Thus, Not Applicable.	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
9	RISK MITIGATION		
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC 9.1A	Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	Logix has established Information Security Risk Management Policy that outlines the detail process for identifying, assessing and mitigating potential risk that could impact organizational objectives.	No exceptions noted.
CC 9.1B	Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	Risk mitigation activities are defined to contain any financial impact of identified risks.	No exceptions noted.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC 9.2A	Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes	Observed that vendor and business partner engagements are assessed to ensure alignment with compliance objectives and regulatory standards.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
	1. scope of services and product specifications, 2. roles and responsibilities, 3. compliance requirements, and 4. service levels.		
CC 9.2B	Assess Vendor and Business Partner Risks — The entity periodically assesses the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.	Logix has defined the process for assessing risks associated with vendors and business partners.	No exceptions noted.
CC 9.2C	Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for managing risks associated with vendors and business partners.	Verified the Information Security Risk management policy and observed that Logix assigns responsibility and accountability for managing risks associated with vendors and business partners to designated personnel.	No exceptions noted.
CC 9.2D	Establishes Communication Protocols for Vendors and Business Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	Logix has established process and executes agreements that outlines the communication methods and contact person for managing services related to issues with external parties.	No exceptions noted.
CC 9.2E	Establishes Exception Handling Procedures from Vendors and Business Partners — The entity establishes exception-handling procedures for service or product issues related to vendors and business partners.	Logix has established an exception handling process for service or product related issues with clients and external parties.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 9.2F	Assesses Vendor and Business Partner Performance – The entity periodically assesses the performance of vendors and business partners.	Logix periodically conducts performance evaluations of its vendors and business partners to assess their performance and adherence to Logix's expectations from them.	No exceptions noted.
CC 9.2G	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments – The entity implements procedures for addressing issues identified with vendor and business partner relationships.	Logix has executed a Service Agreement and established Supplier Relationship Policy that defines the process for addressing vendor-related issues identified during assessments ensuring timely resolution, maintaining service quality, and uphold compliance with organizational objectives.	No exceptions noted.
CC 9.2H	Implements Procedures for Terminating Vendor and Business Partner Relationships – The entity implements procedures for terminating vendor and business partner relationships.	Logix executes Service Agreements with external parties ensuring their commitments towards termination clauses. Processes are in place for terminating vendor and business partner relationship by providing formal email and closing the services.	No exceptions noted.
CC 9.2I	Obtaining Confidentiality Commitments from Vendors and Business Partners – The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners with access to confidential information.	Logix executes Agreements with vendors to formally establish their obligation to protect confidential information accessed during engagement. These agreements define the scope of confidentiality, outlines the types of sensitive data covered, and specify the duration of the commitment.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
CRITERIA FOR SECURITY			
CC 9.2J	Assesses Compliance with Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.	Logix has executed Agreements with vendors and business partners, which defines their obligations to uphold the entity's confidentiality commitments. Vendor risk assessment is performed for assessing ongoing compliance with the organization's data protection and confidentiality requirements.	No exceptions noted.
CC 9.2K	Obtains Privacy Commitments from Vendors and Business Partners — The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.	Logix does not obtain privacy commitments from third parties as it is out of scope. Thus, Not Applicable.	Not Applicable.
CC 9.2L	Assesses Compliance with Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and take corrective action as necessary.	Logix does not obtain privacy commitments from third parties as it is out of scope. Thus, Not Applicable.	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C 1.1A	Identifies Confidential information — Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Data Retention Policy has been established that describes the identification, classification and protection of confidential information, also retention period of confidential information being stored and processed if formally documented.	No exceptions noted.
C 1.1B	Protects Confidential Information from Destruction — Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.	Logix has established Data Protection and Privacy Policy that outlines the protection of confidential information from erasure or destruction during specified retention period of the information.	No exceptions noted.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C 1.2A	Identifies Confidential Information for Destruction — Procedures are in place to identify confidential information requiring destruction at the end of the retention period.	Logix has procedures in place to purge confidential information based on the mutually agreed retention period within executed Service Agreement or the standard period defined in Data Protection and Privacy Policy and can notify relevant personnel of data being purged.	No exceptions noted.
C 1.2B	Destroys Confidential Information — Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	Logix has established Data Disposal Policy that defines secure data deletion and destruction process for the personal data or sensitive information identified for destruction.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR AVAILABILITY			
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (Infrastructure, data, and software) to manage capacity, demand, and to enable the implementation of additional capacity to help meet its objectives.		
