LightEdge Solutions, LLC

SOC 2 Report

For

Colocation, Managed, and Hosted Services

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security and Availability

August 1, 2021, to July 31, 2022

Prepared in Accordance with the
AICPA SSAE No. 18 and IAASB ISAE 3000 Standards

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of LightEdge Solutions, LLC, user entities of LightEdge Solutions, LLC's services, and other parties who have sufficient knowledge and understanding of LightEdge Solutions, LLC's services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor’s Report

To LightEdge Solutions, LLC:

Scope

We have examined LightEdge Solutions, LLC’s (“LightEdge” or the “service organization”) accompanying description of its colocation, managed, and hosted services system, in Section 3, throughout the period August 1, 2021, to July 31, 2022, (the “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 August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge’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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LightEdge, to achieve LightEdge’s service commitments and system requirements based on the applicable trust services criteria. The description presents LightEdge’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LightEdge’s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, “Other Information Provided by LightEdge is presented by LightEdge management to provide additional information and is not a part of the description. Information about LightEdge management’s responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve LightEdge’s service commitments and system requirements based on the applicable trust services criteria.

Service Organization’s Responsibilities

LightEdge 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 LightEdge’s service commitments and system requirements were achieved. LightEdge has provided the accompanying assertion, in Section 2, (“assertion”) about the description and the suitability of design and operating effectiveness of controls stated therein. LightEdge 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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; and
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

a. the description presents LightEdge's colocation, managed, and hosted services system that was designed and implemented throughout the period August 1, 2021, to July 31, 2022, in accordance with the description criteria;
b. the controls stated in the description were suitably designed throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge'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 applied the complementary controls assumed in the design of LightEdge's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of LightEdge'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 LightEdge, user entities of LightEdge's colocation, managed, and hosted services system during some or all of the period of August 1, 2021, to July 31, 2022, business partners of LightEdge subject to risks arising from interactions with the colocation, managed, and hosted 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 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; and
- 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.

Schellman & Company, LLC

Tampa, Florida
August 29, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of LightEdge's colocation, managed, and hosted services system, in Section 3, throughout the period August 1, 2021, to July 31, 2022, (the "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, managed, and hosted services system that may be useful when assessing the risks arising from interactions with LightEdge's system, particularly information about system controls that LightEdge 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LightEdge, to achieve LightEdge's service commitments and system requirements based on the applicable trust services criteria. The description presents LightEdge's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LightEdge's controls. The description does not disclose the actual controls at the subservice organization.

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

a. the description presents LightEdge's colocation, managed, and hosted services system that was designed and implemented throughout the period August 1, 2021, to July 31, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge'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 organizations applied the complementary controls assumed in the design of LightEdge's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of LightEdge's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Founded in 1996, and headquartered in Des Moines, Iowa, LightEdge Solutions, LLC (“LightEdge” or the “Company”) provides an alternative for businesses that traditionally have purchased, maintained, and then depreciated equipment related to IT functions. By leveraging the economies of scale and LightEdge’s networking, cloud, colocation, and security expertise, customers are able to operate their applications and data on redundant IT platforms.

Description of Services Provided

LightEdge provides technology infrastructure for companies that require elevated levels of security and availability. LightEdge operates multiple enterprise-class data centers where they deploy hybrid solutions built on dedicated private cloud, managed hosting, and colocation services. LightEdge specializes in working with companies facing the most stringent regulatory requirements to help ensure compliance with industry standards.

LightEdge keeps security and end-to-end customer care at the forefront of the services provided through the implementation of its service offerings and a 24x7x365 monitored Network Operations Center (NOC).

LightEdge offers a variety of IT services to its customers, which are further defined below:

Data Center Solutions

Colocation solutions in facilities specifically designed to meet customer requirements for computing and storage. Data center services can be customized for individual customer needs including:

- Rack Colocation
- Cage Space
- Private Suites
- Shared Colocation

Cloud Services

Hosted infrastructure solutions with scalable virtual, dedicated or hybrid solutions for servers, storage, and applications.

- Virtual Private Cloud
- Dedicated Private Cloud
- Bare Metal Cloud
- Power Cloud

Data Protection & Business Continuity Solutions

Backup and replication solutions customized for customer environments to ensure applications and data are protected.

- Managed Backup & Recovery
- Managed Data Protection
- Managed Disaster Recovery
- Workplace Recovery

Security Services

Enterprise-grade data center security solutions for mission-critical applications hosting sensitive data, including:

- Access Controls
- Private Network
- Load Balancing & Web Application Firewalling
- Next Generation Firewalling
- Security Information & Event Management (SIEM)
- Intrusion Detection & Prevention
- 24x7x365 Security Operations Center
- Vulnerability Management
- Data Encryption

Principal Service Commitments and System Requirements

LightEdge designs its processes and procedures to meet its objectives for its colocation, managed, and hosted services. Those objectives are based on the service commitments that LightEdge makes to user entities, the laws and regulations and compliance requirements that LightEdge has established for the services.

LightEdge's commitments to their customers related to security and availability are documented and communicated in service level agreements (SLAs), master services agreements (MSAs) and other customer agreements, as well as in the description of the service offering provided online. LightEdge's commitments include the following:

- Maintain administrative, technical, and physical safeguards against the destruction, loss, or alteration of confidential information, and implement security measures to protect confidential information.
- Proactively monitor managed services in accordance with the applicable SLA(s).
- Implement change management processes and procedures to maintain health and availability of systems, and to release hot fixes and service packs.
- Maintain technical and security safeguards including encryption of sensitive data.
- Make the hosted services available to customers at a service level of at least 99.99% during predefined applicable measurable periods.
- Make operations and support available to customers on a 24 hour per day, seven days per week, 365 days per year, basis.
- Monitoring of service availability and notify customers within fifteen minutes of service outages via e-mail.

LightEdge has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- Information security policies are in place to guide LightEdge personnel in the safeguarding of system infrastructure, information assets, and data. Access procedures are in place to govern the acceptable use of information systems and enforce the provisioning and decommissioning of user access, use of unique user credentials, minimum password requirements, and the performance of periodic user access reviews.
- Service guides are in place to guide personnel in the management and monitoring of managed services provided by LightEdge.
- Change management policies and procedures are in place to guide LightEdge personnel in the change management activities including deployment, modification, and removal of configurations within LightEdge

managed services. Change management policies and procedures are documented that outline the recording, reviewing, and implementation of system changes as well as the roles and responsibilities for individuals involved in the change management process.

- Encryption policies and requirements are in place to ensure data in transit and at rest are encrypted using defined minimum encryption standards and protocols.
- Availability monitoring applications are in place to monitor the performance and availability of production sites and alert operations personnel when predefined thresholds are exceeded.
- Key performance indicator (KPI) reports are generated and reviewed on a monthly basis to review compliance with service commitments and review system incidents, responses, and resolution activities.
- Operations personnel are staffed 24 hours per day, seven days per week to monitor production sites and environments.
- Business continuity plans are in place and tested on at least an annual basis.

Components of the System Used to Provide the Service

System Boundaries

The scope of the examination included LightEdge's colocation, managed, and hosted services system at the following data center facilities:

Data Center	Facility Address
Altoona 1	1435 Northridge Circle, Altoona, Iowa 50009
Altoona 2	1401 Northridge Circle, Altoona, Iowa 50009
Austin 1	2916 Montopolis Drive, Suite 300, Austin, Texas 78741
Austin 2	7000-B Burleson Road, Suite 400, Austin, Texas 78744
Kansas City	9050 NE Underground Drive, Pillar 312, Kansas City, Missouri 64161
Omaha	1148 American Parkway, Papillion, Nebraska, 68046
Raleigh	8020 Arco Corporate Drive, Suite 310, Raleigh, North Carolina, 27617
Lenexa	17501 W 98th Street, Lenexa, Kansas 66219
San Diego 1	9305 Lightwave Avenue, San Diego, California 92123
San Diego 2	9725 Scranton Road, San Diego, California 92121
Phoenix 1	120 East Van Buren, Phoenix, Arizona 85004

The aforementioned facilities are supported by personnel located at the Des Moines, Iowa, corporate office facility and on-site staff at each data center facility.

Requests for services are initiated and authorized by user entities by directly contacting customer support personnel at LightEdge. Customer requests are recorded and tracked within an internal ticketing system and are monitored from request initiation to resolution.

The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established SLAs.

Infrastructure

The infrastructure and software supporting the colocation, managed, and hosted services is maintained in the facilities noted in the "System Boundaries" section of the report. The data centers are equipped with physical security safeguards, redundant power supply, and fire detection and suppression controls.

The in-scope infrastructure consists of multiple applications, operating system platforms, servers, and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Active Directory Domain Controller*	Network domain supporting the colocation, managed, and hosted services, and related systems.	Microsoft Windows	Altoona 1 Altoona 2 Austin 1 Austin 2 Raleigh Kansas City San Diego 1
Application, Web, and Database Servers	Production server operating systems supporting the colocation, managed, and hosted services, and related systems.	Microsoft Windows and UNIX servers** with SQL Server database	All locations
Virtual Servers	Virtual machines containing virtualized instances connected via hypervisors providing high-availability and fail tolerance.	VMware vSphere	
Hypervisor	Software allowing multiple virtual instances to share resources of a single hardware host.	VMware ESXi	
Firewall Systems	Firewall systems to filter unauthorized inbound network traffic from the Internet.	Fortinet FortiGate Sophos	
Virtual Private Network (VPN)	Encrypted VPNs requiring multi-factor authentication for remote access to the production environment.		
Customer Portals	Web portals providing customers the ability to monitor their managed infrastructure, hosting services, and requested changes.	N/A	Altoona 1 San Diego 1
Password Management Solution	Third-party password manager used to control passwords granting LightEdge administrative access to production systems.	Passwordstate Bitwarden	Altoona 1 Altoona 2 San Diego 1
The Automated System (TAS)	Internal developed configuration management tool and ticketing system utilized for requesting, tracking, and monitoring of changes and incidents.	TAS	Phoenix 1 San Diego 1 San Diego 2
Badge Access System	Commercial electronic access system used to restrict physical access to the corporate office facility and data center facilities.	N/A	All locations
Backup Systems	Commercial backup systems used for disk-to-disk backups of production data and systems.		

