LIGHTEDGE SOLUTIONS, INC.

SOC 2 REPORT

FOR THE

COLOCATION, MANAGED AND HOSTED SERVICES

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

JANUARY 31, 2015

Attestation and Compliance Services

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

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

Table of Contents

Section I

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To LightEdge Solutions, Inc. ("LightEdge"):

We have examined the attached description of LightEdge's colocation, managed, and hosted services system as of January 31, 2015, (the description) performed at the Des Moines, Iowa, corporate office facility, and the Altoona, Iowa, Minneapolis, Minnesota, and Kansas City, Missouri, data center facilities, and the suitability of the design of controls to meet the criteria for the security and availability principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA*, Technical Practice Aids*) (applicable trust services criteria), as of January 31, 2015.

LightEdge has provided the attached assertion, in Section 2, which is based on the criteria identified in management's assertion. LightEdge is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in LightEdge's assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of January 31, 2015.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in LightEdge's assertion and the applicable trust services criteria

a. the description fairly presents LightEdge's colocation, managed, and hosted services system that was designed and implemented as of January 31, 2015; and

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively as of January 31, 2015.

This report and the description of test of controls and results thereof are intended solely for the information and use of LightEdge; user entities of LightEdge's colocation, managed, and hosted services system as of January 31, 2015; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, and other parties;

- Internal control and its limitations;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria ad how controls address those risks.

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

Tampa, Florida
March 19, 2015

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the attached description of LightEdge Solutions, Inc.'s ("LightEdge") colocation, managed, and hosted services system as of January 31, 2015 (the "description") based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the colocation, managed, and hosted services system, particularly system controls intended to meet the criteria for the security and availability principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the colocation, managed, and hosted services system as of January 31, 2015, based on the following description criteria:

    i. The description contains the following information:

        1. The types of services provided;
        2. The components of the system used to provide the services, which are the following:
            - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)
            - *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)
            - *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)
            - *Processes.* The automated and manual procedures
            - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system;
        3. The boundaries or aspects of the system covered by the description;
        4. How the system captures and addresses significant events and conditions;
        5. The process used to prepare and deliver reports and other information to user entities or other parties;
        6. If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;
        7. For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system;
        8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at LightEdge, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
        9. Any applicable trust services criteria that are not addressed by a control at LightEdge or a subservice organization and the reasons therefore; and
        10. Other aspects of LightEdge's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

ii. The description does not omit or distort information relevant to LightEdge's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed as of January 31, 2015, to meet the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Founded in 1996, and headquartered in Des Moines, Iowa, LightEdge Solutions, Inc. (LightEdge) provides an alternative for businesses that traditionally have purchased, maintained and then depreciated equipment related to information technology (IT) functions. By leveraging the economies of scale inherent in the LightEdge network, customers are able to operate on redundant IT platforms.

Description of Services Provided

LightEdge provides IT related infrastructure support to its customers in the form of managed private networks which allow customers to interact with the services provided on the LightEdge networks. As an adjunct to this network offering, the company offers data center hosting services allowing customers to house critical IT infrastructure in a series of highly available and redundant data centers.

The Company provides managed server platforms consisting of LightEdge owned hardware loaded with Microsoft, or other operating systems and hosted on the LightEdge network in a LightEdge data center. Managed backups are performed based on customer specifications for customers operating on managed servers, collocated servers, and servers located on customer premises.

LightEdge offers a variety of contracted colocation and connectivity services to its customers, which are further defined below:

Small Business "Shared" Colocation

Customers lease space in shared access racks for the purpose of hosting their networking equipment. LightEdge does not have logical access to these devices and simply provides power, cooling and network connectivity.

Rack Based Colocation

Customers can lease lock secured enclosures that are capable of handling multiple server and network appliances. LightEdge does not have logical access to these devices and simply provides power, cooling and network connectivity.

Cage Based Colocation

At the Altoona, Iowa, facility, customers are able to lease a private cage for the deployment of network equipment. LightEdge does not have logical access to the devices maintained in the cage space and is responsible for providing power, cooling and network connectivity.

Managed Servers

In the managed server service model, LightEdge owns the physical hardware, provisions the hardware in its data centers and on its network and will, at the customer's request, configure an initial operating system for the customer. LightEdge does not manage the security or operating system of these devices.

Managed Storage

A managed Storage Area Network (SAN) is available for use by customers in conjunction with managed servers and Blade servers. LightEdge is responsible for the provisioning of space on this SAN and determining which machines have access to which data pools. LightEdge does not manage the content of these storage areas except where they are utilized by a managed application offering.