A 1.1A	Measures Current Usage — The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.	Logix has established Capacity Management Policy as a reference framework for identifying capacity constraints associated with the talent and business requirements.	No exceptions noted.
A 1.1B	Forecasts Capacity — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.	Logix has established Capacity Management Policy to ensure efficient resource utilization and minimize service disruptions during business operations.	No exceptions noted.
A 1.1C	Makes Changes Based on Forecasts — The system change management process is initiated when forecasted usage exceeds capacity tolerances.	Logix has established Capacity Management Policy to ensure efficient resource utilization and minimize service disruptions during business operations.	No exceptions noted.
A 1.2	The entity authorizes, designs, develops, acquires, implements operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A 1.2A	Identifies Environmental Threats — As part of the risk assessment process, management identifies environmental threats that could impair the system's availability, including threats resulting from adverse weather, failure of	The project scope is limited to the services provided by Logix. Physical access controls towards service is out of scope. Thus, Not Applicable.	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR AVAILABILITY			
	environmental control systems, electrical discharge, fire, and water.		
A 1.2B	Designs Detection Measures — Detection measures are implemented to identify anomalies that could result from environmental threat events.	The project scope is limited to the services provided by Logix. Physical access controls towards service is out of scope. Thus, Not Applicable.	Not Applicable.
A 1.2C	Implements and Maintains Environmental Protection Mechanisms — Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.	The project scope is limited to the services provided by Logix. Physical access controls towards service is out of scope. Thus, Not Applicable.	Not Applicable.
A 1.2D	Implements Alert to Analyse Anomalies — Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.	The project scope is limited to the services provided by Logix. Physical access controls towards service is out of scope. Thus, Not Applicable.	Not Applicable.
A 1.2E	Responds to Environmental Threat Events — Procedures are in place for responding to environmental threat events and for periodically evaluating the effectiveness of those policies and procedures. This includes automatic mitigation systems (for example, uninterruptable power systems and generator backup subsystems).	The project scope is limited to the services provided by Logix. Physical access controls towards service is out of scope. Thus, Not Applicable.	Not Applicable.
A 1.2F	Communicates and Reviews Detected Environmental Threat Events — Detected environmental threat events	The project scope is limited to the services provided by Logix. Physical	Not Applicable.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR AVAILABILITY			
	are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.	access controls towards service is out of scope. Thus, Not Applicable.	
A 1.2G	Determines Data Requiring Backup — Data is evaluated to determine whether a backup is required.	Data backup evaluation process is conducted to determine whether backup is required based on operational and business needs. Processes are in place to perform regular backups.	No exceptions noted.
A 1.2H	Performs Data Backup — Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.	Logix conducts daily backup of data, ensuring secure storage at both primary and secondary locations.	No exceptions noted.
A 1.2I	Addresses Offsite Storage — Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	Verified that continuous availability is ensured by performing regular backups and storing them on alternate region than that of primary environment.	No exceptions noted.
A 1.2J	Implements Alternate Processing Infrastructure — Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Business Continuity Plan outlines the procedures for the migration of process to alternate environment to ensure continuity in the event when primary processing infrastructure becomes unavailable.	No exceptions noted.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR AVAILABILITY			
A 1.3 A	Implements Business Continuity Plan Testing — Business continuity plan testing is performed periodically. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Logix has established Business Continuity Plan that defines procedure for preparing, responding to, and recovering from potential disruptions to business operations.	No exceptions noted.
A 1.3 B	Tests Integrity and Completeness of Backup Data — The integrity and completeness of backup information are tested periodically.	Logix has the procedure of conducting regular backups and designated personnel as per role is responsible for testing completeness of backup.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
PI 1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processes and product and service specifications, to support the use of products and services.		
PI 1.1A	Identifies Information Specifications - The entity identifies information	Logix follows a procedure for determination of information specification required to facilitate and	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
	specifications required to support the use of products and services.	utilization of its services ensuring consistency, accuracy and alignment with processing requirements.	