* *LightEdge utilizes Microsoft Active Directory (AD) domains for centralized security for the Windows and UNIX servers deemed "critical." Due to networking constraints, integration with AD is not possible or logical for all servers. Local security accounts are established and monitored for employee use on servers not integrated with an AD domain.*

***The UNIX operating systems (hereafter referred to as "UNIX servers") include Debian, SUSE, Redhat, Solaris, and FreeBSD, among others.*

Critical Systems

In the interest of maintaining security of LightEdge customer data and access to customer network infrastructure, there are certain elements that classify a server as a "critical system."

At least one of the following must be true for LightEdge to define / classify a server as a critical system:

- The server contains sensitive information concerning a user entity's network or server configurations.
- The server contains sensitive password information that can be used to access a user entity's network or server infrastructure.
- The server has network access into a user entity's network.
- The server contains a user entity's data.
- The server relays communications concerning the user entity's systems and/or networks, including configuration information and passwords.
- The server provides employee and/or user entity authentication services and that authentication must provide access to at least one of the systems listed above.

People

The following functional areas support the colocation, managed, and hosted services system:

- Executive Management – oversees company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- NOC – provides Tier 1 support for standard customers.
- Tier 2 Support – handles trouble tickets for customers across product platforms.
- IT Operations – responsible for protecting information and systems from unauthorized access and use while maintaining integrity and availability, maintaining the task of producing goods and services for user entities in an efficient manner via use of staff, resources, facilities, and business solutions.
- Operational Engineering – provides Tier 3 support and maintenance of service platforms, single instance installations for non-complex customers, and occasionally called upon to assist with highly integrated installs and support.
- Product Engineering – creates and deploys new products and provides installation and support services as needed.
- Facilities – maintains and monitors data center equipment and infrastructure.
- Human Resources (HR) – establishes policies, standards, and processes for recruitment, onboarding, employee orientation and training, and off-boarding activities.

Procedures

Access Authentication and Authorization

Documented information security policies are in place to govern acceptable use of information systems and to guide personnel in safeguarding systems infrastructure, information assets, and data. Information sensitivity classifications and employee guidelines are established for the handling and labeling of information based on sensitivity, value, and criticality.

Network domain users are authenticated via a user account and password before being granted network access. System-enforced password parameters are configured and include minimum password length requirements, expiration intervals (maximum password age), complexity requirements, minimum password history remembered, and invalid password account lockout thresholds. Access to in-scope systems is managed by a centralized lightweight directory access protocol (LDAP) allowing users to authenticate with their network domain user account and password. Predefined security groups are also utilized to assign access within the network domain and access related events such as account logon, account logout, and privileged use are logged. Administrative access to the network domain is restricted to user accounts accessible by authorized LightEdge personnel.

A password management solution is utilized by engineering and system support personnel to manage passwords used to access customer infrastructure and restrict access to passwords to authorized personnel based on business responsibilities. Passwords stored within the password management solution are encrypted, and system access is disabled as a component of the employee termination process.

The myLightEdge portal is a web-based application that provides customers the ability to monitor their managed infrastructure and hosting services, request changes in services, and monitor the status of requested changes. myLightEdge users are authenticated via user account and password before being granted access. Passwords are configured to enforce password minimum length and complexity requirements. The ability to administer access privileges to myLightEdge for LightEdge employees and initial client setup is restricted to user accounts accessible by authorized personnel via predefined security groups. Additionally, client access within myLightEdge is configured to restrict customer users from accessing other customers' data. The myLightEdge portal utilizes TLS v1.2 encryption for web communication sessions.

Access Requests and Access Revocation

Dedicated engineering and operations teams are responsible for provisioning logical access to managed infrastructure and hosting services. The ability to access customer environments is restricted to authorized personnel. Employee and contractor user access requests are documented on a standard access request form and require the approval of a manager. Privileged user access reviews are performed on a quarterly basis to help ensure that access to data is restricted and authorized. When an employee ends their employment, a termination checklist is completed to document the off-boarding procedures performed and production system access is revoked. System owners disable user accounts assigned to terminated employees as a component of the employee termination process.

Change Management

Documented maintenance and change management policies and procedures are in place to guide personnel in change management activities affecting existing customer infrastructure. The policies apply to the deployment, modification, and removal of configuration items utilized in the delivery of a LightEdge managed service.

Client support requests must be submitted and approved by an authorized client administrator before project activities are initiated. Once verified, support requests are documented and tracked within the centralized ticketing system. In the event a client support request requires a change to customer infrastructure, operations personnel document and track the change request via a change request form that includes information such as the description of the change, change priority, development and testing plans, risk, and impact analysis, and change status.

A Change Review Board (CRB) is established to function as a governing body to oversee change management activities. In accordance with documented policies, changes can be classified as either standard, minor, or normal.

Risk and impact values are used to classify changes based on the following matrix:

Risk	Impact		
	Low	**Medium**	**High**
Very Low	Standard	Standard	Standard
Low	Standard	Minor	Normal
Medium	Minor	Normal	Normal
High	Minor	Normal	Normal

Changes classified as normal are required to pass a peer review and receive CRB approval during the weekly CRB meeting. CRB approval is documented within the change ticket. Changes classified as minor are required to pass a peer review, and standard changes are immediately set to approved due to the low risk and impact to services. Emergency changes are changes which must be expedited to correct an incident or problem impacting the production environment. In the event of an emergency change request, the CRB is notified of the change via e-mail, and the review and approval process are expedited (i.e., performed outside of the weekly meeting). Approval for emergencies may be given verbally or through e-mail, but the details of the approval are required to be documented within the change ticket prior to ticket closure.

LightEdge has implemented a process to communicate changes to customers that impact customer environments prior to implementation. Changes that impact customer environments are indicated within the change ticket. Client impacting changes classified as "normal" are required to be communicated to customers and implemented in accordance with the corresponding SLA. Client impacting changes classified as "minor" or "standard" are communicated and implemented after business hours or scheduled in coordination with clients. "Minor" or "standard" changes that are not client impacting can be implemented at any time. The ability to implement changes to existing customer infrastructure has been restricted to user accounts accessible by authorized personnel.

Physical Security

Documented policies and procedures are in place to address provisioning, controlling, and monitoring of physical access into the data centers and office facilities. The corporate office facility, located in Des Moines, Iowa, requires visitors to check in at the lobby prior to being granted escorted access to the back-office area. When accessing the data centers, visitors and vendors are required to provide their government issued form of photo identification and check-in to a digital visitor log. Visitors are required to wear a visitor badge and be escorted by LightEdge personnel and/or an authorized customer contact while on-site at one of the data center facilities. An electronic badge access system controls access to and within the data centers and requires multi-factor authentication via biometric scanners and/or personal identification number (PIN) keypads. Badge access into the data centers is restricted to authorized data center personnel and access attempts are logged and traceable to individual cardholders. Additional access procedures are in place, including a mantrap, at the Austin 2, Lenexa, Phoenix 1, Raleigh, San Diego 1, and San Diego 2 data center facilities. The Altoona 1, Altoona 2, Kansas City, and Omaha data centers were noted be equipped with mantraps and tailgating sensors.

An inventory listing of issued physical keys is maintained at each data center facility to ensure LightEdge personnel are aware of the number of physical keys that have been issued. The key inventory includes the quantity of keys issued and a key description (i.e., what the key unlocks). Physical keys are stored in locked cabinets located in a secured room accessible by authorized data center personnel. Key issuance logs are in place at the in-scope data center facilities to track the issuance and return of physical keys to the data centers. The production areas of the data centers are maintained within the building's interior and there are no exterior windows within the production areas of the data centers. Surveillance cameras are located throughout the data centers and a digital video recorder (DVR) system monitors and records activity. Backups of the DVR surveillance recordings are retained for a minimum of 90 days.

The badge access system requires administrative users to authenticate via a user account and password. The ability to create, modify, and delete user access privileges within the badge and biometric system is restricted to administrator accounts accessible by authorized data center personnel. Data center personnel require management approval prior to issuing or modifying badge access privileges. LightEdge badge access privileges are revoked as a component of the employee termination process; to help ensure access privileges are restricted to authorized personnel, the Compliance and Security Team review badge access privileges on a quarterly basis. Client data center access listings are also maintained to identify approved client administrative contacts and data center users. Administrative personnel require approval from an authorized client administrator (noted on the data center access listings) prior to issuing, modifying, or revoking badge access privileges to the client's access. On an annual basis, a notification is sent to the authorized client administrators to validate badge access privileges assigned to individuals within, or authorized by, the client organization.

Environmental Security

LightEdge's colocation, managed, and hosted services are supported by the corporate office facility in Des Moines, Iowa, and the in-scope data centers. Standard operating procedures are in place to govern environmental security practices at each of the facilities. The corporate office facility is equipped with fire detection and suppression systems, including audible and visual fire alarms, smoke detectors, fire extinguishers, and a sprinkler system. The fire extinguisher and sprinkler system within the corporate office facility are owned and managed by the building management company. The building management company is responsible for ensuring the fire detection and suppression systems are inspected and maintained on an annual basis.

The data centers are protected by fire detection systems, audible and visual fire alarms, fire extinguishers, and either dry-pipe water sprinklers or gaseous / chemical fire suppression systems.

LightEdge utilizes third-party security specialists to provide 24x7 monitoring of the fire detection and suppression systems at each in-scope data center. LightEdge management obtains inspection reports from third-party specialists as evidence that the fire extinguishers, fire suppression systems, and alarm systems at each of the data centers undergo maintenance inspections on an annual basis.

