LightEdge Solutions, LLC

SOC 1 Report

For

Colocation, Managed, and Hosted Services

A Type 2 Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

For the Period August 1, 2021, to July 31, 2022

Prepared in Accordance with the
AICPA SSAE No. 18 and IAASB ISAE 3402 Standards

Attestation and Compliance Services

Quality, above all.

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

This report is intended solely for use by the management of LightEdge Solutions, LLC, its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (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 "service organization") description of its colocation, managed, and hosted services system throughout the period August 1, 2021, to July 31, 2022 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of LightEdge believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the colocation, managed, and hosted services system that are not likely to be relevant to user entities' internal control over financial reporting.

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description includes only the control objectives and related controls of LightEdge and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified by LightEdge can be achieved only if complementary subservice organization controls assumed in the design of LightEdge's controls are suitably designed and operating effectively, along with the related controls at LightEdge. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of LightEdge's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in Section 5, "Other Information Provided by LightEdge" is presented by management of LightEdge to provide additional information and is not a part of LightEdge's description of its colocation, managed, and hosted services system made available to user entities during the period August 1, 2021, to July 31, 2022. Information in Section 5 has not been subjected to the procedures applied in the examination of description of the colocation, managed, and hosted services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the colocation, managed, and hosted services system.

Service Organization's Responsibilities

In Section 2, LightEdge has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. LightEdge is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period August 1, 2021, to July 31, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in providing colocation, managed, and hosted services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in LightEdge's assertion in Section 2:

a. the description fairly presents the colocation, managed, and hosted services system that was designed and implemented throughout the period August 1, 2021, to July 31, 2022;
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period August 1, 2021, to July 31, 2022, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of LightEdge's controls throughout the period August 1, 2021, to July 31, 2022; and
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period August 1, 2021, to July 31, 2022, if, as applicable, complementary subservice organization and user entity controls assumed in the design of LightEdge's controls operated effectively throughout the period August 1, 2021, to July 31, 2022.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of LightEdge, user entities of LightEdge's colocation, managed, and hosted services system during some or all of the period August 1, 2021, to July 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Schellman & Company, LLC

Tampa, Florida
August 29, 2022

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

We have prepared the description of LightEdge Solutions, LLC's ("LightEdge") colocation, managed, and hosted services system throughout the period August 1, 2021, to July 31, 2022 (the "description"), for user entities of the system during some or all of the period August 1, 2021, to July 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description includes only the control objectives and related controls of LightEdge and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

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

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

a. the description fairly presents the colocation, managed, and hosted services system made available to user entities of the system during some or all of the period August 1, 2021, to July 31, 2022. The criteria we used in making this assertion were that the description:

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

        (1) the types of services provided including, as appropriate, the classes of transactions processed;

        (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities of the system;

        (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

        (4) how the system captures and addresses significant events and conditions, other than transactions;

        (5) the process used to prepare reports or other information provided for entities;

        (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

        (7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the LightEdge's controls; and

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

ii. includes relevant details of changes to the colocation, managed, and hosted services system during the period covered by the description; and

iii. does not omit or distort information relevant to the scope of the colocation, managed, and hosted services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the colocation, managed, and hosted services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period August 1, 2021, to July 31, 2022, to achieve those control objectives if, as applicable, subservice organizations and user entities applied complementary controls assumed in the design of LightEdge's controls throughout the period August 1, 2021, to July 31, 2022. The criteria we used in making this assertion were that:

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

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

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

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

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.

The colocation, managed, and hosted services system described within this report is an information technology general control (ITGC) system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them. Additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within their environments; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

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 service level agreements (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.

Data Management

<u>Physical Security</u>

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).

<u>Environmental Security</u>

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.

Subservice Organizations

LightEdge utilizes the data center hosting services provided by Digital Realty at the Phoenix 1 data center. LightEdge's colocation, managed, and hosted services system was designed with the assumption that no subservice organization controls were required in the design of LightEdge's controls; therefore, no control objectives related to LightEdge's colocation, managed, and hosted services system are dependent upon complementary subservice organization controls that are suitably designed and operating effectively, along with the related controls at LightEdge.

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.

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

Risk Identification

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.

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 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

Risk Analysis

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.

Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

Control Objectives and Related Control Activities

Selection and Development of Control Activities

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

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

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

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

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

Physical Security

Control Objective: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

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

Control Objective: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats

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.