Managed Backup

A managed backup service is provided for both SAN attached storage and customer servers. The Company provides the application framework for managing the backup process. LightEdge does not manage any of the

content being backed up. Backups are stored either locally on a Network Attached Storage (NAS) device or archived for off-site storage.

Remote Location Access

Each data center is able to exchange data with the other data centers on the network utilizing the LightEdge Multi-protocol Label Switching (MPLS) backbone. The MPLS network allows traffic to be physically segregated such that it cannot be intercepted by another customer's network in transit, ensuring data integrity end–to-end during the transfer. The MPLS network is managed by LightEdge employees and has no customer access.

Core Networking

LightEdge uses a set of Ethernet switching products that segment customer networks from each other. The networks are isolated using Virtual Local Area Network (VLAN) technology that allows many customers' networks to run within the building, while being logically separated from one another.

Managed Firewalls

Incorporated within the network is the ability to create multiple firewalls to restrict traffic flow between networks. These firewalls are used to create separate demilitarized zones (DMZ) for each customer's traffic where required. Additionally, the firewalls are utilized to provide front-end security for managed services provided by LightEdge.

Virtual Private Network (VPN) Access

Remote access to the data centers is provided using a VPN concentrator. LightEdge provides a secure access channel for end users; however, customers are responsible for user account maintenance for each VPN device.

Virtual Data Center

In the managed server service model, LightEdge owns the physical hardware, provisions the hardware in its data centers and on its network and will, at the customer's request, configure an initial operating system for the customer. LightEdge does not manage the security or operating system of these devices.

System Boundaries

As outlined in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

Infrastructure and Software

The scope of the examination included LightEdge's colocation, managed, and hosted services system at the Altoona, Iowa, Minneapolis, Minnesota, and Kansas City, Missouri, data center facilities, which are supported by personnel located at the Des Moines, Iowa, corporate office facility and on-site staff at each data center facility.

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

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Active Directory Domain Controller	Network domain supporting the platform and related systems.	Microsoft Windows	Altoona Minneapolis Kansas City

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Application, Web and Database Servers	Production operating systems supporting the platform and related systems.	Microsoft Windows and UNIX servers with SQL Server database	Altoona Kansas City
Firewall	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Cisco FWSM	Altoona Minneapolis Kansas City
MRS System	System to maintain and secure the passwords used to access customer infrastructure.	SQL Server database	Altoona
myLightEdge Portal	Web portal providing customers the ability to monitor their managed infrastructure, hosting services, and requested changes.	N/A	Altoona
Badge Access System	Electronic access system used to restrict physical access to the corporate office facility and data center facilities.	N/A	Altoona
Avamar and Veeam Backup Systems	Commercial backup systems used for disk-to-disk backups of production data and systems.	N/A	Altoona Kansas City

The following software applications are considered secondary support systems used to support the colocation, managed, and hosted services system. These secondary support systems were not considered “in-scope” primary systems.

Secondary Support Systems	
Production Application	**Business Function Description**
VPN	System used to provide remote LightEdge employees access to the production network.
Ni2 Ticketing System	Ticketing system utilized to document and track customer support requests and incidents.
Zenoss Enterprise Monitoring System	System utilized for monitoring the performance and availability of production sites, servers and devices.
Fortinet FortiGate 200D Intrusion Prevention System (IPS)	System used for detecting and preventing unauthorized connections to the network.
Microsoft Forefront Security Antivirus Software	System used to protect certain Windows production servers and workstations from known and malicious software viruses.
Operational Support System (OSS)	System used for managing customers purchased services data, such as customer circuits, services and security.

People

The following functional areas / groups are used to support the colocation, managed, and hosted servers described within this report:

- Client Install Group (CIG) – provides single instance installations for non-complex customers

- Premier Support Group (PSG) – provides installation and support for complex customers
- Network Operations Center (NOC) – provides Tier 1 support for standard customers
- Tier 2 Support – handles trouble tickets for customers across all product platforms
- Operational Engineering – provides Tier 3 support and maintenance of service platforms, 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

Procedures

Access Authentication and Authorization

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

The MRS system is utilized by engineering and system support personnel to maintain and secure the passwords used to access customer infrastructure; passwords that are stored within the client password database are encrypted. The ability to access the client password database is restricted to authorized personnel based on business responsibilities, and system access assigned to terminated employees is disabled.

The myLightEdge portal is in place to provide customers the ability to monitor their managed infrastructure, hosting services, and requested changes. myLightEdge is configured to restrict customers from accessing other customers' data.

Network domain users are authenticated via user account and password before being granted network access. Passwords are subject to system-enforced parameters, such as password minimum length, expiration intervals (maximum password age), complexity requirements, minimum password history, and invalid password account lockout threshold settings to prevent users from reusing previous passwords. User passwords to the network domain are stored in an encrypted format. Predefined security groups are utilized to assign access permissions and access within the network domain are restricted to authorized personnel.