Each data center is equipped with dedicated air conditioning units that are configured to notify data center personnel in the event that predefined temperature and humidity levels are exceeded. Additionally, production servers at each data center are mounted on racks within the data centers to facilitate cooling and protect servers from localized flooding. LightEdge management obtains inspection reports from third-party specialists as evidence that the air conditioning units undergo maintenance inspections for the Altoona 1, Altoona 2, Kansas City, Omaha, Austin 1, Austin 2, Raleigh, and Lenexa data centers on a quarterly basis. At the San Diego 1 and San Diego 2 data centers, internal personnel perform full preventative maintenance on an annual basis and routine maintenance on a quarterly basis.

Production equipment within the data centers is connected to uninterruptible power supply (UPS) systems that are configured to provide temporary electricity in the event of a power outage. Additionally, the data centers are connected to dedicated power generators that provide electricity during long-term power outages. LightEdge management obtains inspection reports from third-party specialists as evidence that the UPS systems and generators undergo maintenance inspections according to a predefined maintenance schedule (semi-annual inspections for the UPS systems and annual inspections for the generators). In addition to the third-party inspections, the generators are load tested on at least an annual basis.

Data Backup and Disaster Recovery

LightEdge utilizes the Avamar and Veeam backup systems to perform disk-to-disk backups of production data and systems. IBM PowerCloud and Acronis backup software is also used for managed backups of customer environments and virtual machines. These systems are configured to perform backups of client production environments and log the status of backup jobs at least weekly, or more frequently if specified within customer approved backup schedules. Changes to the backup schedule are initiated by the customer and completed by backup personnel. The automated backup systems are configured to notify operations personnel via e-mail of backup job success and failures. A consolidated alert report is sent to operations personnel for review on a daily basis to identify potential issues with the backup systems. In addition, backup data are replicated between geographically separate data centers at a frequency determined by the customer.

Additionally, business continuity plans are in place for each business unit to guide personnel in procedures to protect against disruptions caused by an unexpected event. These plans are evaluated and tested on an annual basis.

Incident Response

Documented incident response and support procedures are in place to guide operations personnel in the monitoring, documenting, escalating, and resolving of problems affecting managed hosting and network services. These procedures include procedures regarding severity level definitions, escalation, ticket handling, and response time requirements for service alerts. Operations personnel utilize a centralized ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services. Additionally, KPI reports are generated by the online operational metrics reporting dashboard and reviewed by management during the monthly management meetings to evaluate system incident, response, and resolution activities.

System Monitoring

LightEdge personnel utilize standard and preconfigured build procedures during the installation and deployment of production servers to help ensure systems are consistently configured and hardened. As part of system builds, antivirus software is installed on in-scope production servers and workstations. The antivirus software is configured to scan registered clients on a daily basis and scan files upon access or modification. Antivirus definitions are updated automatically as they are released.

An enterprise monitoring system is in place to monitor the performance and availability of production sites, servers, and devices. To help ensure availability, operations personnel monitor client environments 24x7 and the monitoring system is configured to alert operations personnel via e-mail and onscreen notifications when predefined thresholds (e.g., bandwidth, central processing unit (CPU) utilization, and disk space) are exceeded. Operations personnel utilize a centralized ticketing system to document, prioritize, escalate, and resolve problems affecting the availability of contracted services. These problems and outages are categorized by operations personnel with predefined severity levels.

A firewall system is in place to filter unauthorized inbound network traffic from the internet and deny any type of network connection that is not explicitly authorized by LightEdge. An intrusion prevention system (IPS) is utilized to analyze and report network events and block suspected or actual network security breaches.

Data

Physical Security

The badge access system provides reports to LightEdge management personnel regarding active and inactive badge holders, access permissions assigned, and activity logs used to record access attempts (successful and unsuccessful).

Environmental Security

Environmental equipment at the data center facilities, such as the fire detection and suppression systems, climate control systems, and power supply systems, are subject to preventive maintenance by internal and/or third-party specialists. The resulting inspection reports are used to help ensure equipment is maintained and functions properly. Additionally, monitoring systems are utilized to notify facilities personnel in the event environmental levels within the data centers exceed predefined thresholds. These reports can be used for trending and capacity management to assess data center facilities and equipment needs.

MyLightEdge.com

LightEdge provides a web portal for customers to perform basic administration and performance monitoring of services purchased by those customers. Customers are able to retrieve performance logs on a circuit-by-circuit basis. In addition, customers are able to add or remove users to managed services as well as open trouble tickets for incidents or requests related to the services in which they are enrolled.

Customer Data

LightEdge uses several third-party systems to manage data regarding customers' purchased services. Information regarding customer circuits, services, and security is stored in these systems. The systems either reside within LightEdge's internal network and utilizes a web-based application only accessible from the corporate network or through a cloud provider using single sign-on (SSO) to access data.

System Security and Availability Monitoring

An enterprise monitoring system is utilized to monitor the performance and availability of production sites, servers, and devices. An IPS is used for detecting and preventing unauthorized connections to the network, and antivirus software is used to provide virus detection and prevention for Windows production servers and workstations. Reports from the monitoring and security systems are used to analyze security and availability trends within the colocation, managed, and hosted services system.

Ticketing and Change Request Systems

Centralized ticketing systems are used to track customer support requests and incidents as well as change requests for production systems. Reports can be generated from the ticketing and request systems for trending and analysis.

Significant Changes During the Period

LightEdge Solutions, LLC acquired Cavern Technologies in September 2021 and NFINIT in April 2022. As such, controls applicable to Cavern Technologies and the related data center facility (Lenexa) only operated during the September 1, 2021, to July 31, 2022, portion of the period. Controls applicable to NFINIT and related data center facilities (San Diego 1, San Diego 2, and Phoenix 1) only operated during the April 1, 2022, to July 31, 2022, portion of the period.

Subservice Organizations

The data center hosting services provided by Digital Realty at the Phoenix 1 data center were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty, alone or in combination with controls at LightEdge, and the types of controls expected to be implemented at Digital Realty to achieve LightEdge's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Digital Realty	Applicable Trust Services Criteria
Digital Realty is responsible for implementing controls that restrict physical access to the Phoenix 1 data center facility.	CC6.4 – CC6.5
Digital Realty is responsible for implementing controls that protect against environmental vulnerabilities and changing environmental conditions at the Phoenix 1 data center facility.	A1.1 – A1.2

Control Environment

The control environment at LightEdge is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; the oversight and direction provided by the Executive Committee and Senior Management; its organizational structure and the assignment of authority and responsibility; management's commitment to competence; and accountability through management's philosophy and operating style and HR policies and practices.

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 LightEdge's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of LightEdge's 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. Management communicates entity values and behavioral standards to personnel through policy statements and codes of conduct. Specific control activities that LightEdge has implemented in this area are described below.

- Management formally documents and reviews on an annual basis the organizational policy statements that communicate entity values and behavioral standards to personnel.
- Management maintains an Employee Handbook that communicates entity values and behavioral standards.

- Employees sign an acknowledgment form indicating they read and understand administrative policies including those found in the Employee Handbook.
- Background checks are performed for employees as a component of the hiring process.
- Employees and vendors are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Management actively monitors and reports on employees' electronic communication.
- Performance evaluations of employees are conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.
- An employee sanction procedure is documented within the Employee Handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.

Executive Committee and Senior Management Oversight

LightEdge's control consciousness is influenced significantly by the participation of the Executive Committee and Senior Management. Responsibilities of the Executive Committee are documented and understood by Executive and Senior Management personnel. Additionally, external audits are performed on an annual basis. Specific control activities that LightEdge has implemented in this area are described below.

- A committee of Senior Management personnel is in place to oversee management activities and company operations.
- Senior Management personnel meet on a monthly basis to discuss management activities and operational issues.
- An external audit is performed on an annual basis to monitor financial statement reporting practices.

Organizational Structure and Assignment of Authority and Responsibility

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

LightEdge's 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. This includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, policies and communications directed at ensuring that 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 are in place. Specific control activities that LightEdge has implemented in this area are described below:

- Organizational charts are in place to define the organizational structure, reporting lines, and responsibilities. These charts are communicated to employees and updated as needed.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.

Commitment to Competence

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

Specific control activities that LightEdge 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 position requirements.
- Background checks are performed for employees as a component of the hiring process.
- Employees are required to acknowledge upon hire that they have been given access to the Employee Handbook and understand their responsibility for adhering to the entity's code of conduct.
- Employees are required to complete security awareness training upon hire and on a monthly basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
- Performance evaluations of employees are conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.
- An employee sanction procedure is documented within the Employee Handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.
- Management monitors compliance with training requirements on a quarterly basis.

Accountability

LightEdge has defined lines of management authority, which are outlined in the organizational chart. On a monthly basis, the Senior Management Team, consisting of Executives and Managers across functional areas, meets to discuss any issues with the potential to impact multiple departments. Management maintains an "open door" policy to encourage personnel to bring forth questions or concerns. LightEdge uses documented hiring practices to ensure that new employees are qualified for their job responsibilities. The hiring process requires prospective candidates to interview with the department members with whom the candidate will work and with Senior Management. The Chief Executive Officer (CEO) or Chief Operating Officer (COO) approves each prospective employee before LightEdge extends an employment offer. Hiring policies and procedures include confirmation of prior work experience through performance of reference checks.

LightEdge has established a code of ethics to guide its employees with the handling of internal and customer information. The code of ethics is contained within the Employee Handbook. New employees sign the Employee Handbook Acknowledgement Form on their first day of employment. Additionally, employees are required to sign a Professional Employee Agreement, which includes standard employment terms including requirements to conform with LightEdge's code of ethics as described in the Employee Handbook. Employees receive annual performance reviews. Each employee is evaluated based on performance criteria and management provides each employee with feedback. Salary increases and incentives are determined on the basis of the annual review. Many of the Company's personnel hold certifications that are relevant to their area of expertise. LightEdge has an on-site trainer that is responsible for tracking the education requirements, as well as pending expiration dates, for these certifications.