Customer Provisioning

Control Objective: Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

Client-specific standard operating procedures are in place to address requirements for new client implementations. LightEdge maintains contracts with each client to define the terms of service provided, description of services provided, pricing, service agreements, and contract terms. Project managers utilize a centralized ticketing system to record client implementation requirements and to facilitate and track implementation activities, project status, and assigned resources. Project managers are responsible for amending any contracts when services or features change during the implementation process or are deemed undeliverable for any reason. A copy of the contract amendment is stored in the customer's contract folder and a copy of the contract amendment is given to the customer for their records. Project managers provide client personnel with a start of service notification upon completion of implementation activities. LightEdge restricts the ability to provision new client environments to authorized provisioning personnel.

Support requests to make changes to a client's active services must be submitted or approved by an authorized client administrator before project activities are initiated. Once verified, the support requests are documented and tracked within the centralized ticketing system. Upon completion of the service change, notification is then sent via e-mail to the account management team who records the requested changes in the form of a contract amendment to the client's contracted services.

Logical Security

Control Objective: Control activities provide reasonable assurance that managed infrastructure and hosting services are protected from unauthorized or unintentional use and modification.

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.

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.

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.

Customer data including client databases, files, disks, data and/or systems are encrypted at rest based on company encryption policies and requirements. Additionally, customers that subscribe to LightEdge's VPN tunnel offering are provided with encrypted VPN connections to help ensure that remote connections to the managed production environment are secured.

Data Backup

Control Objective: Control activities provide reasonable assurance that application and data files are backed up in a timely manner and securely stored.

LightEdge utilizes commercial backup systems to perform disk-to-disk backups of production data and systems. 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.

Maintenance and Change Management

Control Objective: Control activities provide reasonable assurance that changes to existing customer infrastructure are authorized, approved, and documented before being implemented in the production environment.

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.

System Availability

Control Objective: Control activities provide reasonable assurance that customer infrastructure is available for operation and use, and that problems are identified, investigated, and resolved in a timely manner.

Production server hardware is protected by equipment warranties to provide service, replacement, and on-site maintenance to help ensure systems continue to function properly and remain available over time. Monthly management meetings are held to review asset inventory reports and help ensure availability of production systems.

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.

Customer Support and Incident Response

Control Objective: Control activities provide reasonable assurance that customer inquiries and issues are responded to in a timely manner.

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, key performance indicator (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.

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 Management” 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 Activities

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 intrusion protection system (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.

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)

Monitoring of Subservice Organizations

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.

Reporting 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

LightEdge's colocation, managed, and hosted services system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to LightEdge's colocation, managed, and hosted services system to be solely achieved by LightEdge's control activities. Accordingly, user entities, in conjunction with the colocation, managed, and hosted services system, should establish their own internal controls or procedures to complement those of LightEdge.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls that ensure a facility access listing of personnel, vendors, and contractors authorized to access the data center(s) housing the user entity's equipment is maintained, and LightEdge is notified of any changes.	Physical Security
User entities are expected to implement controls that ensure LightEdge is notified of on-site visits of employees, vendors, and contractors prior to arrival at the data center(s).	
User entities with rack-based colocation are expected to implement controls that ensure rack combination locks are configured and periodically changed.	
User entities are expected to implement controls that ensure implementations are completed in accordance with contractual specifications upon notification that implementation activities are completed.	Customer Provisioning
User entities are expected to implement controls that ensure LightEdge is notified of changes made to technical or administrative contact information.	
User entities are expected to implement controls that ensure the supervision, management, and control of the use of LightEdge's services by their personnel.	
User entities are expected to implement controls that ensure the logical security of their infrastructure, including the implementation of access control systems and configuration of password security requirements on their infrastructure.	Logical Security
User entities are expected to implement controls that ensure the management and administration of remote access via their VPN devices / systems.	
User entities are expected to implement controls that ensure the establishment of control procedures to administer security for those applications and databases residing on LightEdge managed servers.	
User entities are expected to implement controls that ensure LightEdge is notified of required backup schedules and retention requirements.	Data Backup
User entities are expected to implement controls that ensure the identification of representatives authorized to request changes.	Maintenance and Change Management
User entities are expected to implement controls that ensure LightEdge is notified of requested changes and for ensuring that change and support requests submitted to LightEdge are complete and accurate.	
User entities are expected to implement controls that ensure escalation procedures are established and maintained for problems identified on their network services or hosts. User entities are responsible for communicating these procedures to LightEdge and for notifying LightEdge of changes to the escalation procedures as applicable.	Systems Availability and Customer Support and Incident Response
User entities are expected to implement controls that ensure the entity responds to incidents reported by LightEdge in a timely manner.	