Access Requests and Access Revocation

Dedicated engineering and operations teams are responsible for provisioning logical access to managed infrastructure and hosting services. 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 an annual basis to help ensure that access to data is restricted and authorized. System owners disable user accounts assigned to terminated employees.

Change Management

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

Client support requests must be submitted and approved by an authorized client administrator before project activities are initiated. Once verified, the support requests are documented and tracked within the Ni2 ticketing system. In the event that 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. The ability to implement changes to existing customer infrastructure has been restricted to user accounts accessible by authorized personnel.

A Change Review Board (CRB) is established to function as a governing body to oversee change management activities. Changes that affect customer infrastructure are implemented after being approved by the CRB during a weekly meeting. In the event of an emergency change request, the CRB is notified of the change via e-mail, and the review and approval process is expedited outside of the weekly meeting.

Physical and Environmental Security

Documented policies and procedures are in place to address the granting, controlling and monitoring of physical access into the data centers and office facilities. At the corporate office facility located in Des Moines, Iowa, a receptionist monitors access and manages visitors' access into the building during business hours. When accessing the data centers, located in Altoona, Iowa, Minneapolis, Minnesota, and Kansas City, Missouri, visitors and vendors are required to provide photo identification and sign a visitor log. An electronic badge access system controls access to and within the data centers. In addition, the Altoona and Kansas City data centers utilize multi-factor authentication through the use of biometric scanners and personal identification number (PIN) keypads, as well as, mantraps and tailgating sensors. Badge access into the data centers is restricted to authorized operations personnel and access attempts are logged and traceable to individual cardholders.

The badge access system requires administrative users to authenticate via a user account and password. These users, who have the ability to create, modify and delete user badge access privileges, are authorized and must receive approval by management prior to issuing or modifying badge access. Badge access privileges are revoked by badge administrators as a component of the employee termination process. In addition, data center access listings are maintained to identify approved administrative contacts and data center users. The badge administrators require approval from an authorized client administrator (noted on the data center access listings) prior to issuing, modifying, or revoking badge access privileges to clients. On an annual basis, department managers review badge access privileges and authorized client administrators validate badge access privileges assigned to individuals within (or authorized by) their organization.

Physical key inventory listings are maintained and physical keys are stored in locked cabinets located in a secured room accessible by authorized personnel. Key usage logs are maintained to track the issuance and return of physical keys to the data centers. There are no exterior windows within the server rooms. Surveillance cameras are located within the data centers and a digital video recorder (DVR) system monitors and records access. Backups of the DVR surveillance recordings are maintained for a minimum of three months.

Standard operating procedures are in place to govern environmental security practices at the facilities. To protect the corporate office facility, the building is equipped with 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 ensures that the fire extinguishers and sprinkler system are inspected by a third party on an annual basis.

The data centers are protected by fire extinguishers, audible and visual fire alarms, and fire suppression systems. The Altoona data center utilizes an HFC-125 fire suppression system in Server Rooms #1 and #2 and dry-pipe water sprinklers in Server Room #3; the Minneapolis data center utilizes a FM-200 fire suppression system; and the Kansas City data center utilizes dry-pipe water sprinkler system throughout the facility. Management has contracted with a third party monitoring company to provide 24x7 monitoring of the fire detection and suppression systems at the Altoona data center. The building management companies at the Minneapolis and Kansas City data centers contract with third party monitoring companies to provide LightEdge with 24x7 monitoring of the fire detection and suppression systems. In addition, the chief security officer (CSO) obtains inspection reports as evidence that the fire extinguishers, fire suppression systems, and alarm systems at each of the data centers are inspected by third party specialists 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 thresholds are exceeded. The CSO obtains inspection reports as evidence that the air conditioning units are inspected by third party specialists on a quarterly basis. Production servers are mounted on racks within the data center to facilitate cooling and protect servers from localized flooding.

Production equipment is connected to uninterruptible power supply (UPS) systems that are configured to provide temporary electricity in the event of a power outage. The CSO obtains inspection reports as evidence that the UPS systems are inspected by third party specialists on a semi-annual basis to help ensure proper functioning. Additionally, the data centers are connected to dedicated power generators that provide electricity during long-

term power outages and inspection reports. The CSO obtains inspection reports as evidence that the generators are inspected by third party specialists on an annual basis.

