A-LIGN

EdgeConneX Holdings, LLC

Type 2 SOC 2

2025

edgeconnex®

REPORT ON EDGECONNEX HOLDINGS, LLC’S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

May 1, 2024 to April 30, 2025

Table of Contents

SECTION 1

ASSERTION OF EDGECONNEX HOLDINGS, LLC MANAGEMENT

ASSERTION OF EDGECONNEX HOLDINGS, LLC MANAGEMENT

May 5, 2025

We have prepared the accompanying description of EdgeConneX Holdings, LLC's ('EdgeConneX' or 'the Company') Colocation Services System titled "EdgeConneX Holdings, LLC's Description of Its Colocation Services System throughout the period May 1, 2024 to April 30, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Colocation Services System that may be useful when assessing the risks arising from interactions with EdgeConneX's system, particularly information about system controls that EdgeConneX has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

EdgeConneX uses IES Commercial Inc. ('IES') and Salute Incorporated ('SALUTE') to provide data center staffing and monitoring services, and CrowdStrike to provide antivirus monitoring services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EdgeConneX, to achieve EdgeConneX's service commitments and system requirements based on the applicable trust services criteria. The description presents EdgeConneX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EdgeConneX's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EdgeConneX, to achieve EdgeConneX's service commitments and system requirements based on the applicable trust services criteria. The description presents EdgeConneX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EdgeConneX's controls.

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

a. the description presents EdgeConneX's Colocation Services System that was designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that EdgeConneX's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of EdgeConneX's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that EdgeConneX's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of EdgeConneX's controls operated effectively throughout that period.

Edmund Wilson

Edmund Wilson
COO
EdgeConneX Holdings, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: EdgeConneX Holdings, LLC

Scope

We have examined EdgeConneX's accompanying description of its Colocation Services System titled "EdgeConneX Holdings, LLC's Description of Its Colocation Services System throughout the period May 1, 2024 to April 30, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that EdgeConneX's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

EdgeConneX uses IES and SALUTE to provide data center staffing and monitoring services, and CrowdStrike to provide antivirus monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EdgeConneX, to achieve EdgeConneX's service commitments and system requirements based on the applicable trust services criteria. The description presents EdgeConneX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EdgeConneX's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EdgeConneX, to achieve EdgeConneX's service commitments and system requirements based on the applicable trust services criteria. The description presents EdgeConneX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EdgeConneX's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

EdgeConneX is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that EdgeConneX's service commitments and system requirements were achieved. EdgeConneX has provided the accompanying assertion titled "Assertion of EdgeConneX Holdings, LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. EdgeConneX is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects,

a. the description presents EdgeConneX's Colocation Services System that was designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that EdgeConneX's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of EdgeConneX's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that EdgeConneX's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of EdgeConneX's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4*,* is intended solely for the information and use of EdgeConneX, user entities of EdgeConneX's Colocation Services System during some or all of the period May 1, 2024 to April 30, 2025, business partners of EdgeConneX subject to risks arising from interactions with the Colocation Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements 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.

A-LIGN ASSURANCE

Tampa, Florida
May 5, 2025

SECTION 3

EDGECONNEX HOLDINGS, LLC’S DESCRIPTION OF ITS COLOCATION SERVICES SYSTEM THROUGHOUT THE PERIOD MAY 1, 2024 TO APRIL 30, 2025

OVERVIEW OF OPERATIONS

Company Background

EdgeConneX, based in Herndon, Virginia, was formed in 2010, enabling fiber and infrastructure solutions for network providers and building owners. Through organic growth, EdgeConneX has grown from a small team, with operations primarily based in Herndon, Virginia, to a company of nearly 200 employees including growing resource pools based out of Denver, Colorado, Amsterdam, Netherlands and Singapore, Singapore. After years of experience in the cable and wireless segments, EdgeConneX turned to the world of data centers offering space, power, and connectivity to customers with edge network needs.

The Company's Edge Services provide space, power, and connectivity to enable digital content and localized cloud solutions. With EdgeConneX, content delivery is optimized by placing Edge Data Centers® and Edge PoPs® at the most critical locations-as close as possible to the end users' point of access. By using EdgeConneX services, digital content can be delivered with higher performance and lower latency, with a more efficient cost structure.

EdgeConneX also enables the full benefits of the cloud by providing hybrid, multi-cloud solutions through Edge Data Centers® located in close proximity to end users. EdgeConneX has delivered more than 3,000 locations across their portfolio of Edge Services. EdgeConneX manages a proprietary database of four million buildings, 14 million businesses and 200,000 cell towers that are utilized in partnership with their customers to determine the most optimal site for upcoming infrastructure.

Description of Services Provided

EdgeConneX specializes in providing purpose-built, edge-of-network facilities that enable the delivery of bandwidth intensive, latency sensitive content and applications to local consumers and enterprises. EdgeConneX is redefining the edge of the internet by designing and deploying Edge Data Centers® that are strategically positioned nearest to network provider aggregation points, establishing new local peering facilities. This ensures content delivery with an improved quality of service and increased security.

EdgeConneX facilitates distribution models in support of their customer's content and applications at the edge of the network. These purpose-built Edge Data Centers® are designed and deployed in conjunction with EdgeConneX customers to ensure the most proper placement of their content and applications. EdgeConneX works with incumbent local exchange carriers (ILECs), cable, wireless, content, and enterprise companies to provide infrastructure.