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 included the applicable controls for the colocation, managed, and hosted services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period August 1, 2021, through 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 specified control objectives were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

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

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

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during testing. 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 evidentiary matter 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 and evaluated for accuracy and 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.

Test Results

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

PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	Documented policies and procedures are in place to address the granting, controlling, and monitoring of physical access.	Inspected the data center standard operating procedures and access control policy to determine that documented policies and procedures were in place to address the granting, controlling, and monitoring of physical access.	No exceptions noted.
	Corporate Office Facility (Multi-Tenant Office Building) – Des Moines, Iowa		
1.02	Visitors to the corporate office facility are required to check in at the lobby before being escorted into the back-office area. Access to the back-office area is restricted via a badge access system.	Observed the corporate office facility visitor entrance process to determine that visitors to the corporate office facility were required to check in at the lobby before being escorted into the back-office area, and that the back-office area was restricted via a badge access system.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Data Center Facilities (Altoona 1, Altoona 2, Kansas City, Omaha, Austin 1, Austin 2, Raleigh, Lenexa, Phoenix 1, San Diego 1, San Diego 2)		
1.03	Visitors and vendors are required to present government-issued photo identification prior to being granted data center access.	Inquired of the data center facility managers regarding data center access to determine that visitors and vendors were required to present government-issued photo identification prior to being granted data center access.	No exceptions noted.
		Observed the data center access procedures to determine that visitors and vendors were required to present government-issued photo identification prior to being granted data center access.	No exceptions noted.
1.04	Visitors are required to sign a visitor log upon entering the main entrance of the data centers.	Observed the data center visitor entrance process to determine that visitors were required to sign a visitor log upon entering the main entrance of the data centers.	No exceptions noted.
		Inspected the visitor logs maintained during the period to determine that visitor logs were utilized at each data center throughout the period.	No exceptions noted.
1.05	An electronic badge access system is utilized to control access to and within the data centers.	Observed the data centers to determine that an electronic badge access system was utilized to control access to and within each data center.	No exceptions noted.
		Inspected example recent and historical badge access logs generated during the period to determine that an electronic badge access system was utilized throughout the period to control access to and within each data center.	No exceptions noted.
1.06	LightEdge employee data center access is restricted to badge access cards assigned to authorized personnel based on business responsibility.	Inspected the badge access listings with assistance of the facilities manager to determine that data center access for LightEdge employees was restricted to badge access cards assigned to authorized personnel based on business responsibility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.07	The badge access system logs access attempts traceable to individual cardholders.	Inspected example recent and historical badge access logs generated during the period to determine that the badge access system logged access attempts traceable to individual cardholders.	No exceptions noted.
1.08	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.
1.09	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.
1.10	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.
1.11	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.
1.12	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.13	Access to the production areas of the data centers is restricted through the use of multi-factor authentication (badge plus biometric/PIN combination).	Observed the process for gaining access to the production areas to determine that access to the production areas of the data centers was restricted through the use of multi-factor authentication (badge plus biometric/PIN combination).	No exceptions noted.
1.14	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 with the assistance of the facilities managers 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.
1.15	Data center access listings are maintained to identify approved administrative contacts and data center users.	Inspected the data center access listing for a sample of clients with access to the data centers during the period to determine that data center access listings were maintained to identify approved administrative contacts and data center users for each client sampled.	No exceptions noted.
1.16	Client access requests for the issuance, modification, or revocation of badge access privileges require approval from an authorized client administrator.	Inspected the client access authorization for a sample of client badge access requests completed during the period to determine that an authorized client administrator approved each access sampled.	No exceptions noted.
1.17	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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 1
1.18	Physical keys are maintained in a locked cabinet in a secured room accessible by authorized data center personnel.	Observed the storage location used for physical keys to determine that physical keys were maintained in a locked cabinet located in a secured room accessible by authorized data center personnel.	No exceptions noted.
1.19	An inventory listing of issued physical keys is maintained for the data centers.	Inspected the physical key inventory listings to determine that an inventory listing of issued physical keys was maintained for each data center.	The test of the control activity, performed in May 2022, disclosed that an inventory listing issued physical keys was not maintained at Lenexa data center facility. Subsequent testing of the control activity, performed in June 2022, disclosed that a physical key inventory listing was implemented at the Lenexa data center facility.
1.20	A DVR is in place to monitor and record access within the data centers.	Inspected images from the DVR system to determine that a DVR was in place to monitor and record access within each data center.	No exceptions noted.
1.21	DVR backups of surveillance recordings are maintained for a minimum of 90 days.	Inspected recent and historical images from the DVR system to determine that DVR backups of surveillance recordings were maintained for a minimum of 90 days for each data center.	The test of the control activity disclosed that historical DVR images for the San Diego 2 data center facility were not maintained for a minimum of 90 days.
1.22	There are no exterior windows in the production areas of the data centers.	Observed the data centers to determine that there were no exterior windows in the production areas of the data centers.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.23	Key usage logs are maintained to track the issuance and return of physical keys to the data centers.	Inspected the key usage logs maintained during the period to determine that key usage logs were maintained throughout the period to track the issuance and return of physical keys.	No exceptions noted.
	Data Center Facilities (Altoona 1, Altoona 2, Austin 2, Kansas City, Omaha, Lenexa, Raleigh, Phoenix 1, San Diego 1, and San Diego 2)		
1.24	Access to the production areas of the data centers is restricted through the use of a mantrap.	Observed the process for gaining access to the data center production areas to determine that access to the production areas of each data center was restricted through the use of a mantrap.	No exceptions noted.
	Data Centers (Altoona 1, Altoona 2, Kansas City, and Omaha)		
1.25	Access to the production areas of the data centers is restricted through the use of tailgating sensors.	Observed the process for gaining access to the data center production areas to determine that access to the production areas of each data center was restricted through the use of tailgating sensors.	No exceptions noted.

ENVIRONMENTAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	Documented procedures are in place to help govern environmental security practices.	Inspected the data center standard operating procedures to determine that documented procedures were in place to help govern environmental security practices.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Corporate Office Facility (Des Moines, Iowa)		
2.02	The corporate office facility is equipped with the following fire detection and suppression controls: • Fire extinguishers • Sprinkler system • Audible and visual fire alarms	Observed the fire detection and suppression controls at the corporate office facility to determine that the corporate office facility was equipped with the following fire detection and suppression controls: • Fire extinguishers • Sprinkler system • Audible and visual fire alarms	No exceptions noted.
	Data Center Facilities		
2.03	The data centers are equipped with the following fire detection and suppression devices: • Fire extinguishers • Fire suppression systems • Audible and visual fire alarms	Observed the data centers to determine that the data centers were equipped with the following fire detection and suppression devices: • Fire extinguishers • Fire suppression systems • Audible and visual fire alarms	No exceptions noted.
2.04	Third-party security specialists monitor fire detection and suppression systems 24 hours per day.	Inquired of the data center facility managers regarding monitoring of fire suppression controls at the data centers to determine that third-party security specialists monitored the fire and alarm systems 24 hours per day.	No exceptions noted.
		Inspected the security contracts and example invoices received during the period to determine that third-party security specialists were contracted to monitor the fire detection and suppression systems 24 hours per day.	No exceptions noted.
2.05	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.
2.06	The data centers are equipped with dedicated air conditioning units to regulate temperature and humidity levels.	Observed the data centers to determine that the data centers were equipped with dedicated air conditioning units to regulate temperature and humidity levels.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.07	The air conditioning units are configured to notify data center personnel in the event that predefined temperature levels are exceeded.	Inspected the air conditioning unit monitoring configurations and alarm notification received during the period for each data center to determine that the air conditioning units were configured to notify data center personnel in the event that predefined temperature levels were exceeded.	No exceptions noted.
2.08	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.
2.09	Production servers are mounted on racks within the data centers to facilitate cooling and protect servers from localized flooding.	Observed the data center production areas to determine that production servers were mounted on racks within the data centers to facilitate cooling and protect servers from localized flooding.	No exceptions noted.
2.10	Production equipment is connected to UPS systems configured to provide temporary electricity in the event of a power outage.	Observed the data center production equipment to determine that UPS systems were in place to provide temporary electricity in the event of a power outage.	No exceptions noted.
2.11	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.
2.12	The data centers are connected to dedicated power generators configured to provide electricity in the event of a power outage.	Observed the generators located at the data centers to determine that generators were in place to provide electricity in the event of a power outage.	No exceptions noted.
2.13	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.14	The generators are load tested on at least an annual basis.	Inspected the most recent data center generator load test results to determine that load testing of the generators was performed during the period.	No exceptions noted.

