



LIGHTEGE SOLUTIONS, LLC

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

COLOCATION, MANAGED, AND HOSTED SERVICES SYSTEM

FOR THE PERIOD OF AUGUST 1, 2021, TO JULY 31, 2022

Attestation and Compliance Services



Proprietary & Confidential

Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To LightEdge Solutions, LLC:

Scope

We have examined LightEdge Solutions, LLC's ("LightEdge") accompanying assertion titled "Assertion of LightEdge Solutions, LLC Service Organization Management" ("assertion") that the controls within LightEdge's colocation, managed, and hosted services system ("system") were effective 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 of the boundaries of the system 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 of the boundaries of the system 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.

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 also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LightEdge is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve LightEdge's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve LightEdge's service commitments and system requirements based on the applicable trust services criteria.

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

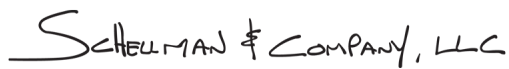
Inherent Limitations

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 LightEdge's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within LightEdge's colocation, managed, and hosted services system were effective throughout the period August 1, 2021, through July 31, 2022, to provide reasonable assurance that LightEdge's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHHELLMAN & COMPANY, LLC

Tampa, Florida
August 29, 2022

ASSERTION OF LIGHTEDGE SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within LightEdge Solutions, LLC's ("LightEdge") colocation, managed, and hosted services system ("system") throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system 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's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2021, to July 31, 2022, to provide reasonable assurance that LightEdge's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE COLOCATION, MANAGED, AND HOSTED SERVICES SYSTEM

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

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

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 98 th 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.

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.

Infrastructure and Software

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 to 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 meet those criteria.

Control Activities 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

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.

Trust Services Criteria Not Applicable to the In-Scope System

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