EdgeConneX hosts data centers in the following markets:

Market	Site
Amsterdam, Netherlands	EDCAMS01/02/03/04/05/06
Arcata California	EDCACV01
Atlanta, Georgia	EDCATL01/02
Barcelona, Spain	EDCBCN01
Boston, Massachusetts	EDCBOS01
Brussels, Belgium	EDCBRU01
Buenos Aires, Argentina	EDCBUE01
Chicago, Illinois	EDCCHI01/02
Denver, Colorado	EDCDEN01

Market	Site
Detroit, Michigan	EDCDET01
Dublin, Ireland	EDCDUB01/02/03
Houston, Texas	EDCHOU01
Jacksonville, Florida	EDCJAX01
Jakarta, Indonesia	EDCJKT01
Las Vegas, Nevada	EDCLAS01
Madison, Wisconsin	EDCMAD01
Memphis, Tennessee	EDCMEM01
Miami, Florida	EDCMIA01/02
Minneapolis, Minnesota	EDCMSP01
Munich, Germany	EDCMUC01
Nashville, Tennessee	EDCNAS01
Norfolk, Virginia	EDCNOR01
Phoenix, Arizona	EDCPHX01
Pittsburgh, Pennsylvania	EDCPIT01
Portland, Oregon	EDCPOR01/02
Richmond, Virginia	EDCRIC01
Sacramento, California	EDCSAC01
Santiago, Chile	EDCSCL01/02
San Diego, California	EDCSDG01
Seattle, Washington	EDCSEA01
Salt Lake City, Utah	EDCSLC01
Slidell, Louisiana	EDCSLI01
Santa Clara, California	EDCSVC01/02
Tallahassee, Florida	EDCTAL01
Tel Aviv, Israel	EDCTLV01/11/21
Toronto, Canada	EDCTOR01
Warsaw, Poland	EDCWAW01/02/03

Space

- Each data center contains between 5,400 sq. ft. and 20,0000 sq. ft. of raised floor for tenant racks
- EdgeConneX maintains right of first refusal (ROFR) on adjacent spaces
- The data centers maintain close proximity to metro downtown areas and international airports
- Customer workspace is available
- The data centers maintain available space for secure customer storage
- Wi-Fi access via segmented guest network and cell phone repeaters/boosters is present throughout the facilities

Cooling

- Temperature and humidity monitored, controlled, and managed to industry standards
- 30 inch raised/under floor forced air plenum
- N+1 computer room air conditioning units (CRACs) located in separate suites, maximizing customer-designated areas

Power

- Concurrently maintainable power in a minimum of an N+1 configuration to include:
  - Power Distribution Units (PDU)
  - Uninterrupted Power Supply (UPS)
  - Generators
- Capable of 20+kW per cabinet
- Capable of 600+ watts per sq. ft
- Ghost space not required for cooling power dense installations
- Real-time branch circuit monitoring

Security

- Multi-stage security containment systems that use Personal Identification Numbers (PIN) and live video authentication
- Mantraps and strictly enforced protocols regarding entry access
- 24/7 Color Closed Circuit Television (CCTV) / video surveillance and >90-day online video storage
- Interior managed security zones
- National network operations center for security management
- 24/7 NOC services

Network

- Fiber Points of Entry (POEs) are diverse, with a variety of fiber conduits to physically diverse Meet Me Rooms (MMRs)
- Comcast, Cox, Integra, Zayo, XO, CenturyLink, Utopia, Level 3, Verizon, AT&T, Xmission and Windstream are available providers
- Interconnection services are available

Fire Suppression/Detection

- Pre-action, zoned dry-pipe sprinkler systems with zoned maintenance aisles and separate suites
- Fire extinguishers are present in the facilities
- Smoke detectors are present in the facilities

Optional Services

- Remote hands services for break fixes, configuration, and troubleshooting
- EdgeConneX services: design, build, implement and maintain customer equipment infrastructure
- EdgeOS™, the next generation data center operating system provides real-time visibility, including ticketing and Service Level Agreement (SLA) management for all Edge Data Center locations

Principal Service Commitments and System Requirements

EdgeConneX designs its processes and procedures to meet its objectives for its colocation services. Those objectives are based on the service commitments that EdgeConneX makes to user entities, the laws and regulations that govern the provision of colocation services, and the financial, operational, and compliance requirements that EdgeConneX has established for the services.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided to user entities.

EdgeConneX establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in EdgeConneX's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific processes required in the operation of the colocation services.

Components of the System

Infrastructure

Primary infrastructure used to provide EdgeConneX's Colocation Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
ATS	ASCO 1600 amp	Automatic transfer switch
UPS	Liebert	Uninterruptable power supply
Remote Power Panel	Liebert	Power monitoring and distribution
CRAC	Liebert	Used in electrical rooms and Data Center Hall for environmental controls
Generator	MTU	Emergency generator powered by diesel for power outages
Security Access Pin Pad	Lenel	Manage access to facilities
Fire Communication System	Fike	Fire monitoring and alarm system along with fire suppression equipment
PDU	Liebert	Transformer from 480V to 120/208 to RPPs

Software

Primary software used to EdgeConneX's Colocation Services System includes the following:

Primary Software	
Software	**Purpose**
EdgeOS™	Proprietary platform used to monitor all activity within the Data Centers
RIO	Proprietary program used to manage pre-deployment of Data Centers

People

The EdgeConneX staff provides support for the above services in each of the following functional areas:

- Executive Management - provides general oversight and strategic planning of operations as well as overall corporate development

- Systems Team - responsible for delivering, maintaining, and updating a responsive system that fully complies with functional specifications
- Product - works with all functional teams in the company to design, build, and provide the support for the line of services
- Operations - responsible for effective provisioning, installing/configuring, operating, and maintaining of data center hardware and facilities
- Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements
- Sales/Business Development - works with customers setting expectations and working to ensure deployments meet customer needs
- Client Services - works with existing customers to ensure customer satisfaction as well as communicate vital information around billing, SLA management and deployments

Data

Customer services are managed with specific requirements formally established in customer contracts. Customer information is captured which is utilized by EdgeConneX in delivering its data center services. Such information includes, but is not limited to, the following:

- Space, power, connectivity
- Alert notifications and monitoring reports generated from the proprietary monitoring application, EdgeOS™
- Vulnerability or security alerts received from various sources
- Incident reports documented via the ticketing systems

Processes, Policies and Procedures

Formal Information Technology (IT) policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to EdgeConneX policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any EdgeConneX team member.

Physical Security

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to EdgeConneX policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any EdgeConneX team member.

EdgeConneX utilizes a two-factor authentication protocol for entering all Edge Data Centers. PINs are used to enter the mantrap from outside of the facility. Second authentication step is either Biometric, Network Operations Center (NOC) identification, or text back procedures based on the location and user permissions.