Risk Assessment

Objective Setting

LightEdge recognizes the importance of the ongoing identification and management of risk in order to provide management reasonable assurance that LightEdge's strategic and operational objectives can be achieved. The risk assessment process includes identification and analysis of risks that pose a threat the organization's ability to perform the in-scope services. The process starts with determining the organization's objectives as these objectives are key to understanding the risks and allows identification and analysis of those risks relative to the objectives. Management has committed to customers to carry out certain objectives in relation to the services provided. These commitments are documented to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and company's mission.

Risk Identification and Analysis

LightEdge has considered risks that could affect the organization's ability to provide reliable colocation, managed, and hosted services to its user entities. Management considers risks that could affect customers based on the services to which they subscribe, for example:

- Risks for network customers include loss of service due to misconfiguration, upstream outages, or physical disruption. For managed security services, risks include misconfiguration, flaws in code running on the firewalls, and traffic overflows. Risks for backup customers include misconfiguration or failure of equipment.
- Risks related to software errors are handled by subscribing to and reviewing error report lists from major manufacturers. Applicable systems are upgraded when a significant security flaw is identified to the latest generally stable release of code.
- Risks for colocation customers are failure of electric delivery or cooling systems. Physical issues are addressed with daily systems reviews, preventative maintenance, and automated monitoring.

The LightEdge risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Identification and resolution of longer-term issues are left to the project management teams and are handled as defined projects for completion by each team.

Risk analysis is an essential process to LightEdge's continued success. Senior Management has implemented a process whereby the likelihood and consequence of various risks to the in-scope services have been assessed. Senior leadership broadly defines risk levels to the identified risks, according to the following three categories: low risk, moderate risk, and high risk. A formal risk assessment is performed on an annual basis; however, risks are identified on an ongoing basis and assessed by the Compliance and Security Team.

Risk treatment is recorded in the risk register. Risks with a low score are treated as accepted in the risk register and marked as such. Risks with a medium or high score remain open until treated, transferred to a third party, avoided, or accepted. One or more treatment options must be selected for risks with a medium or high score:

- Selection of security control(s) from Annex A of the ISO/IEC 27001 standard or another standard such as the controls defined within the System and Organization Controls (SOC) 1 or SOC 2 reports.
- Transferring the risk to a third party – examples include purchasing an insurance policy or signing a contract with suppliers or partners.
- Avoiding the risk by discontinuing a business activity that causes such risk.
- Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialize.

Identified risks are reviewed regularly to ensure effectiveness of the Risk Management Policy. The review is conducted during the quarterly management review meetings, or more frequently in the case of significant organizational changes, significant change in technology, change of business objectives, changes in the business environment, etc.

LightEdge operates a peer reviewed change management process to help ensure that network and system level changes are fully reviewed and understood prior to implementation, thus reducing the risk of additional vulnerabilities being introduced into the production environment.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, including fraud incentives and pressures for employees, fraud opportunities, and employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriate of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis, considers the potential for fraud.

Risk Mitigation

Risk mitigation activities include the identification, selection, and development of control activities that reduce the assessed risks to predefined levels of acceptance. However, the relative costs versus benefits should also be considered when determining the risk mitigation activities. The organization has documented policies and procedures to guide personnel throughout this process and achieve repeatable results. Risk assessment and mitigation activities also address risks arising from potential business disruptions.

Risks arising from using vendors and business partners are also considered during the risk assessment and mitigation process. Vendors are considered, assigned access, managed, and monitored in accordance with the vendor management policy. This policy is reviewed, updated, and approved annually. Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Prior to sharing information designated as confidential with third parties, nondisclosure agreements of confidentiality and protection are required to be signed.

Monitoring procedures, including periodic audit reviews, are in place to ensure continual compliance by vendors and business partners. As part of the vendor evaluation process, a risk profile and risk level are assigned to vendors based on risk factors described in the vendor management policy. The assessed risk level determines the periodicity with which periodic audit reviews are to take place; vendors helping to support the in-scope services are assessed on an annual basis which includes an assessment of audit reports or completion of a security assessment.

Trust Services Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability categories.

Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of LightEdge's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. 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.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability are applicable to the colocation, managed, and hosted services system.

Information and Communication Systems

Relevant Information

Information is necessary for LightEdge to carry out internal control responsibilities to support the achievement of its objectives related to the colocation, managed, and hosted services system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. For information regarding the relevant information used by LightEdge, refer to the "Data" section above.

LightEdge has implemented an internal knowledge base to disseminate information to employees. The information is primarily in relation to responses to customer inquiries, but also includes general information. Individual departments are charged with maintaining their relevant information in the knowledge base. Once information is finalized, it is published to the knowledge base for company-wide distribution. Publishing to the network is performed by IT and operations management who follow a two-step process ensuring that changes are approved prior to release to the production environment. Restrictive access controls are also applied if the material being published is not intended for general viewing.

LightEdge has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities, and that significant events are communicated.

Communications

Internal Communications

LightEdge has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for all employees, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate to their supervisor or management.

External Communications

LightEdge has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include the use of e-mail messages and the customer contact line to communicate time-sensitive information. These e-mail communications include, but are not limited to, system alerts, planned changes/maintenance, system outages, and known issues. Customer support personnel contact customers via e-mail or other communication method upon identification of security or availability events that affect the customer environment are detected.

Monitoring

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as customer complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

LightEdge performs ongoing monitoring to help ensure that business systems operate effectively as part of daily operations. Aspects of the ongoing monitoring procedures include the following:

- Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.
- A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices.
- An IPS is utilized to analyze and report network events and block suspected or actual network security breaches.
- Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.

Monitoring systems at LightEdge are set with automatic alerting thresholds that generate system alerts to the network operations team for any failures noted within LightEdge's systems. System alerts are categorized by severity and dispatched accordingly to operations teams for investigation. Automated alert and escalation processes are in place depending on severity level of an alert with Class 1 and Class 2 alerts receiving director of support and / or vice president level notification within four hours of occurrence, if not resolved.

Separate Evaluations

Management has implemented an internal audit program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. The internal audit program assesses control activities that have been implemented to mitigate risks identified as part of the risk assessment process. Control activities within the scope are assigned a risk level associated with the assessed level of risk it is intended to mitigate; controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks. Results of the internal audit process, including findings, are communicated to members of the Senior Management Team.

The Senior Management Team meets on a monthly basis to review company issues and plan direction. Reviews of current and upcoming audits (internal and external) are performed quarterly during these meetings and input is solicited from team members. Product managers are encouraged to review controls impacting their products and provide feedback to further enhance compliance efforts.

Subservice Organization Monitoring

Vendor monitoring procedures include periodic reviews of audit reports to help ensure continual compliance by vendors and business partners. Vendors that help to support the in-scope services are assessed on an annual basis which includes an assessment of audit reports or completion of a security assessment.

Internal and External Auditing

LightEdge supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. LightEdge has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including:

- Type 2 SOC 1 examinations
- Type 2 SOC 2 examinations
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley (SOX)
- National Institute of Standards and Technology (NIST) 800-53
- International Organization for Standardization (ISO) 20000-1
- ISO 22301
- ISO 27001
- Health Information Trust Alliance (HITRUST)

Evaluating and Communicating Deficiencies

Customer complaints are received via a public e-mail address and reviewed on a quarterly basis for consideration on how to improve control activities. Regulator comments and feedback are incorporated and reviewed by Senior Management at the conclusion of any audit or auditable actions.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to the colocation, managed, and hosted services system provided by LightEdge. The scope of the testing was restricted to the colocation, managed, and hosted services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period August 1, 2021, to July 31, 2022.