PI1.1B	Defines Data Necessary to Support a Product or Service - When data is provided as part of a service or a product or as part of a reporting obligation related to a product or service: 1. The definition of the data is available to the users of the data. 2. The definition of the data includes the following information: a. The population of events or instances included in the data. b. The nature of each element of the data. c. Source(s) of the data. d. The unit(s) of measurement of data elements. e. The accuracy/ correctness/ precision of measurement. f. The uncertainty or confidence interval is inherent in each data element and the population of those elements. g. The date the data was observed or the period during which the events relevant to the data occurred.	Observed that data is classified in accordance with the Logix's standards and client requirements and effectively communicated to relevant users.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
	h. The factors and the date and period were used to determine the inclusion and exclusion of items in the data elements and population. 3. The definition is complete and accurate. 4. The description of the data identifies any information necessary to understand each data element and the population in a manner consistent with its definition and intended purpose that has not been included within the data.		
PI 1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
PI 1.2A	Defines Characteristics of Processing Inputs - The characteristics of processing inputs necessary to meet requirements are defined.	Logix defines the characteristics of processing inputs as per Service Agreement to ensure consistency, accuracy and alignment with system requirements and business objectives.	No exceptions noted.
PI 1.2B	Evaluates Processing Inputs - Processing inputs are evaluated for compliance with defined input requirements.	Logix evaluates processing inputs to ensure that the collection and use of personal data align with defines purposes, legal requirements, and organizational policies.	No exceptions noted.
PI 1.2C	Creates and Maintains Records of System Inputs - Records of system input activities are created and maintained completely and accurately promptly.	Logix has defined procedures to create and maintained records of system inputs accurately by relevant individual in timely manner.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
PI 1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
PI 1.3A	Defines Processing Specifications - The processing specifications necessary to meet product or service requirements are defined.	Logix has clearly defined specifications aligned with service requirements, supporting consistent delivery of expected outcomes.	No exceptions noted.
PI 1.3B	Defines Processing Activities - Processing activities are defined to result in products or services that meet specifications.	Processing activities are well-defined and effectively communicated to relevant stakeholders, ensuring that products and services meet established specifications.	No exceptions noted.
PI 1.3C	Detects and Corrects Production Errors - The production process detects and corrects errors promptly.	Logix does not host the production environment, it provides services based on client requirements on their environment and agreed Statement of Work.	No exceptions noted.
PI 1.3D	Records System Processing Activities - System processing activities are recorded completely and accurately promptly.	Resource and talent activities are recorded completely, accurately, and in a timely manner by Logix to detect and correct errors.	No exceptions noted.
PI 1.3E	Processes Inputs - Inputs are processed completely, accurately, and timely as authorized following defined processing activities.	Logix ensures that all inputs are processed in a complete, accurate, and timely manner, by strictly following authorized procedures and established processing guidelines.	No exceptions noted.
PI 1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and following timely specifications to meet the entity's objectives.		
PI 1.4A	Protects Output - Output is protected when stored or delivered to prevent	Logix ensures that output is protected during storage and delivery to prevent	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
	theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.	destruction or corruption that could compromise its ability to meet required specifications.	
PI 1.4B	Distributes output Only to Intended Parties - Output is distributed or made available only to intended parties.	Logix ensures that service output is individual to client requirement and delivered as per service requirement.	No exceptions noted.
PI 1.4C	Distributes output Completely and Accurately - Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.	Logix ensures that service output is individual to client requirement and delivered accurately within timeframe as per service requirement.	No exceptions noted.
PI 1.4D	Creates and Maintains Records of System Output Activities - Records of system output activities are created and maintained completely and accurately promptly.	Logix has procedures for providing system output activities that are created and maintained completely and accurate in timely manner.	No exceptions noted.
PI 1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely as per system specifications to meet the entity's objectives.		
PI 1.5A	Protects Stored Items - Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.	Authorized personnel as per role is responsible for safeguarding stored items against theft, corruption, or destruction that could compromise the output's ability to meet required specifications.	No exceptions noted.
PI 1.5B	Archives and Protects System Records - System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.	Logix has processes in place to identify data and system records for archival and protect the archived data using appropriate security measures.	No exceptions noted.

Ref. No.	Description and Design of Controls	Testing the Design of Controls	Conclusions
ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY			
PI 1.5C	Stores Data Completely and Accurately - Procedures are in place to provide for the complete, accurate, and timely storage of data.	Logix ensures that all collected data is stored in a complete and accurate manner, aligning with the integrity principles.	No exceptions noted.
PI 1.5D	Creates and Maintains Records of System Storage Activities - Records of system storage activities are created and maintained completely and accurately promptly.	Logix has procedure for creating and maintaining a complete record of system storage activities in a timely manner.	No exceptions noted.

END OF DOCUMENT