The access PIN system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees, Customers, and vendors granted access PINs are assigned to roles based on their job responsibilities.

Upon an employee's termination of employment, the Human Resources (HR) department generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. On a routine basis, the director of operations audits access levels to ensure that people with data center access credentials are updated to exclude terminated persons and/or contractors no longer needing to be on site.

On a routine basis, a list of each vendor's employees is submitted for vendor review. Vendors are required to return the confirmation of access within two weeks. The Director follows up on any access lists not returned.

Environmental protections are monitored continuously through EdgeOS™ in order to maintain proper data center conditions. Alarms and alerts are activated when certain service level agreements are not met, and appropriate action will be taken.

Logical Access

EdgeConneX uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

EdgeConneX uses a proprietary and patented software program to monitor and control all aspects of each data center from people management as well as equipment and facility management.

All resources with access are managed in EdgeOS™ and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing reviews of access by role.

Employees and approved vendor personnel sign on to the secured EdgeConneX network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity. There is also a guest network segmented from the rest of the data center that any person can access.

Customer employees' access EdgeOS™ services through the Internet using the secure socket layer (SSL) functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with the EdgeConneX configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. Prior to the employee's start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the IT team to create user IDs and access rules. Access rules have been pre-defined based on the defined roles by direct managers of that person. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

The HR system generates a list of terminated employees as needed. This report is used by the IT team to delete employee access. As needed, HR runs a list of active employees. The IT department uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the IT team for processing. The IT manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the Vice President (VP) of Systems reviews employees with access to privileged roles and requests modifications through the event management system.

Customer Requests and Incident Management

EdgeConneX maintains policies and procedures to guide personnel in documenting and implementing customer requests and incidents. Customer request and incident handling procedures include initiation processes, documentation requirements, quality assurance testing requirements, and required approval procedures.

EdgeOS™ is utilized to document the customer request and incident management procedures for changes, incidents, and new implementations. Management approves changes prior to implementation into the production environment and documents those approvals within EdgeOS™.

Facility environmental are monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and remote hands services are deployed to trouble shoot any issues in order to prevent any SLA violations.

Boundaries of the System

The scope of this report includes the Colocation Services System performed in the Amsterdam, Netherlands (EDCAMS01, EDCAMS02, EDCAMS03, EDCAMS04, EDCAMS05, EDCAMS06); Arcata, California (EDCACV01); Atlanta, Georgia (EDCATL01, EDCATL02); Barcelona, Spain (EDCBCN01); Boston, Massachusetts (EDCBOS01); Brussels, Belgium (EDCBRU01); Buenos Aires, Argentina (EDCBUE01); Chicago, Illinois (EDCCHI01, EDCCHI02); Denver, Colorado (EDCDEN01 and Corporate Office); Detroit, Michigan (EDCDET01); Dublin, Ireland (EDCDUB01, EDCDUB02, EDCDUB03); Herndon, Virginia (Corporate Office); Houston, Texas (EDCHOU01); Jacksonville, Florida (EDCJAX01); Jakarta, Indonesia (EDCJKT01); Las Vegas, Nevada (EDCLAS01); Madison, Wisconsin (EDCMAD01); Memphis, Tennessee (EDCMEM01); Miami, Florida (EDCMIA01, EDCMIA02); Minneapolis, Minnesota (EDCMSP01); Munich, Germany (EDCMUC01); Nashville, Tennessee (EDCNAS01); Norfolk, Virginia (EDCNOR01); Phoenix, Arizona (EDCPHX01); Pittsburgh, Pennsylvania (EDCPIT01); Portland, Oregon (EDCPOR01, EDCPOR02); Richmond, Virginia (EDCRIC01); Sacramento, California (EDCSAC01); Santiago, Chile (EDCSCL01, EDCSCL02); San Diego, California (EDCSDG01); Seattle, Washington (EDCSEA01); West Valley City, Utah (EDCSLC01); Slidell, Louisiana (EDCSLI01); Santa Clara, California (EDCSVC01, EDCSVC02); Tallahassee, Florida (EDCTAL01); Tel Aviv, Israel (EDCTLV01, EDCTLV11, EDCTLV21); Toronto, Ontario, Canada (EDCTOR01); and Warsaw, Poland (EDCWAW01, EDCWAW02, EDCWAW03).

This report does not include the data center staffing and monitoring services provided by IES or SALUTE or the antivirus monitoring services provided by CrowdStrike.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the EdgeConneX control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of EdgeConneX ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formal documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel

- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook

Commitment to Competence

EdgeConneX management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Reviews are performed to help managers and employees manage performance

Management's Philosophy and Operating Style

The EdgeConneX management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole
- Executive management is updated routinely on daily operations of facilities
- Board of Directors meet to guide the company making sure company goals are set out clearly
- Annual All-Hands meetings are conducted for all EdgeConneX staff

Organizational Structure and Assignment of Authority and Responsibility

The EdgeConneX organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The EdgeConneX assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

EdgeConneX success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. The EdgeConneX HR's policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

The EdgeConneX risk assessment process identifies and manages risks that could potentially affect the ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. EdgeConneX identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by EdgeConneX, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- IT Risk - changes in systems, users, and cybersecurity
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

EdgeConneX has established the Product Organization to be responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. EdgeConneX attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of the EdgeConneX Colocation Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. EdgeConneX addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, EdgeConneX management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are integral components of EdgeConneX internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, IT. At EdgeConneX information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, All-Hands calls are hosted to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate EdgeConneX personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. EdgeConneX management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

EdgeConneX management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in EdgeConneX operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of EdgeConneX personnel.

Reporting Deficiencies

EdgeOS™ is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Changes to the System Since the Last Review

EdgeConneX commissioned EDTLV21 on January 1, 2025, the third data center location in Israel. No other significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

The following criteria are not applicable to the Colocation Services System:

Criteria Not Applicable to the System		
Category	**Criteria**	**Reason**
Common Criteria / Security	CC6.7	EdgeConneX's services do not include the transmission, movement, or removal of information.

Subservice Organizations

This report does not include the data center staffing and monitoring services provided by IES and SALUTE or the antivirus monitoring services provided by CrowdStrike.