Customer Provisioning

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	Client-specific provisioning procedures are in place to address requirements for new client implementations.	Inspected the provisioning procedures for a sample of clients onboarded during the period to determine that documented provisioning procedures were in place for each client sampled.	No exceptions noted.
3.02	Contracts are maintained with each client to define the terms of services provided and document the following: • Description of services • Pricing • Service agreements • Contract terms	Inspected the contract for a sample of clients onboarded during the period to determine that a contract was documented for each sampled client to define the terms of services provided and included the description of services, pricing, service agreements, and contract terms.	No exceptions noted.
3.03	Project managers record client implementation requirements in a project plan to facilitate and track implementation activities and project status.	Inspected the project plan for a sample of clients onboarded during the period to determine that implementation requirements were documented in a project plan for each client sampled.	No exceptions noted.
3.04	Project managers notify client personnel upon completion of implementation activities.	Inspected the service activation notifications for a sample of clients onboarded during the period to determine that project managers notified client personnel upon completion of implementation activities for each client sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.05	Provisioning setup is restricted to user accounts accessible by authorized LightEdge personnel.	Inspected the operating system user groups and access permissions with the assistance of the business operations manager to determine that provisioning setup was restricted to user accounts accessible by authorized LightEdge personnel.	No exceptions noted.
3.06	Client support requests are submitted and tracked electronically via a ticketing system.	Inspected the listing of client support requests received during the period to determine that each client support request sampled was submitted and tracked electronically via a ticketing system.	No exceptions noted.
3.07	Client support requests are required to be submitted and/or approved by an authorized client administrator.	Inspected the support ticket and list of authorized client administrators for a sample of client support requests received during the period to determine that each client support request sampled was submitted and/or approved by an authorized client administrator.	No exceptions noted.