Tests of Operating Effectiveness

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

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

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

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

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

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

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

Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management formally documents and reviews on an annual basis the organizational policy statements that communicate entity values and behavioral standards to personnel.	Inspected the information security policies and employee handbook to determine that management formally documented and reviewed the organizational policy statements that communicated entity values and behavioral standards to personnel during the period.	No exceptions noted.
CC1.1.2	Employees are required to acknowledge upon hire that they have been given access to the employee handbook and understand their responsibility for adhering to LightEdge's code of conduct.	Inspected the employee handbook acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged that they had been given access to the employee handbook and understood their responsibility for adhering to LightEdge's code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Employees are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the employee handbook acknowledgment for a sample of employees hired during the period to determine that each employee sampled signed confidentiality statements agreeing not to disclose proprietary or confidential information to unauthorized parties.	No exceptions noted.
CC1.1.4	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background check for a sample of employees hired during the period to determine that background checks were performed as a component of the hiring process.	No exceptions noted.
CC1.1.5	Performance evaluations of employees are conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.	Inspected the performance evaluation for a sample of current employees to determine that a performance evaluation was conducted for each employee sampled to evaluate the performance of employees against expected levels of performance and conduct.	No exceptions noted.
CC1.1.6	An employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	Inspected the employee handbook to determine that an employee sanction procedure was documented that communicated that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	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.			
CC1.2.1	Compliance committee meetings are held on a quarterly basis to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the compliance committee meeting calendar entry and minutes for a sample of quarters during the period to determine that meetings were held during each sampled quarter to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	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.			
CC1.3.1	Organizational charts are in place to define the organizational structure, reporting lines, and responsibilities. These charts are communicated to employees and updated as needed.	Inquired of the compliance manager regarding organizational management to determine that organizational charts were in place and updated as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the LightEdge organizational chart to determine that organizational charts were in place that defined the organizational structure, reporting lines, and responsibilities.	No exceptions noted.
		Inspected the organizational chart acknowledgments for a sample of employees hired during the period to determine that organizational charts were communicated to each employee sampled.	No exceptions noted.
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions hired during the period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.3.3	Management has assigned the responsibility of the maintenance and enforcement of LightEdge's security and availability policies and procedures to the chief security officer.	Inspected the information security policy to determine that management has assigned the responsibility of the maintenance and enforcement of LightEdge's security and availability policies and procedures to the chief security officer.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions hired during the period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.4.2	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background check for a sample of employees hired during the period to determine that background checks were performed as a component of the hiring process.	No exceptions noted.
CC1.4.3	Performance evaluations of employees are conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.	Inspected the performance evaluation for a sample of current employees to determine that a performance evaluation was conducted for each employee sampled to evaluate the performance of employees against expected levels of performance and conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.4	Employees are required to complete security awareness training upon hire and on a monthly basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the compliance manager regarding security awareness training to determine that employees were required to complete security training upon hire and on a monthly basis thereafter to ensure they understood their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training documentation for a sample of current employees and employees hired during the period to determine that each employee sampled completed security awareness training upon hire and for each month during the period.	No exceptions noted.
CC1.4.5	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inquired of the compliance manager regarding employee training to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected the training portal to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.4.6	Management monitors compliance with training requirements on a quarterly basis.	Inspected the training completion report and the recurring compliance meeting calendar entry and minutes to determine that management monitored compliance with training requirements on a quarterly basis.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management formally documents and reviews on an annual basis the organizational policy statements that communicate entity values and behavioral standards to personnel.	Inspected the information security policies and employee handbook to determine that management formally documented and reviewed the organizational policy statements that communicated entity values and behavioral standards to personnel during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.2	Internal control responsibilities regarding security and availability are documented within the information security policy. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and procedures and acknowledgements for a sample of employees hired during the period to determine that internal control responsibilities regarding security and availability were documented and each employee sampled acknowledged that they had read and understood their responsibilities.	The test of the control activity disclosed that the information security policies and procedures were not acknowledged upon hire for four (4) of 28 employees sampled.
		Inspected the information security policies and procedures and acknowledgements for a sample of current employees to determine that internal control responsibilities regarding security and availability were documented, and each employee sampled acknowledged that they had read and understood their responsibilities.	No exceptions noted.
CC1.5.3	Compliance committee meetings are held on a quarterly basis to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the compliance committee meeting calendar entry and minutes for a sample of quarters during the period to determine that meetings were held during each sampled quarter to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	No exceptions noted.
CC1.5.4	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions hired during the period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.5.5	Performance evaluations of employees are conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.	Inspected the performance evaluation for a sample of current employees to determine that a performance evaluation was conducted for each employee sampled to evaluate the performance of employees against expected levels of performance and conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Information security policies and procedures are documented and reviewed on an annual basis that identify information required to support the functioning of internal control and achievement of objectives and associated system requirements.	Inspected the information security policies and procedures to determine that policies and procedures were documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated system requirements.	No exceptions noted.
CC2.1.2	Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	Inspected the security monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	No exceptions noted.
CC2.1.3	A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices.	Inspected the monitoring application configurations to determine that a monitoring application was in place to monitor the performance and availability of production sites, servers, and devices.	No exceptions noted.
CC2.1.4	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed monthly and that remediation plans were documented and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.
CC2.1.5	LightEdge's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that LightEdge's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.6	Internal audits are performed on an annual basis by the internal audit function. The audit results are documented and reviewed by management.	Inspected the most recent internal audit reports, quarterly compliance review meeting minutes, and summary of audit results presented to management to determine that internal audits were performed by the internal audit function and that the results were documented and reviewed by management during the period.	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.			
CC2.2.1	Documented policies and procedures are in place and communicated via the company intranet to guide personnel in areas including, but not limited to, the following: • Information security • Acceptable use • Information classification • Change management • Logical and physical access controls	Inspected the information security policies and evidence of communication via the company intranet to determine that documented policies and procedures were in place to guide personnel in areas including, but not limited to, the following: • Information security • Acceptable use • Information classification • Change management • Logical and physical access controls	No exceptions noted.
CC2.2.2	Employees are required to complete security awareness training upon hire and on a monthly basis thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the compliance manager regarding security awareness training to determine that employees were required to complete security training upon hire and on a monthly basis thereafter to ensure they understood their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training documentation for a sample of current employees and employees hired during the period to determine that each employee sampled completed security awareness training upon hire and for each month during the period.	No exceptions noted.
CC2.2.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions hired during the period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.4	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC2.2.5	Compliance committee meetings are held on a quarterly basis to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the compliance committee meeting calendar entry and minutes for a sample of quarters during the period to determine that meetings were held during each sampled quarter to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Service guides for the colocation, managed, and hosted services are documented and communicated to authorized internal and external users.	Inquired of the compliance manager regarding the system description to determine that service guides for the colocation, managed, and hosted services were documented and communicated to authorized internal and external users.	No exceptions noted.
		Inspected the service guides for the colocation, managed, and hosted services, and evidence of communication to users to determine that service guides for the colocation, managed, and hosted services were documented and communicated to authorized internal and external users.	No exceptions noted.
CC2.3.2	LightEdge's security and availability commitments and the associated system requirements are documented in the MSA and SLAs.	Inspected the MSA and applicable SLAs to determine that LightEdge's security and availability commitments and the associated system requirements were documented in the MSA and applicable SLAs.	No exceptions noted.
CC2.3.3	Vendors and third parties are required to sign confidentiality agreements as a component of the onboarding process.	Inspected the nondisclosure agreement for a sample of vendors and third parties utilized during the period to determine that each vendor and third-party sampled was required to sign a confidentiality agreement as a component of the onboarding process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	Documented incident response and support procedures are in place to guide operations personnel in monitoring, documenting, escalating, and resolving problems affecting managed hosting and network services. These procedures include, but are not limited to, the following: • Severity level definitions • Escalation procedures • Ticket handling procedures • Response time requirements for service alerts	Inspected the service request, incident, and problem management procedures to determine that documented incident response and support procedures were in place to guide operations personnel in monitoring, documenting, escalating, and resolving problems affecting managed hosting and network services and included the following: • Severity level definitions • Escalation procedures • Ticket handling procedures • Response time requirements for service alerts	No exceptions noted.
CC2.3.5	A support portal is made available to external users to guide them in identifying and reporting security and availability failures, incidents, concerns, and other complaints to LightEdge.	Inspected the support portal to determine that a portal was made available to external users to guide them in identifying and reporting security and availability failures, incidents, concerns, and other complaints to LightEdge.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Internal control responsibilities regarding security and availability are documented within the information security policy. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and procedures and acknowledgements for a sample of employees hired during the period to determine that internal control responsibilities regarding security and availability were documented and each employee sampled acknowledged that they had read and understood their responsibilities.	Refer to the test results for control activity CC1.5.2.
		Inspected the information security policies and procedures and acknowledgements for a sample of current employees to determine that internal control responsibilities regarding security and availability were documented, and each employee sampled acknowledged that they had read and understood their responsibilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.1.3	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the most recent risk assessment and risk assessment meeting minutes to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC3.1.4	Compliance committee meetings are held on a quarterly basis to review internal control performance.	Inspected the compliance committee meeting minutes for a sample of quarters during the period to determine that meetings were held for each quarter sampled to review internal control performance.	No exceptions noted.
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.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the risk management policy and most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.3	An inventory listing of hardware and software within the scope of services is maintained and reviewed on at least an annual basis as part of the annual internal audit.	Inspected the most recent risk assessment documentation to determine that an inventory listing of hardware and software within the scope of services was maintained and reviewed on at least an annual basis as part of the internal audit.	No exceptions noted.
CC3.2.4	LightEdge's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that LightEdge's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.2.5	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of quarterly compliance review meetings.	Inspected the compliance review meeting minutes for a sample of quarters during the period to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of quarterly compliance review meetings for each quarter sampled.	No exceptions noted.
CC3.2.6	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed monthly and that remediation plans were documented and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.
CC3.2.7	Internal audits are performed on an annual basis by the internal audit function. The audit results are documented and reviewed by management.	Inspected the most recent internal audit reports, quarterly compliance review meeting minutes, and summary of audit results presented to management to determine that internal audits were performed by the internal audit function and that the results were documented and reviewed by management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.8	The compliance team reviews vendor audit reports and/or security questionnaires on an annual basis to help ensure that vendors are in compliance with LightEdge's security and availability requirements.	Inspected the vendor security questionnaire for a sample of vendors to determine that the compliance team reviewed vendor security questionnaires during the period to ensure vendors were in compliance with LightEdge's security and availability requirements for each vendor sampled.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks including the potential for fraud.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risk including the potential for fraud.	No exceptions noted.
CC3.3.2	A risk assessment is performed on an annual basis that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented for management review.	Inspected the risk management policy and most recent risk assessment to determine that a risk assessment was performed on an annual basis that considered the potential for fraud and that identified risks were rated using a risk evaluation process and were formally documented for management review.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	LightEdge's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Inspected example security updates and notifications received during the period to determine that LightEdge's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.4.2	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of quarterly compliance review meetings.	Inspected the compliance review meeting minutes for a sample of quarters during the period to determine that developments in technology and the impact of applicable laws or regulations were considered by senior management as part of quarterly compliance review meetings for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the risk management policy and most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
Monitoring Activities			
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.			
CC4.1.1	An internal audit plan is in place to guide the internal audit function when performing the internal system audit process.	Inspected the internal audit plan to determine that an internal audit plan was in place to guide the internal audit function when performing the internal system audit process.	No exceptions noted.
CC4.1.2	Internal audits are performed on an annual basis by the internal audit function. The audit results are documented and reviewed by management.	Inspected the most recent internal audit reports, compliance review meeting minutes, and summary of audit results presented to management to determine that internal audits were performed by the internal audit function and that the results were documented and reviewed by management during the period.	No exceptions noted.
CC4.1.3	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed monthly and that remediation plans were documented and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.
CC4.1.4	SOC audits and ISO certification assessments are conducted by an accredited independent third-party assessor on an annual basis.	Inquired of the compliance manager regarding third-party assessments to determine that SOC audits and ISO certification assessments were performed by an accredited independent third-party assessor on an annual basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent SOC reports and ISO certifications to determine that SOC audits and ISO certification assessments were performed by an accredited independent third-party assessor on an annual basis.	No exceptions noted.
CC4.1.5	The compliance team reviews vendor audit reports and/or security questionnaires on an annual basis to help ensure that vendors are in compliance with LightEdge's security and availability requirements.	Inspected the vendor security questionnaire for a sample of vendors to determine that the compliance team reviewed vendor security questionnaires during the period to ensure vendors were in compliance with LightEdge's security and availability requirements for each vendor sampled.	No exceptions noted.
CC4.1.6	Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	Inspected the security monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	No exceptions noted.
CC4.1.7	A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices.	Inspected the monitoring application configurations to determine that a monitoring application was in place to monitor the performance and availability of production sites, servers, and devices.	No exceptions noted.
CC4.1.8	The monitoring application is configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds are exceeded on monitored systems.	Inspected the monitoring application configurations and example alerts generated during the period to determine that the monitoring application was configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
CC4.1.9	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
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.			
CC4.2.1	An internal audit plan is in place to guide the internal audit function when performing the internal system audit process.	Inspected the internal audit plan to determine that an internal audit plan was in place to guide the internal audit function when performing the internal system audit process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Internal audits are performed on an annual basis by the internal audit function. The audit results are documented and reviewed by management.	Inspected the most recent internal audit reports, compliance review meeting minutes, and summary of audit results presented to management to determine that internal audits were performed by the internal audit function and that the results were documented and reviewed by management during the period.	No exceptions noted.
CC4.2.3	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed on a monthly basis and that remediation plans were documented and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.
CC4.2.4	SOC audits and ISO certification assessments are conducted by an accredited independent third-party assessor on an annual basis.	Inquired of the compliance manager regarding third-party assessments to determine that SOC audits and ISO certification assessments were performed by an accredited independent third-party assessor on an annual basis.	No exceptions noted.
		Inspected the most recent SOC reports and ISO certifications to determine that SOC audits and ISO certification assessments were performed by an accredited independent third-party assessor on an annual basis.	No exceptions noted.
CC4.2.5	The compliance team reviews vendor audit reports and/or security questionnaires on an annual basis to help ensure that vendors are in compliance with LightEdge's security and availability requirements.	Inspected the vendor security questionnaire for a sample of vendors to determine that the compliance team reviewed vendor security questionnaires during the period to ensure vendors were in compliance with LightEdge's security and availability requirements for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Activities			
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.			
CC5.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC5.1.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inspected the risk management policy and most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC5.1.3	Assigned risk owners select and develop risk response actions to mitigate risks identified during the annual risk assessment process. Risk response actions are documented within the risk register by the risk owners for risks above the tolerable threshold.	Inspected the risk management policy and the most recent risk assessment to determine that assigned risk owners selected and developed risk response actions to mitigate risks identified during the annual risk assessment process and that risk response actions were documented within the risk register by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners select and develop risk response actions over technology to mitigate the risks identified during the annual risk assessment process. Risk response actions are documented within risk registers by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment to determine that assigned risk owners select and develop risk response actions over technology to mitigate the risks identified during the annual risk assessment process. Risk response actions were documented within the risk registers by the risk owners for risks above the tolerable threshold.	No exceptions noted.