Subservice Description of Services

IES and SALUTE provide the security staffing and monitoring resources that are required to operate a data center. EdgeConneX utilizes CrowdStrike to provide endpoint security protection and threat intelligence services.

Complementary Subservice Organization Controls

EdgeConneX's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organizations controls. It is not feasible for all of the trust services criteria related to EdgeConneX's services to be solely achieved by EdgeConneX control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of EdgeConneX.

The following subservice organizations controls should be implemented by IES to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organizations - IES		
Category	**Criteria**	**Control**
Common Criteria / Security	CC4.1, CC7.2, CC7.3, CC7.4, CC7.5	Incidents and issues are handled according to entity established policies as part of the incident response process.
	CC4.1, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1	Customer service requests and potential incidents are handled according to entity established policies.
	CC6.4	Physical access to the data center facilities is restricted to authorized internal and external users.

The following subservice organizations controls should be implemented by SALUTE to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organizations - SALUTE		
Category	**Criteria**	**Control**
Common Criteria / Security	CC4.1, CC7.2, CC7.3, CC7.4, CC7.5	Incidents and issues are handled according to entity established policies as part of the incident response process.
	CC4.1, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1	Customer service requests and potential incidents are handled according to entity established policies.

Subservice Organizations - SALUTE		
Category	**Criteria**	**Control**
	CC6.4	Physical access to the data center facilities is restricted to authorized internal and external users.

The following subservice organizations controls should be implemented by CrowdStrike to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organizations - CrowdStrike		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.8, CC7.1	The antivirus software is monitored in real time.

EdgeConneX management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, EdgeConneX performs monitoring of the subservice organizations controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

EdgeConneX's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to EdgeConneX's services to be solely achieved by EdgeConneX control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of EdgeConneX's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to EdgeConneX.
2. User entities are responsible for notifying EdgeConneX of changes made to EdgeOS™ technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of EdgeConneX services by their personnel consistent with the EdgeConneX Acceptable Use Policy.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize EdgeConneX services.
6. User entities are responsible for immediately notifying EdgeConneX of any actual or suspected information security breaches, including compromised user accounts.
7. User entities are responsible for configuring and maintaining their own backup architecture.