Logical Security

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that managed infrastructure and hosting services are protected from unauthorized or unintentional use and modification.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.01	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.	Inspected the information security policies to determine that documented information security policies were in place and addressed acceptable use of information systems and safeguarding of systems infrastructure, information assets and data.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.02	Information sensitivity classifications and employee guidelines are established for the handling and labeling of information based on sensitivity, value, and criticality.	Inspected the information security policies to determine that information sensitivity classifications and employee guidelines were documented for the handling and labeling of information based on sensitivity, value, and criticality.	No exceptions noted.
4.03	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.
4.04	Dedicated engineering and operations teams are responsible for provisioning logical access to managed infrastructure and hosting services.	Inquired of the compliance manager regarding logical access to determine that dedicated engineering and operations teams were in place and responsible for provisioning logical access to managed infrastructure and hosting services.	No exceptions noted.
		Inspected the operating system user groups and access permissions to determine that dedicated engineering and operations teams were in place.	No exceptions noted.
4.05	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.
4.06	The ability to access customer environments is restricted to user accounts accessible by authorized personnel based on business responsibility.	Inspected the operating system user groups and access permissions with assistance of the business operations manager to determine that the ability to access customer environments was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.07	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.
		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.
4.08	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.
4.09	System owners disable network user accounts assigned to terminated employees.	Inspected the network user access permissions for a sample of employees terminated during the period to determine that active network accounts were not assigned to the terminated employees sampled.	No exceptions noted.
4.10	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 user access review for a sample of quarters during the period to determine that user access reviews were performed for each sampled quarter to help ensure that access to data was restricted and authorized.	No exceptions noted.
4.11	The myLightEdge web portal is in place to provide customers the ability to monitor the following: • Managed infrastructure • Hosting services • Changes	Inquired of the compliance manager regarding the myLightEdge web portal to determine that an online portal was in place to provide customers the ability to monitor the following: • Managed infrastructure • Hosting services • Changes	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the myLightEdge web portal to determine that an online portal was in place to provide customers the ability to monitor the following: • Managed infrastructure • Hosting services • Changes	No exceptions noted.
4.12	The myLightEdge web portal is configured to restrict customers from accessing other customers' data.	Inspected the web portal backend code and myLightEdge web portal access denied screens to determine that myLightEdge was configured to restrict customers from accessing other customers' data.	No exceptions noted.
	Internal Server Authentication – Network Domain		
4.13	Network users are authenticated via a user account and password before being granted access to the network domain.	Inspected the network domain configurations to determine that network users were authenticated via a user account and password before being granted access to the network domain.	No exceptions noted.
4.14	The network domain is configured to enforce the following password requirements: • Password minimum length • Password expiration intervals • Password complexity • Password history	Inspected the network domain policies to determine that the network domain was configured to enforce the following password requirements: • Password minimum length • Password expiration intervals • Password complexity • Password history	No exceptions noted.
4.15	The network domain is configured to store network user account passwords in an encrypted format.	Inquired of the compliance manager regarding network domain authentication security to determine that the network domain was configured to store network user account passwords in an encrypted format.	No exceptions noted.
		Inspected the network authentication configurations to determine that the network domain was configured to store network user account passwords in an encrypted format.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Internal Server Access – Network Domain		
4.16	Predefined security groups are utilized to assign role-based access privileges and segregate access within the network domain.	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 within the network domain.	No exceptions noted.
4.17	Administrative access privileges to the network domain are restricted to user accounts accessible by authorized personnel.	Inspected the network domain administrator to determine that administrative access privileges to the network domain were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	Encryption as a Service (EaaS)		
4.18	Client databases, files, disks, data and/or systems are encrypted at rest.	Inspected the storage properties for a sample of clients to determine that encryption for data at rest was in place for each client sampled.	No exceptions noted.
4.19	For customers that subscribe to the VPN tunnel offering, encrypted VPN connections are provided to help ensure that remote connections to the managed production environment are secure.	Inquired of the compliance manager regarding remote connectivity to determine that customers that subscribed to the VPN tunnel offering were provided encrypted VPN connections to help ensure that remote connections to the managed production environment were secure.	No exceptions noted.
		Inspected the VPN configuration for a sample of VPN tunnel customers during the period to determine that a dedicated connection, via an encrypted tunnel and/or secure internet connection, was in place for each client sampled.	No exceptions noted.

DATA BACKUP

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that application and data files are backed up in a timely manner and securely stored.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Automated backup systems are utilized to perform disk-to-disk backups of production data and systems.	Inspected the backup system configurations and backup logs generated during the period for a sample of clients to determine that automated backup systems were utilized to perform disk-to-disk backups of production data and systems for each client sampled.	No exceptions noted.
5.02	The automated backup systems are configured to perform backups of client production environments on at least a weekly 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 weekly backups of the production environments for each client sampled.	No exceptions noted.
5.03	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.
5.04	A consolidated alert report is sent to operations personnel for review on a daily basis to identify potential issues with system backups.	Inquired of the compliance manger regarding the monitoring of system backups to determine that operations personnel reviewed a consolidated alert report on a daily basis to identify potential issues with system backups.	No exceptions noted.
		Inspected the consolidated alert report notification configuration and example consolidated alert report generated during the period to determine that the automated backup systems e-mailed a consolidated alert report to operations personnel for review on a daily basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.05	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.
5.06	The automated backup system is configured to encrypt data in transit to protect the backup information in transit to storage locations.	Inspected the backup system configurations to determine that backups were encrypted in transit to protect the backup information in transit to storage locations.	No exceptions noted.

MAINTENANCE AND CHANGE MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to existing customer infrastructure are authorized, approved, and documented before being implemented in the production environment.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	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.
6.02	Client support requests are submitted and tracked electronically via a ticketing system.	Inspected the listing of client support requests received during the period to determine that each client support request sampled was submitted and tracked electronically via a ticketing system.	No exceptions noted.
6.03	Client support requests are required to be submitted and/or approved by an authorized client administrator.	Inspected the support ticket and list of authorized client administrators for a sample of client support requests received during the period to determine that each client support request sampled was submitted and/or approved by an authorized client administrator.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.04	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.
6.05	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.
6.06	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.07	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 compliance 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.