Control #	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.			
CC5.3.1	Documented policies and procedures are in place and communicated via the company intranet to guide personnel in areas including, but not limited to, the following: • Information Security • Acceptable Use • Information Classification • Change Management • Logical and Physical Access Controls	Inspected the information security policies and evidence of communication via the company intranet to determine that documented policies and procedures were in place to guide personnel in areas including, but not limited to, the following: • Information Security • Acceptable Use • Information Classification • Change Management • Logical and Physical Access Controls	No exceptions noted.
CC5.3.2	Information security policies and procedures are documented and reviewed on an annual basis that identify information required to support the functioning of internal control and achievement of objectives and associated system requirements.	Inspected the information security and information classification policies to determine that a policy was formally documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	No exceptions noted.
CC5.3.3	Employees are required to acknowledge upon hire that they have been given access to the employee handbook and understand their responsibility for adhering to the entity's code of conduct.	Inspected the employee handbook acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged that they had been given access to the employee handbook and understood their responsibility for adhering to the entity's code of conduct.	No exceptions noted.
CC5.3.4	An employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	Inspected the employee handbook to determine that an employee sanction procedure was documented that communicated that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Logical and Physical Access Controls			
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.			
CC6.1.1	Documented standard build procedures are utilized for the installation and maintenance of production servers and include use of security groups and access permissions to restrict the ability to apply patches to authorized users.	Inspected the standard build procedures to determine that documented standard build procedures were utilized for the installation and maintenance of production servers and included use of security groups and access permissions to restrict the ability to apply patches to authorized users.	No exceptions noted.
CC6.1.2	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Inspected the in-scope system user account listings, LDAP configurations, and password policies to determine that the in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	No exceptions noted.
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to the in-scope systems.	Inspected the production network user and group access listings to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to the in-scope systems.	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope systems administrator to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.5	Encrypted VPNs are required for remote access to the production network and authenticate users with a user account and password.	Inspected the VPN encryption and authentication settings to determine that encrypted VPNs were required for remote access to the production network and authenticated users with a user account and password.	No exceptions noted.
CC6.1.6	Engineering and system support personnel utilize a client password database to manage passwords utilized to access customer infrastructure. Password are stored in an encrypted format.	Inquired of the compliance manager regarding customer infrastructure passwords to determine that engineering and system support personnel utilized a client password database to manage passwords utilized to access customer infrastructure and passwords were stored in an encrypted format.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the client password database table to determine that a client password database was in place to manage passwords and that passwords were stored in an encrypted format.	No exceptions noted.
CC6.1.7	The ability to access the client password database is restricted to user accounts accessible by authorized personnel.	Inspected the operating system user groups and client database access permissions to determine that the ability to access the client password database was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
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.			
CC6.2.1	New employee and contractor user access requests are documented on a standard access request form and require the approval of a manager.	Inspected the access request form for a sample of employees hired during the period to determine that user access requests were documented on a standard access request form and were approved by a manager for each employee sampled.	No exceptions noted.
CC6.2.2	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inspected the termination checklist for a sample of employees terminated during the period to determine that access was revoked for each employee sampled as a component of the employee termination process.	No exceptions noted.
CC6.2.3	User access reviews are performed for in-scope systems on a quarterly basis to help ensure that access to data is restricted and authorized.	Inspected the most recently completed user access reviews for a sample of quarters during the period to determine that IT management reviewed privileged user accounts to help ensure that access to data was restricted and authorized for each quarter sampled.	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.			
CC6.3.1	New employee and contractor user access requests are documented on a standard access request form and require the approval of a manager.	Inspected the access request form for a sample of employees hired during the period to determine that user access requests were documented on a standard access request form and were approved by a manager for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.2	A termination ticket is completed, and access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket for a sample of employees terminated during the period to determine that access was revoked for each employee sampled as a component of the employee termination process.	No exceptions noted.
CC6.3.3	User access reviews are performed for in-scope systems on a quarterly basis to help ensure that access to data is restricted and authorized.	Inspected the most recently completed user access reviews for a sample of quarters during the period to determine that IT management reviewed privileged user accounts to help ensure that access to data was restricted and authorized for each of the quarters sampled.	No exceptions noted.
CC6.3.4	Predefined security groups are utilized to assign role-based access privileges and segregate access to the in-scope systems.	Inspected the production network user and group access listings to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to the in-scope systems.	No exceptions noted.
CC6.3.5	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope systems administrator to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.

[Intentionally Blank]