8. User entities are responsible for restricting the transmission, movement, and removal of information to authorized internal and external users and processes, and protect it during transmission, movement, or removal.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security and Availability Categories)
Security refers to the protection of: i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of EdgeConneX's description of the system. Any applicable trust services criteria that are not addressed by control activities at EdgeConneX are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of EdgeConneX was limited to the Trust Services Criteria, related criteria and control activities specified by the management of EdgeConneX and did not encompass all aspects of EdgeConneX's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook and information security policies and procedures to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Personnel are provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	Inspected the signed confidentiality statement and employee handbook for a sample of new hires to determine that personnel were provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	No exceptions noted.
		Personnel are required to pass a criminal and financial trust background check before they are hired.	Inspected the completed background checks for a sample of new hires to determine that personnel were required to pass a criminal and financial trust background check before they were hired.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Personnel are required to acknowledge the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices on an annual basis.	Inspected the training acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior.	Inspected the employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and information security policies and procedures to determine that executive management-maintained independence from those that operated the key controls within the environment.	No exceptions noted.
		Executive management meets at least quarterly with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the management meeting minutes for a sample of quarters to determine that executive management met at least quarterly with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment quarterly.	Inspected the internal audit report and management meeting minutes for a sample of quarters to determine that executive management evaluated the skills and competencies of those that operated the internal controls within the environment at least quarterly.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the organizational chart, governance plan, and job description for a sample of roles to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	Inspected the organizational chart and completed risk assessment report to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revised these when necessary to help meet changing commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Reporting relationships and organizational structures are reviewed at least annually by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	Inspected the organizational chart to determine that reporting relationships and organizational structures were reviewed at least annually by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Inspected the job description for a sample of roles to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, governance plan, and the job description for a sample of roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the onboarding procedures and completed onboarding documentation for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Job requirements are documented in the job descriptions and candidates abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.	Inspected the onboarding procedures and job description for a sample of roles to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer evaluation process.	No exceptions noted.
		Management establishes skills and continued training with its commitments and requirements for employees.	Inspected the information security training program and acknowledgements of training for a sample of current and new employees to determine that management established skills and continued training with its commitments and requirements for employees.	No exceptions noted.
		Employees are required to complete security awareness training upon hire and at least annually thereafter.	Inspected the information security training program and acknowledgements of training for a sample of current and new employees to determine that employees were required to complete security awareness training upon hire and at least annually thereafter.	No exceptions noted.
		The entity assesses training needs on a quarterly basis.	Inspected the information security training program and management meeting minutes for a sample of quarters to determine that the entity assessed the training needs on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to pass a criminal and financial trust background check before they are hired.	Inspected the completed background checks for a sample of new hires to determine that personnel were required to pass a criminal and financial trust background check before they were hired.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	Inspected the organizational chart and completed risk assessment report to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revised these when necessary to help meet changing commitments and requirements.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed at least annually by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	Inspected the organizational chart to determine that reporting relationships and organizational structures were reviewed at least annually by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Inspected the job description for a sample of roles to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	Inspected the signed confidentiality statement and employee handbook for a sample of new hires to determine that personnel were provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	No exceptions noted.
		Executive management reviews the responsibilities assigned to operational personnel at least annually and makes updates, if necessary.	Inspected the organizational chart, governance plan, and job description for a sample of roles to determine that executive management reviewed the responsibilities assigned to operational personnel at least annually and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel.	Inspected the organizational and information security policies and procedures and the shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel.	No exceptions noted.
		Procedures manuals are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the network and data flow diagrams and information security policies and procedures to determine that procedures manuals were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Inspected the job description for a sample of roles to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.
		Policy and procedure documents for significant processes are available to required personnel.	Inspected the company policies and procedures to determine that policy and procedure documents for significant processes were available to required personnel.	No exceptions noted.
		A description of the organization structure and organizational roles and responsibilities is posted and available to entity internal users.	Inspected the organizational chart to determine that a description of the organization structure and organizational roles and responsibilities was posted and available to entity internal users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	Inspected the signed confidentiality statement and employee handbook for a sample of new hires to determine that personnel were provided with the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices upon hire.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices on an annual basis.	Inspected the training acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook, organizational code of conduct, and statement of confidentiality and privacy practices on an annual basis.	No exceptions noted.
		Employees are required to complete security awareness training upon hire and at least annually thereafter.	Inspected the information security training program and acknowledgements of training for a sample of current and new employees to determine that employees were required to complete security awareness training upon hire and at least annually thereafter.	No exceptions noted.
		Management establishes skills and continued training with its commitments and requirements for employees.	Inspected the information security training program and acknowledgements of training for a sample of current and new employees to determine that management established skills and continued training with its commitments and requirements for employees.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management meets at least quarterly with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the management meeting minutes for a sample of quarters to determine that executive management met at least quarterly with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel on a quarterly basis.	Inspected the information security objectives and metrics and management meeting minutes for a sample of quarters to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel on a quarterly basis.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	System descriptions are available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description is available to authorized users via the entity's customer-facing website.	Inspected the system and data center description sheets available via the customer-facing website to determine that system descriptions were available to authorized external users that delineated the boundaries of the system and described relevant system components as well as the purpose and design of the system. Documentation of the system description was available to authorized users via the entity's customer-facing website.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the executed service agreement for a sample of third-parties to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the executed service agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the service agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Proposed system changes affecting customers are communicated and confirmed with customers through ongoing communications mechanisms.	Inspected a sample system change communication sent to customers to determine that proposed system changes affecting customers were communicated and confirmed with customers through ongoing communications mechanisms.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets quarterly with operational management to discuss the results of assessments performed by third-parties.	Inspected the management meeting minutes for a sample of quarters to determine that executive management met quarterly with operational management to discuss the results of assessments performed by third-parties.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior.	Inspected the employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics on a quarterly basis.	Inspected the information security objectives and metrics and management meeting minutes for a sample of quarters to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics on a quarterly basis.	No exceptions noted.
		During the risk assessment process, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the completed risk assessment report to determine that during the risk assessment process, management identified changes to business objectives, commitments and requirements, internal operations, and external factors that threatened the achievement of business objectives and updated the potential threats to system objectives.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures and the completed risk assessment report to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the organizational and information security policies and procedures and the shared drive to determine that executive management reviewed policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		During the risk assessment and management process, management personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the completed risk assessment report to determine that during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that had occurred.	No exceptions noted.