SYSTEM AVAILABILITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that customer infrastructure is available for operation and use, and that problems are identified, investigated, and resolved in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	Management meetings are held on a monthly basis to review asset inventory reports and help ensure availability of production systems.	Inspected the management meeting invitation and asset inventory reports reviewed during management meetings for a sample of months during the period to determine that management meetings were held each month sampled to review asset inventory reports and help ensure availability of production systems.	No exceptions noted.
7.02	Standard and preconfigured server build procedures are in place to guide personnel in the installation and deployment of production servers.	Inspected the production server build procedures to determine that standard and preconfigured server build procedures were in place to guide personnel in the installation and deployment of production servers.	No exceptions noted.
7.03	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.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.04	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.
7.05	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.
7.06	Operations personnel utilize predefined severity levels to categorize and escalate outages.	Inspected the severity level definitions and a listing of tickets generated during the period to determine that operations personnel utilized predefined severity levels to categorize and escalate outages.	No exceptions noted.
7.07	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.
7.08	Antivirus software is installed on Windows production servers and workstations.	Inspected the antivirus software configurations and registered client listing to determine that antivirus software was configured for Windows production servers and workstations.	No exceptions noted.
7.09	The antivirus software is configured to update virus definitions automatically as they are released.	Inspected the antivirus software configurations to determine that antivirus software was configured to update virus definitions automatically as they are released.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.10	Antivirus software is configured to provide real-time scanning of files as they are accessed or modified.	Inspected the antivirus software configurations to determine that antivirus software was configured to provide real-time scanning of files for registered clients/devices.	No exceptions noted.
7.11	The antivirus software is configured to perform full scans of registered clients/devices on a daily basis.	Inspected the antivirus software configurations to determine that the antivirus software was configured to perform full scans of registered clients/devices on a daily basis.	No exceptions noted.

Customer Support and Incident Response

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that customer inquiries and issues are responded to in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.01	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.	No exceptions noted.
		Inspected the service request, incident, and problem management procedures to determine that the incident response and support procedures included the following: • Severity level definitions • Escalation procedures • Ticket handling procedures • Response time requirements for service alerts	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.02	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.
8.03	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.

SECTION 5

OTHER INFORMATION PROVIDED BY LIGHTEDGE

Management's Response to Testing Exceptions

Physical Security

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.17	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 1
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.		
1.19	An inventory listing of issued physical keys is maintained for the data centers.	Inspected the physical key inventory listings to determine that an inventory listing of issued physical keys was maintained for each data center.	The test of the control activity, performed in May 2022, disclosed that an inventory listing issued physical keys was not maintained at Lenexa data center facility. Subsequent testing of the control activity, performed in June 2022, disclosed that a physical key inventory listing was implemented at the Lenexa data center facility.
Management's Response:	It was identified during a data center walkthrough that the Lenexa data center did not have a physical key check-in/check-out log in use. A check-in/check-out log has been implemented at the Lenexa data center following our standard company policy.		
1.21	DVR backups of surveillance recordings are maintained for a minimum of 90 days.	Inspected recent and historical images from the DVR system to determine that DVR backups of surveillance recordings were maintained for a minimum of 90 days for each data center.	The test of the control activity disclosed that historical DVR images for the San Diego 2 data center facility were not maintained for a minimum of 90 days.
Management's Response:	Due to aging camera infrastructure at San Diego 2, the vendor and internal support were unable to access historical recordings. LightEdge is implementing a new camera and NVR system at the San Diego 2 data center.		

Maintenance and Change Management

<table>
<tr><th>#</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>6.05</td><td>Changes to existing customer infrastructure (except for “standard” changes) require CRB and/or peer approval prior to implementation.</td><td>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.</td><td>The test of the control activity disclosed that approval was not obtained for four (4) of 40 non-standard changes sampled.</td></tr>
<tr><td><b>Management’s Response:</b></td><td colspan="3">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.</td></tr>
<tr><td>6.06</td><td>Infrastructure changes impacting the security and/or availability of customer environments (“normal” changes) are communicated to the customer prior to implementation.</td><td>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.</td><td>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.</td></tr>
<tr><td><b>Management’s Response:</b></td><td colspan="3">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.</td></tr>
</table>