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.4.1	Physical access control systems and procedures are in place to restrict access to and within the corporate facility and data centers housing the facilities, backup media, and other system components such as firewalls, routers, and servers to authorized individuals.	Observed the physical access control systems and procedures at the corporate facility and data centers to determine that the following physical access controls were in place to restrict access: • Visitors to the corporate office facility were required to check-in at the lobby before being escorted into the back-office area secured via an electronic badge access system • Photo identification was required to obtain data center access for visitors and vendors • Visitors were required to sign a visitor log upon entering the main entrance of the data centers • Visitors required an escort at while onsite at the data centers • An electronic badge access system requiring multi-factor authentication was utilized to control access to and within the data centers • Physical keys were maintained in a locked cabinet located in a secure room accessible by authorized personnel • There were no exterior windows in the production areas of the data centers • A DVR system was in place to monitor and record access within the data centers • Visitors were required to surrender their badge upon exiting the data centers	No exceptions noted.
CC6.4.2	Administrative users authenticate to the badge access system via a user account and password.	Inspected the badge access system login prompt to determine that the badge access system required administrative users to authenticate via a user account and password.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.3	The ability to create, modify, and delete user badge access privileges is restricted to user accounts accessible by authorized data center personnel.	Inspected the badge access system administrator listing with assistance of the facilities manager to determine that the ability to create, modify, and delete user badge access privileges was restricted to user accounts accessible by authorized data center personnel.	No exceptions noted.
CC6.4.4	Requests for the issuance or modification of badge access privileges require manager approval.	Inspected the manager approval for a sample of employees hired during the period to determine that manager approval was obtained for each employee sampled.	No exceptions noted.
CC6.4.5	Badge access privileges are revoked as a component of the employee termination process.	Inspected the badge access listing for a sample of employees terminated during the period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
CC6.4.6	Administrative access to the biometric security system at the data centers is restricted to user accounts accessible by authorized data center personnel.	Inspected the biometric security system administrator user listing to determine that administrative access to the biometric security system at the data centers was restricted to user accounts accessible by authorized data center personnel.	No exceptions noted.
CC6.4.7	The compliance and security team reviews badge access privileges on a quarterly basis.	Inspected the badge access privilege review for a sample of quarters during the period to determine that the compliance and security team reviewed badge access privileges for each quarter sampled.	No exceptions noted.
CC6.4.8	Badge access privileges are sent to authorized client administrators for validation on an annual basis.	Inquired of the facilities manager regarding client badge access validation to determine that reports of badge access privileges were sent to authorized client administrators for validation on an annual basis.	No exceptions noted.
		Inspected the most recent badge access validation ticket for a sample of clients with access to the data centers to determine that a badge access validation ticket was sent during the period for each client sampled.	The test of the control activity disclosed that badge access validations were not sent to authorized client administrators for validation during the period for the following data center facilities: • San Diego 1 • San Diego 2 • Phoenix
	Digital Realty is responsible for implementing controls that restrict physical access to the Phoenix 1 data center facility.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.5.1	Information security policies and procedures are documented and reviewed on an annual basis that identify information required to support the functioning of internal control and achievement of objectives and associated system requirements.	Inspected the information security and information classification policies to determine that a policy was formally documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.	No exceptions noted.
	Digital Realty is responsible for implementing controls that restrict physical access to the Phoenix 1 data center facility.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A firewall system is in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.	Inspected the network diagram and the firewall ruleset to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that was not explicitly authorized.	No exceptions noted.
CC6.6.2	An IPS is utilized to analyze and report network events and block suspected or actual network security breaches.	Inspected the IPS configurations and an example system alert generated during the period to determine that an IPS was utilized to analyze and report network events and deny any type of network connection that was not explicitly authorized.	No exceptions noted.
CC6.6.3	Encrypted VPNs are required for remote access to the production network and authenticate users with a user account and password.	Inspected the VPN encryption and authentication settings to determine that encrypted VPNs were required for remote access to the production network and authenticated users with a user account and password.	No exceptions noted.
CC6.6.4	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS encryption certificates for the myLightEdge portal to determine that web servers utilized encryption for web communication sessions.	No exceptions noted.
CC6.6.5	Firewall rules are reviewed on an annual basis to help ensure only necessary connections are configured within the rulesets.	Inquired of the compliance manager regarding firewall rules to determine that firewall and router rules were reviewed on an annual basis to help ensure only necessary connections were configured within the rulesets.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent firewall ruleset review to determine that firewall and router rules were reviewed during the period.	The test of the control activity disclosed that firewall and router rulesets were not reviewed on an annual basis for the network domain governing the following data center facilities: • San Diego 1 • San Diego 2 • Phoenix
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.			
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the privacy statement and cryptographic controls policy to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Documented policies and procedures are in place to guide personnel in security requirements for removable media.	Inspected the removable media physical security policies to determine that documented policies and procedures were in place to guide personnel in security requirements for removable media.	No exceptions noted.
CC6.7.3	Encrypted VPNs are required for remote access to the production network and authenticate users with a user account and password.	Inspected the VPN encryption and authentication settings to determine that encrypted VPNs were required for remote access to the production network and authenticated users with a user account and password.	No exceptions noted.
CC6.7.4	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS encryption certificates for the myLightEdge portal to determine that web servers utilized encryption for web communication sessions.	No exceptions noted.
CC6.7.5	Administrative access privileges to manage/modify, run backup jobs, and restore backup files are restricted to user accounts accessible by authorized personnel.	Inspected the backup system administrator listings to determine that administrative access privileges to the backup systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	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.			
CC6.8.1	A central antivirus server is utilized to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients on a real-time basis • Scan registered clients on a daily basis	Inspected the enterprise antivirus software configurations and registered client list to determine that enterprise antivirus software was installed on production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients on a real-time basis • Scan registered clients on a daily basis	No exceptions noted.
System Operations			
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.			
CC7.1.1	Documented standard build procedures are utilized for the installation and maintenance of production servers and include use of security groups and access permissions to restrict the ability to apply patches to authorized users.	Inspected the standard build procedures to determine that documented standard build procedures were utilized for the installation and maintenance of production servers and included use of security groups and access permissions to restrict the ability to apply patches to authorized users.	No exceptions noted.
CC7.1.2	Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	Inspected the security monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	No exceptions noted.
CC7.1.3	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed monthly and that remediation plans were documented and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC7.2.1	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC7.2.2	Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	Inspected the security monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	No exceptions noted.
CC7.2.3	An IPS is utilized to analyze and report network events and block suspected or actual network security breaches.	Inspected the IPS configurations and an example system alert generated during the period to determine that an IPS was utilized to analyze and report network events and deny any type of network connection that was not explicitly authorized.	No exceptions noted.
CC7.2.4	A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices.	Inspected the monitoring application configurations to determine that a monitoring application was in place to monitor the performance and availability of production sites, servers, and devices.	No exceptions noted.
CC7.2.5	The monitoring application is configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds are exceeded on monitored systems.	Inspected the monitoring application configurations and example alerts generated during the period to determine that the monitoring application was configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
CC7.2.6	Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.	Inspected the vulnerability assessment for a sample of months during the period to determine that vulnerability scans were performed monthly and that remediation plans were documented and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the most recently performed penetration test to determine that a penetration test was performed during the period and that the identified security vulnerabilities were triaged by the information security team and monitored through resolution.	No exceptions noted.
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.			
CC7.3.1	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC7.3.2	Management meetings are held on a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inspected the calendar invitation and meeting minutes for a sample of months during the period to determine that management meetings were held each month sampled to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
CC7.3.3	KPI reports are reviewed on a monthly basis to evaluate system incidents, responses, and resolution activities.	Inspected the management meeting invites and operational metrics reports for a sample of months during the period to determine that KPI reports were documented to evaluate system incidents, responses, and resolution activities for each month sampled.	No exceptions noted.
CC7.3.4	Operations personnel utilize an issue management / ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services.	Inspected the ticketing system and a listing of tickets generated during the period to determine that operations personnel utilized an issue management / ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services.	No exceptions noted.
CC7.3.5	Incidents requiring a change to the system follow the standard change control process.	Inquired of the compliance manager regarding incidents requiring a change to the system to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC7.4.1	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.
CC7.4.2	Management meetings are held on a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inspected the calendar invitation and meeting minutes for a sample of months during the period to determine that management meetings were held each month sampled to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
CC7.4.3	KPI reports are reviewed on a monthly basis to evaluate system incidents, responses, and resolution activities.	Inspected the management meeting invites and operational metrics reports for a sample of months during the period to determine that KPI reports were documented to evaluate system incidents, responses, and resolution activities for each month sampled.	No exceptions noted.
CC7.4.4	Operations personnel utilize an issue management / ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services.	Inspected the ticketing system and a listing of tickets generated during the period to determine that operations personnel utilized an issue management / ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services.	No exceptions noted.
CC7.4.5	Incidents requiring a change to the system follow the standard change control process.	Inquired of the compliance manager regarding incidents requiring a change to the system to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Inspected the escalation procedures to determine that documented escalation procedures were in place to guide employees in reporting, acting upon, and resolving reported events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.2	Management meetings are held on a monthly basis to discuss incidents and corrective measures to help ensure that incidents are resolved.	Inspected the calendar invitation and meeting minutes for a sample of months during the period to determine that management meetings were held each month sampled to discuss incidents and corrective measures to help ensure that incidents were resolved.	No exceptions noted.
CC7.5.3	KPI reports are reviewed on a monthly basis to evaluate system incidents, responses, and resolution activities.	Inspected the management meeting invites and operational metrics reports for a sample of months during the period to determine that KPI reports were documented to evaluate system incidents, responses, and resolution activities for each month sampled.	No exceptions noted.
Change Management			
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.			
CC8.1.1	Documented maintenance and change management policies and procedures are in place to guide personnel in change management activities affecting existing customer infrastructure.	Inspected the change management policies and procedures to determine that maintenance and change management policies and procedures were in place to guide personnel in change management activities affecting existing customer infrastructure.	No exceptions noted.
CC8.1.2	A change management meeting is held on a weekly basis to discuss and communicate ongoing and upcoming projects that affect the system.	Inspected the change management recurring meeting invite and listing of changes reviewed for a sample of weeks during the period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled.	No exceptions noted.
CC8.1.3	Change requests are documented and tracked via a change request form and include, but are not limited to, the following information: • Description of the change • Change priority • Development and testing plans • Risk and impact analysis • Change status	Inspected the change request form for a sample of customer infrastructure changes implemented during the period to determine that each change sampled was documented and tracked via a change request form and included the following: • Description of the change • Change priority • Development and testing plans • Risk and impact analysis • Change status	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.4	Changes to existing customer infrastructure (except for "standard" changes) require CRB and/or peer approval prior to implementation.	Inquired of the compliance manager regarding customer infrastructure changes to determine that changes to existing infrastructure required CRB and/or peer approval prior to implementation.	No exceptions noted.
		Inspected the change request form for a sample of customer infrastructure changes implemented during the period to determine that each non-standard change sampled was approved by the CRB and/or peer approval process.	The test of the control activity disclosed that approval was not obtained for four (4) of 40 non-standard changes sampled.
CC8.1.5	Infrastructure changes impacting the security and/or availability of customer environments ("normal" changes) are communicated to the customer prior to implementation.	Inquired of the compliance manager regarding change management to determine that infrastructure changes impacting the security and/or availability of customer environments were communicated to the customer prior to implementation.	No exceptions noted.
		Inspected the customer notification for a sample of "normal" customer infrastructure changes implemented during the period to determine that infrastructure changes affecting customer environment's security and/or availability were communicated to the customer prior to implementation.	The test of the control activity disclosed that a customer notification was not communicated prior to implementation for one (1) of 10 "normal" customer infrastructure changes sampled.
CC8.1.6	Incidents requiring a change to the system follow the standard change control process.	Inquired of the compliance manager regarding incidents requiring a change to the system to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC8.1.7	The ability to implement changes to existing customer infrastructure is restricted to user accounts accessible by authorized personnel.	Inspected the operating system user groups and access permissions with assistance of the business operations manager to determine that the ability to implement changes to existing customer infrastructure was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.8	Backout procedures are documented for each change implementation to allow for rollback of changes when changes impair system operation.	Inspected the change tickets for a sample of changes implemented during the period to determine that backout procedures were documented for each change sampled to allow for rollback of changes in the event that a change impaired system operation.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in the identification, selection, and development of risk mitigation activities for risks arising from potential business disruptions.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in the identification, selection, and development of risk mitigation activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis that considers risks arising from potential business disruptions. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the risk management policy and the most recently completed risk assessment to determine that a risk assessment was performed on an annual basis that considered risks arising from potential business disruptions and identified risks were formally documented and rated using a risk evaluation process, along with mitigation strategies, for management review.	No exceptions noted.
CC9.1.3	Assigned risk owners select and develop risk response actions to mitigate risks identified during the annual risk assessment process. Risk response actions are documented within the risk register by the risk owners for risks above the tolerable threshold.	Inspected the risk management policy and the most recent risk assessment to determine that assigned risk owners selected and developed risk response actions to mitigate risks identified during the annual risk assessment process and that risk response actions were documented within the risk register by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC9.1.4	A business continuity plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity plan to determine that a business continuity plan was in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.5	Risk mitigation activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of LightEdge to meet its objectives.	Inspected the third-party cyber insurance policy to determine that risk management activities considered the use of insurance to offset the financial impact of loss events that would impair the ability of LightEdge to meet its objectives.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	A vendor management policy is in place to guide personnel in the following vendor management activities: • Vendor tracking • Ongoing monitoring • Oversight and validation of compliance	Inspected the vendor management policy to determine that a vendor management policy was in place to guide personnel in the following vendor management activities: • Vendor tracking • Ongoing monitoring • Oversight and validation of compliance	No exceptions noted.
CC9.2.2	The compliance team reviews vendor audit reports and/or security questionnaires on an annual basis to help ensure that vendors are in compliance with LightEdge's security and availability requirements.	Inspected the vendor security questionnaire for a sample of vendors to determine that the compliance team reviewed vendor security questionnaires during the period to ensure vendors were in compliance with LightEdge's security and availability requirements for each vendor sampled.	No exceptions noted.
CC9.2.3	Vendors and third parties are required to sign confidentiality agreements as a component of the onboarding process.	Inspected the nondisclosure agreement for a sample of vendors and third parties utilized during the period to determine that each vendor and third-party sampled was required to sign a confidentiality agreement as a component of the onboarding process.	No exceptions noted.