		The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations, and standards.	Inspected the entity's completed audit reports to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		During the risk assessment process, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the completed risk assessment report to determine that during the risk assessment process, management identified changes to business objectives, commitments and requirements, internal operations, and external factors that threatened the achievement of business objectives and updated the potential threats to system objectives.	No exceptions noted.
		During the risk assessment and management process, management personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the completed risk assessment report to determine that during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that had occurred.	No exceptions noted.
		Management evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.	Inspected the completed risk assessment report to determine that management evaluated the effectiveness of controls and mitigation strategies in meeting identified risks and recommended changes based on its evaluation.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment report to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment report to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed risk assessment report to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed risk assessment report to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arose from the use of IT.	No exceptions noted.
		During the risk assessment and management process, management personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the completed risk assessment report to determine that during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that had occurred.	No exceptions noted.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and the completed risk assessment report to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and the completed risk assessment report to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing environmental protections. This software sends automated messages to the operations personnel when specific predefined thresholds are met.	Inspected the monitoring software configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing environmental protections, and that the software sent automated messages to the operations personnel when specific predefined thresholds were met.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the organizational and information security policies and procedures and the shared drive to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On a quarterly basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the internal audit report and management meeting minutes for a sample of quarters to determine that on a quarterly basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
		Logical access reviews are performed monthly.	Inspected the completed logical user access review for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Physical access reviews are performed at least quarterly.	Inspected the completed physical user access review for a sample of quarters to determine that physical access reviews were performed quarterly.	No exceptions noted.
		The entity provisions and deprovisions client access client access upon receipt of automated e-mail generated from client request.	Inspected the completed physical user access review, automated access review configuration settings, and example e-mail to determine that the entity provisioned and deprovisioned client access client access upon receipt of automated e-mail generated from client request.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment report to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Executive management assesses the results of the compliance and risk assessments performed on the environment.	Inspected the risk advisory management meeting minutes to determine that executive management assessed the results of the compliance and risk assessments performed on the environment.	No exceptions noted.
		Resolution of security events is reviewed at the weekly operations and security group meetings.	Inquired of the Compliance Manager regarding the resolution of security events to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
			Inspected the operations meeting minutes for a sample of weeks to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the completed risk assessment report to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart, governance plan, and job description for a sample of roles to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the organizational and information security policies and procedures and the shared drive to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the organizational and information security policies and procedures and the shared drive to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and the completed risk assessment report to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Disaster recovery plans are developed and updated at least annually.	Inspected the disaster recovery plan to determine that disaster recovery plans were developed and updated at least annually.	No exceptions noted.
		Disaster recovery plans, including restoration of backups, are tested at least annually.	Inspected the disaster recovery plan and test documentation to determine that disaster recovery plans, including restoration of backups, were tested at least annually.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
			Inspected the EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the organizational and information security policies and procedures and the shared drive to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel.	Inspected the organizational and information security policies and procedures and the shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the security policies and procedures to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment report to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel.	Inspected the organizational and information security policies and procedures and the shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel.	No exceptions noted.
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the organizational chart, governance plan, and job description for a sample of roles to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Inspected the job description for a sample of roles to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.	A master list of the entity's system components is maintained.	Inspected the EdgeConneX asset listing to determine that a master list of the entity's system components was maintained.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security and the access control policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		The EdgeOS™ online application matches each user account to a single customer account number. User access is restricted to their respective data.	Inquired of the Compliance Manager regarding EdgeOS™ application authentication to determine that the EdgeOS™ online application matched each user account to a single customer account number. User access was restricted to their respective data.	No exceptions noted.
			Inspected the EdgeOS™ application authentication settings to determine that the EdgeOS™ online application matched each user account to a single customer account number. User access was restricted to their respective data.	No exceptions noted.
		A role-based security process has been defined with an access control system for EdgeOS™ that is required to use roles when possible.	Inspected the EdgeOS™ user listing with roles to determine that a role-based security process was defined with an access control system for EdgeOS™ that was required to use roles when possible.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Privileged access to sensitive resources is restricted to defined user roles.</td><td>Inquired of the Senior Network Systems Administrator regarding privileged access to determine that privileged access to sensitive resources was restricted to defined user roles.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the EdgeOS™ administrator user listing to determine that privileged access to sensitive resources was restricted to defined user roles.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>EdgeOS™ users are authenticated via authorized user accounts and passwords.</td><td>Inspected the EdgeOS™ application authentication configurations to determine that EdgeOS™ users were authenticated via authorized user accounts and passwords.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The EdgeOS™ application is configured to enforce password standards including minimum password length, history, expiration, and complexity.</td><td>Inspected the EdgeOS™ application password configurations to determine that the EdgeOS™ application was configured to enforce password standards including minimum password length, history, expiration, and complexity.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	User access requests are documented, tracked, and approved by a direct supervisor.	Inspected the supporting user access request ticket for a sample of new hires and the EdgeOS™ listing to determine that user access requests were documented, tracked, and approved by a direct supervisor.	No exceptions noted.
		Terminated employee access to EdgeOS™ is revoked as a component of the termination procedures.	Inquired of the Compliance Manager regarding the process for revoking user access to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
			Observed the logical access revocation procedures to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
			Inspected the completed access termination request for a sample of terminated employees and the EdgeOS™ user listing to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
		Changes in user access are documented, tracked, and approved by a direct supervisor.	Inquired of the Compliance Manager regarding the process for changing user logical or physical access to determine that changes in user access were documented, tracked, and approved by a direct supervisor.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the user access change request tickets for a sample of transferred employees to determine that changes in user access were documented, tracked, and approved by a direct supervisor.	Testing of the control activity disclosed there were no changes in access required during the review period.
		Logical access reviews are performed monthly.	Inspected the completed logical user access review for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Physical access reviews are performed at least quarterly.	Inspected the completed physical user access review for a sample of quarters to determine that physical access reviews were performed quarterly.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The EdgeOS™ online application matches each user account to a single customer account number. User access is restricted to their respective data.	Inquired of the Compliance Manager regarding EdgeOS™ application authentication to determine that the EdgeOS™ online application matched each user account to a single customer account number. User access was restricted to their respective data.	No exceptions noted.
			Inspected the EdgeOS™ application authentication settings to determine that the EdgeOS™ online application matched each user account to a single customer account number. User access was restricted to their respective data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		User access requests are documented, tracked, and approved by a direct supervisor.	Inspected the supporting user access request ticket for a sample of new hires and the EdgeOS™ listing to determine that user access requests were documented, tracked, and approved by a direct supervisor.	No exceptions noted.