Additional Criteria for Availability

Control #	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.			
A1.1.1	A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices and notify operations personnel via e-mail and onscreen alerts when predefined thresholds are exceeded on monitored systems.	Inspected the monitoring application configurations and example alerts generated during the period to determine that a monitoring application was in place to monitor the performance and availability of production sites, servers, and devices and notify operations personnel via e-mail and onscreen alerts when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.1.2	Management meetings and operational review meetings are held on a monthly and quarterly basis, respectively, to review availability trends and availability forecasts as compared to system commitments.	Inspected the management and operational review meeting minutes for a sample of months and quarters during the period to determine that management and operational review meetings were held each quarter and month sampled to review availability trends and availability forecasts as compared to system commitments.	No exceptions noted.
	Digital Realty is responsible for implementing controls that protect against environmental vulnerabilities and changing environmental conditions at the Phoenix 1 data center facility.		
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.			
A1.2.1	The data centers are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units	Observed the environmental protection equipment within the data centers to determine that the data centers were equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units	No exceptions noted.
A1.2.2	Management obtains inspection reports from third-party specialists as evidence that the fire detection and suppression systems undergo maintenance inspections on an annual basis.	Inspected the most recent fire system inspection reports to determine that third-party specialists inspected the fire detection and suppression systems during the period.	No exceptions noted.
A1.2.3	Management obtains inspection reports from third-party specialists as evidence that the UPS systems undergo maintenance inspections on a semi-annual basis.	Inspected UPS system inspection reports received during the period to determine that third-party specialists inspected the UPS systems on a semi-annual basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A.1.2.4	Management obtains inspection reports from third-party specialists as evidence that the generators undergo maintenance inspections on an annual basis.	Inspected the most recent generator inspection reports to determine that third-party specialists inspected the generators during the period.	No exceptions noted.
A1.2.5	Internal personnel or third-party specialists inspect air conditioning systems according to a predefined maintenance schedule.	Inspected the air conditioning inspection reports for a sample of quarters during the period to determine internal personnel or third-party specialists inspected the air conditioning units according to a predefined maintenance schedule.	No exceptions noted.
A1.2.6	The monitoring application is configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds are exceeded on monitored systems.	Inspected the monitoring application configurations and example alerts generated during the period to determine that the monitoring application was configured to notify operations personnel via e-mail and onscreen alerts when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.2.7	Operations personnel are available on a 24x7 basis to monitor client environments.	Inquired of the facilities manager regarding monitoring to determine that operations personnel were available on a 24x7 basis to monitor client environments.	No exceptions noted.
		Inspected the staffing schedule utilized during the period to determine that operations personnel were staffed on a 24x7 basis.	No exceptions noted.
A1.2.8	The automated backup systems are configured to perform backups of client production environments on at least a daily basis.	Inspected the backup system configurations and backup logs generated during the period for a sample of clients to determine that automated backup systems were configured to perform at least daily backups of the production environments for each client sampled.	No exceptions noted.
A1.2.9	The automated backup systems are configured to log the status of backup jobs and notify operations personnel via e-mail regarding the success or failure of backup jobs.	Inspected the data backup notification configurations and example e-mails generated during the period to determine that automated backup systems were configured to log the status of backup jobs and notify operations personnel via e-mail regarding the success or failure of backup jobs.	No exceptions noted.
A1.2.10	Backup data is replicated between data centers that are geographically separated.	Inspected the backup replication configurations and an example backup job log generated during the period to determine that backup data was replicated between data centers that were geographically separated.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.11	A business continuity plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity plan to determine that a business continuity plan was in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	Digital Realty is responsible for implementing controls that protect against environmental vulnerabilities and changing environmental conditions at the Phoenix 1 data center facility.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	IT personnel perform restoration of backup files at least annually as a component of business operations to help ensure system recovery.	Inquired of the compliance manager regarding backup restorations to determine that IT personnel performed restorations of backup files at least annually as a component of business operations to help ensure system recovery.	No exceptions noted.
		Inspected the results of example backup restorations performed during the period to determine that IT personnel performed restorations of backup files at least annually as a component of business operations.	No exceptions noted.
A1.3.2	The business continuity plan is tested on an annual basis.	Inquired of the compliance manager regarding business continuity testing to determine that the business continuity plan was tested on an annual basis.	No exceptions noted.
		Inspected the results of the annual business continuity plan test to determine that the business continuity plan was tested during the period.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY LIGHTEDGE

Management’s Response to Testing Exceptions

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC1.5.2 CC3.1.1	Internal control responsibilities regarding security and availability are documented within the information security policy. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and procedures and acknowledgements for a sample of employees hired during the period to determine that internal control responsibilities regarding security and availability were documented and each employee sampled acknowledged that they had read and understood their responsibilities.	The test of the control activity disclosed that the information security policies and procedures were not acknowledged upon hire for four (4) of 28 employees sampled.
Management’s Response:	Prior policy acknowledgements were leveraged for a majority of the users brought on through acquisition, which erroneously delayed the LightEdge policy acknowledgement process. The Human Resource Team reviewed all employee records and immediately implemented new procedures to ensure this does not occur with future acquisitions.		
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.			
CC6.4.8	Badge access privileges are sent to authorized client administrators for validation on an annual basis.	Inspected the most recent badge access validation ticket for a sample of clients with access to the data centers to determine that a badge access validation ticket was sent during the period for each client sampled.	The test of the control activity disclosed that badge access validations were not sent to authorized client administrators for validation during the period for the following data center facilities: • San Diego 1 • San Diego 2 • Phoenix
Management’s Response:	This control was not required at the San Diego 1, San Diego 2, and Phoenix data centers prior to the LightEdge acquisition. During the audit, it was identified that this process was not completed timely as part of the LightEdge and NFINIT integration process. NFINIT clients will be included in the LightEdge customer badge validation going forward.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.5	Firewall rules are reviewed on an annual basis to help ensure only necessary connections are configured within the rulesets.	Inspected the most recent firewall ruleset review to determine that firewall and router rules were reviewed during the period.	The test of the control activity disclosed that firewall and router rulesets were not reviewed on an annual basis for the network domain governing the following data center facilities: • San Diego 1 • San Diego 2 • Phoenix
Management’s Response:	This control was not required at the San Diego 1, San Diego 2, and Phoenix 1 data centers prior to the LightEdge acquisition. During the audit, it was identified that this process was not completed timely as part of the LightEdge and NFINIT integration process. NFINIT firewalls will be included in the LightEdge firewall reviews going forward.		

Control #	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.			
CC8.1.4	Changes to existing customer infrastructure (except for “standard” changes) require CRB and/or peer approval prior to implementation.	Inspected the change request form for a sample of customer infrastructure changes implemented during the period to determine that each non-standard change sampled was approved by the CRB and/or peer approval process.	The test of the control activity disclosed that approval was not obtained for four (4) of 40 non-standard changes sampled.
Management’s Response:	LightEdge investigated the non-standard/emergency change process. The employees responsible for executive the 4 changes noted did not document the required emergency change approval. Approval was obtained and management was aware of all activities during the change, but documentation was not maintained. All employees responsible for change management have been retrained on the change management process.		
CC8.1.5	Infrastructure changes impacting the security and/or availability of customer environments (“normal” changes) are communicated to the customer prior to implementation.	Inspected the customer notification for a sample of “normal” customer infrastructure changes implemented during the period to determine that infrastructure changes affecting customer environment’s security and/or availability were communicated to the customer prior to implementation.	The test of the control activity disclosed that a customer notification was not communicated prior to implementation for one (1) of 10 “normal” customer infrastructure changes sampled.
Management’s Response:	LightEdge reviewed the change management process including external communication procedures. The employee responsible for sending communication of the infrastructure change to the customer did not send the communication prior to implementation. This employee has been retrained on the infrastructure change notification process and additional processes and reviews have been put in place.		