		Terminated employee access to EdgeOS™ is revoked as a component of the termination procedures.	Inquired of the Compliance Manager regarding the process for revoking user access to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
			Observed the logical access revocation procedures to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
			Inspected the completed access termination request for a sample of terminated employees and the EdgeOS™ user listing to determine that terminated employee access to EdgeOS™ was revoked as a component of the termination procedures.	No exceptions noted.
		Privileged access to sensitive resources is restricted to defined user roles.	Inquired of the Senior Network Systems Administrator regarding privileged access to determine that privileged access to sensitive resources was restricted to defined user roles.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the EdgeOS™ administrator user listing to determine that privileged access to sensitive resources was restricted to defined user roles.	No exceptions noted.
		A role-based security process has been defined with an access control system for EdgeOS™ that is required to use roles when possible.	Inspected the EdgeOS™ user listing with roles to determine that a role-based security process was defined with an access control system for EdgeOS™ that was required to use roles when possible.	No exceptions noted.
		Logical access reviews are performed monthly.	Inspected the completed logical user access review for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Physical access reviews are performed at least quarterly.	Inspected the completed physical user access review for a sample of quarters to determine that physical access reviews were performed quarterly.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Documented physical security policies and procedures are in place to guide personnel in physical security practices.	Inspected the physical and environmental security policy and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security practices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A PIN based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	Observed the physical access procedures to the data center facilities to determine that a PIN based physical access control system was implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	No exceptions noted.
			Inspected the physical and environmental security policy and procedures and the PIN access listing to determine that a PIN based physical access control system was implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	No exceptions noted.
		At EdgeConneX managed facilities, a mantrap is utilized to restrict access to the facilities and prevent tailgating.	Inquired of the Compliance Manager regarding mantraps to determine that at EdgeConneX managed facilities, a mantrap was utilized to restrict access to the facilities and prevent tailgating.	No exceptions noted.
			Observed the physical access procedures to the data center facilities to determine that at EdgeConneX managed facilities, a mantrap was utilized to restrict access to the facilities and prevent tailgating.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Contractors and other third-parties are issued expiring PINs based on access request submissions.	Inquired of the Compliance Manager regarding contractor and third-party access to determine that contractors and other third-parties were issued expiring PINs based on access request submissions.	No exceptions noted.
			Inspected the supporting access request ticket for a sample of contractor and third-party access requests to determine that contractors and other third-parties were issued expiring PINs based on access request submissions.	No exceptions noted.
		Visitors are required to be escorted by an employee when visiting the data center facilities.	Inquired of the Compliance Manager regarding visitor access to determine that visitors were required to be escorted by an employee when visiting the data center facilities.	No exceptions noted.
			Observed the data center facility access procedures to determine that visitors were required to be escorted by an employee when visiting the data center facilities.	No exceptions noted.
		Visitors are required to sign in through a log when visiting the data center facilities.	Inquired of the Compliance Manager regarding visitor logs to determine that visitors were required to sign in through a log when visiting the data center facilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Observed the data center facility access procedures to determine that visitors were required to sign in through a log when visiting the data center facilities.	No exceptions noted.
			Inspected the visitor log to determine that visitors were required to sign in through a log when visiting the data center facilities.	No exceptions noted.
		Surveillance cameras are installed at the data center facilities and monitored by NOC personnel.	Inquired of the Compliance Manager regarding surveillance cameras to determine that surveillance cameras were installed at the data center facilities and monitored by NOC personnel.	No exceptions noted.
			Observed the video surveillance cameras at the data center facilities to determine that surveillance cameras were installed at the data center facilities and monitored by NOC personnel.	No exceptions noted.
		Video surveillance footage of the EdgeConneX managed data center facilities is stored and retained.	Inquired of the Compliance Manager regarding video surveillance to determine that video surveillance footage of the EdgeConneX managed data center facilities was stored and retained.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the physical and environmental security policy and procedures to determine that video surveillance footage of the EdgeConneX managed data center facilities was stored and retained.	No exceptions noted.
			Inspected the video surveillance system configurations and footage to determine that video surveillance footage of the EdgeConneX managed data center facilities was stored and retained.	No exceptions noted.
		User access requests are documented, tracked, and approved by a direct supervisor.	Inspected the supporting user access request ticket for a sample of new hires and the EdgeOS™ listing to determine that user access requests were documented, tracked, and approved by a direct supervisor.	No exceptions noted.
		Physical access of terminated employees is revoked as a component of the termination procedures.	Inquired of the Compliance Manager regarding access revocation to determine that physical access of terminated employees was revoked as a component of the termination procedures.	No exceptions noted.
			Inspected the Access Control Standard to determine that physical access of terminated employees was revoked as a component of the termination procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed PIN access revocation for a sample of terminated employees and the PIN access listing to determine that physical access of terminated employees was revoked as a component of the termination procedures.	Testing of the control activity disclosed that no employees with PIN access were terminated during the review period.
		Logical access reviews are performed monthly.	Inspected the completed logical user access review for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Physical access reviews are performed at least quarterly.	Inspected the completed physical user access review for a sample of quarters to determine that physical access reviews were performed quarterly.	No exceptions noted.
		The entity provisions and deprovisions client access client access upon receipt of automated e-mail generated from client request.	Inspected the completed physical user access review, automated access review configuration settings, and example e-mail to determine that the entity provisioned and deprovisioned client access client access upon receipt of automated e-mail generated from client request.	No exceptions noted.
		Doors that bypass mantraps can only be opened by the PINs of designated personnel.	Inquired of the Compliance Manager regarding mantraps to determine that doors that bypass mantraps could only be opened by the PINs of designated personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed the data center facility access procedures to determine that doors that bypass mantraps could only be opened by the PINs of designated personnel.	No exceptions noted.
			Inspected the PIN user access listing to determine that doors that doors that bypass mantraps could only be opened by the PINs of designated personnel.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the document and records retention policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Compliance Manager regarding data destruction and disposal to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the document and records retention policies and procedures to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected a sample of certificates of destruction to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Users can only access EdgeOS™ remotely through transit layer security (TLS) encryption.	Inspected the EdgeOS™ encryption configurations to determine that users could only access EdgeOS™ remotely through TLS encryption.	No exceptions noted.
		External access to EdgeOS™ is restricted through the use of user authentication and message encryption systems such as TLS.	Inspected the EdgeOS™ authentication and encryption configurations to determine that external access to EdgeOS™ was restricted through the use of user authentication and message encryption systems such as TLS.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.	Not applicable - EdgeConneX’s services do not include the transmission, movement, or removal of information.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The ability to install software on workstations and laptops is restricted to IT support personnel.	Inquired of the Senior Network Systems Administrator regarding workstation software to determine that the ability to install software on workstations and laptops was restricted to IT support personnel.	No exceptions noted.
			Inspected the denial notification received when an employee attempted to download an application or software to determine that the ability to install software on workstations and laptops was restricted to IT support personnel.	No exceptions noted.
		Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the antivirus software dashboard to determine that antivirus software was installed on workstations, laptops, and servers supporting such software.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the security policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Logging and monitoring software are used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests.	Inspected the monitoring software configurations and an example alert to determine that logging and monitoring software were used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests.	No exceptions noted.
		The ability to install software on workstations and laptops is restricted to IT support personnel.	Inquired of the Senior Network Systems Administrator regarding workstation software to determine that the ability to install software on workstations and laptops was restricted to IT support personnel.	No exceptions noted.
			Inspected the listing of users with the ability to install software on workstations to determine that the ability to install software on workstations and laptops was restricted to IT support personnel.	No exceptions noted.
		Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the antivirus software dashboard to determine that antivirus software was installed on workstations, laptops, and servers supporting such software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
		Resolution of security events is reviewed at the weekly operations and security group meetings.	Inquired of the Compliance Manager regarding the resolution of security events to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the operations meeting minutes for a sample of weeks to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Resolution of security events is reviewed at the weekly operations and security group meetings.	Inquired of the Compliance Manager regarding the resolution of security events to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
			Inspected the operations meeting minutes for a sample of weeks to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	Inspected the incident response policies and procedures to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Operations personnel follow defined protocols for evaluating reported events.	Inspected the incident response policies and procedures to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that operations personnel followed defined protocols for evaluating reported events.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Resolution of security events is reviewed at the weekly operations and security group meetings.	Inquired of the Compliance Manager regarding the resolution of security events to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
			Inspected the operations meeting minutes for a sample of weeks to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	Inspected the incident response policies and procedures to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Resolution of security events is reviewed at the weekly operations and security group meetings.	Inquired of the Compliance Manager regarding the resolution of security events to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.
			Inspected the operations meeting minutes for a sample of weeks to determine that resolution of security events was reviewed at the weekly operations and security group meetings.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	Inspected the incident response policies and procedures to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that internal and external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting EdgeOS™ ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Disaster recovery plans are developed and updated at least annually.	Inspected the disaster recovery plan to determine that disaster recovery plans were developed and updated at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Disaster recovery plans, including restoration of backups, are tested at least annually.	Inspected the disaster recovery plan and test documentation to determine that disaster recovery plans, including restoration of backups, were tested at least annually.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Proposed system changes affecting customers are communicated and confirmed with customers through ongoing communications mechanisms.	Inspected a sample system change communication sent to customers to determine that proposed system changes affecting customers were communicated and confirmed with customers through ongoing communications mechanisms.	No exceptions noted.
		Customer service requests are evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.	Inspected the ticket for a sample of customer service requests to determine that customer service requests were evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.	No exceptions noted.
		Customer service requests are reviewed and approved prior to work commencing on the requested change.	Inspected the ticket for a sample of customer service requests to determine that customer service requests were reviewed and approved prior to work commencing on the requested change.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		During the risk assessment process, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the completed risk assessment report to determine that during the risk assessment process, management identified changes to business objectives, commitments and requirements, internal operations, and external factors that threatened the achievement of business objectives and updated the potential threats to system objectives.	No exceptions noted.
		During the risk assessment and management process, management personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the completed risk assessment report to determine that during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that had occurred.	No exceptions noted.
		Management evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.	Inspected the completed risk assessment report to determine that management evaluated the effectiveness of controls and mitigation strategies in meeting identified risks and recommended changes based on its evaluation.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Risk Mitigation</th></tr>
<tr><th>CC9.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.</td><td>Inspected the certificate of liability insurance to determine that the entity had purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.</td><td>No exceptions noted.</td></tr>
<tr><td>CC9.2</td><td>The entity assesses and manages risks associated with vendors and business partners.</td><td>Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.</td><td>Inspected the third-party and vendor policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</td><td>Inspected the completed risk assessment report and evaluation form for a sample of critical vendors to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.</td><td>Inspected the completed risk assessment report and evaluation form for a sample of critical vendors to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the executed service agreement for a sample of third-parties to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the executed service agreement for a sample of third-parties to determine that the entity’s third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	Inspected the third-party and vendor policies and procedures to determine that management assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the third-party and vendor policies and procedures to determine that the entity had documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the third-party and vendor policies and procedures to determine that the entity had documented procedures for terminating third-party relationships.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	EdgeOS™ is configured to monitor utilization and power usage on an ongoing basis.	Inquired of the Compliance Manager regarding utilization and power monitoring to determine that EdgeOS™ was configured to monitor utilization and power usage on an ongoing basis.	No exceptions noted.
			Observed the EdgeOS™ monitoring configurations and an example alert to determine that EdgeOS™ was configured to monitor utilization and power usage on an ongoing basis.	No exceptions noted.
		Critical infrastructure components are reviewed for criticality classification and assignment of a minimum level of redundancy.	Inquired of the Compliance Manager regarding critical infrastructure components to determine that critical infrastructure components were reviewed for criticality classification and assignment of a minimum level of redundancy.	No exceptions noted.
			Observed the data center facilities' redundant infrastructure to determine that critical infrastructure components were reviewed for criticality classification and assignment of a minimum level of redundancy.	No exceptions noted.
			Inspected the hardware maintenance policies and procedures to determine that critical infrastructure components were reviewed for criticality classification and assignment of a minimum level of redundancy.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Future demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by senior management.	Inquired of the Compliance Manager regarding forecasting and capacity planning to determine that future demand was forecasted and compared to scheduled capacity on an ongoing basis, and that forecasts were reviewed and approved by senior management.	No exceptions noted.
			Inspected the processing demand forecasting report to determine that future demand was forecasted and compared to scheduled capacity on an ongoing basis, and that forecasts were reviewed and approved by senior management.	No exceptions noted.
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental protections are installed at the data center facilities that include the following: • Heating, ventilation, and air conditioning (HVAC) • Battery and generator backup in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Dry pipe sprinklers	Inquired of the Compliance Manager regarding environmental protections at the data centers to determine that environmental protections were installed at the data center facilities that included the following: • HVAC • Battery and generator backup in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Dry pipe sprinklers	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed the data centers' environmental protection equipment to determine that environmental protections were installed at the data center facilities that included the following: • HVAC • Battery and generator backup in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Dry pipe sprinklers	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing environmental protections. This software sends automated messages to the operations personnel when specific predefined thresholds are met.	Inspected the monitoring software configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing environmental protections, and that the software sent automated messages to the operations personnel when specific predefined thresholds were met.	No exceptions noted.
		Environmental protections receive maintenance on at least an annual basis.	Inquired of the Compliance Manager regarding preventative environmental maintenance to determine that environmental protections received maintenance on at least an annual basis.	No exceptions noted.
			Inspected the HVAC/CRAC maintenance reports to determine that environmental protections received maintenance on at least an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the UPS maintenance reports to determine that environmental protections received maintenance on at least an annual basis.	No exceptions noted.
			Inspected the generator maintenance reports to determine that environmental protections received maintenance on at least an annual basis.	No exceptions noted.
			Inspected the fire suppression systems maintenance reports to determine that environmental protections received maintenance on at least an annual basis.	No exceptions noted.
		Disaster recovery plans are tested at least annually.	Inspected the disaster recovery plan and test documentation to determine that disaster recovery plans, including restoration of backups, were tested at least annually.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the Compliance Manager regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the backup data encryption configurations to determine that backup media was stored in an encrypted format.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		EdgeConneX uses a multi-location strategy for its facilities to permit the resumption of operations in the event of a disaster at a specific data center facility.	Inspected the disaster recovery plan and test documentation to determine that EdgeConneX used a multi-location strategy for its facilities to permit the resumption of operations in the event of a disaster at a specific data center facility.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Disaster recovery plans, including restoration of backups, are tested at least annually.	Inspected the disaster recovery plan and test documentation to determine that disaster recovery plans, including restoration of backups, were tested at least annually.	No exceptions noted.
		Test results are reviewed, and the disaster recovery plan is adjusted by management as needed.	Inquired of the Compliance Manager regarding disaster recovery to determine that test results were reviewed, and the disaster recovery plan was adjusted by management as needed.	No exceptions noted.
			Inspected the disaster recovery plan and test documentation to determine that test results were reviewed, and the disaster recovery plan was adjusted by management as needed.	No exceptions noted.