Data Backup and Disaster Recovery

LightEdge utilizes the Avamar and Veeam backup systems to perform disk-to-disk backups of production data and systems. These systems are configured to perform daily backups of client production environments and log the status of backup jobs. Operations personnel are notified via e-mail of backup job success and failures and review a consolidated alert report on a daily basis to identify potential issues with system backups. In addition, backup data is replicated between the data centers and the backup data is encrypted during transit (Altoona is replicated to Minneapolis; Minneapolis is replicated to Altoona; Kansas City is replicated to Altoona).

Incident Response

Documented incident response and support procedures are in place to guide operations personnel in the monitoring, documenting, escalating, and resolving of problems affecting managed hosting and network services. These procedures include procedures regarding severity level definitions, escalation procedures, ticket handling procedures, and response time requirements for service alerts.

The centralized ticketing system is used to track identified issues and customer requests. Additionally, key performance indicator (KPI) reports are generated by the online operational metrics reporting dashboard and reviewed by management on a monthly basis to evaluate system incident, response and resolution activities.

System Monitoring

Production server hardware is protected by equipment warranties to provide service, replacement and on-site maintenance. Server build procedures are in place to guide personnel in the installation and deployment of production servers. Antivirus software is installed on certain production servers and workstations, and is configured to scan registered clients on a daily basis, and scan files on a real-time basis.

The Zenoss enterprise monitoring application monitors the performance and availability of production sites, servers and devices. Operations personnel monitor client environments 24x7, and the Zenoss system alerts operations personnel via onscreen notifications when predefined thresholds are exceeded, such as bandwidth, central processing unit (CPU) usage, and disk usage. The Ni2 issue management system is utilized to document, prioritize, escalate and resolve problems affecting contracted services. These problems and outages are categorized by operations personnel with predefined severity levels.

Data

Physical Security

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

Environmental Security

Environmental equipment at the data center facilities, such as the fire detection and suppression systems, climate control systems, and power supply systems, are subject to preventive maintenance by internal and/or third party specialists. The resulting inspection reports are used to help ensure equipment is maintained and functions properly.

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 such as Exchange and VPN. Lastly, customers are able to open trouble tickets for incidents or requests related to the services in which they are enrolled.

Operational Support System (OSS)

LightEdge uses an internally developed OSS to manage data regarding customers purchased services. Information regarding customer circuits, services and security is stored in this system. The system resides within LightEdge's internal network and utilizes a web-based application only accessible from the corporate network.

Subservice Organizations

No subservice organizations were included in the scope of this assessment. Therefore, the description does not address the criteria in Section 2, items (a)(i)(6) and (a)(i)(8).

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; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the senior management and the executive committee.

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 the service organization has implemented in this area are described below.

- 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.
- Employees sign a proprietary information agreement agreeing not to disclose proprietary or third party confidential information, including customer information, to unauthorized parties.
- Management actively monitors and reports on employees' electronic communication.

Senior Management and Executive Committee Participation

LightEdge's control consciousness is influenced significantly by the participation of the executive committee. 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 the service organization 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 bi-weekly 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 the service organization has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority, responsibility and lines of reporting.
- Management has considered the reporting structure and accountability for business functions and segregated responsibilities by functional areas.

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 the service organization has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into position requirements.
- An employee training program is in place.

Accountability

LightEdge has defined lines of management authority, which are outlined in the organizational chart. On a bi-weekly 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 of Receipt of Materials 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. LightEdge management conducts informal performance reviews for new employees at the end of a 90-day probationary period. 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 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. All 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 at 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

- Fraud incentives and pressures for employees
- Fraud opportunities
- 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 the entity's success. Management has implemented a process whereby the likelihood and impact of various risks to the in-scope services have been assessed.

LightEdge conducts quarterly risk assessment meetings with a rotating schedule of the products provided. In general, each product will be fully reviewed once every two years. Additionally, weekly engineering meetings address likely operational risks to the services and platforms.

The most recent risk assessment identified the following:

Area	Results of Risk Assessment
Facility Security	Likely scenarios resulting in risks to facility security: • Failure of inbound power • Failure of specific power equipment in the critical power chain • Failure of air handling units Note, risks for physical damage to the building are considered to be limited due to construction
Network	Likely scenarios resulting in risks to network availability: • Physical service disruption due to compromised inbound cabling • Loss of upstream service by a given provider
Logical Security	Likely scenario resulting in risks to logical security: • Misconfiguration of customer Internet facing equipment
Backup Management	Failures of the backup disk array systems are possible, but unlikely due to redundancy built into the array

LightEdge operates a peer reviewed change management and control 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.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities

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

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability principles are applicable to the colocation, managed, and hosted services system. Therefore, the description does not address the (a)(i)(9) criteria in Section 2.

Information and Communication Systems

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.

Monitoring

Monitoring Activities

Management at LightEdge undergoes periodic external audits and assessments to evaluate control effectiveness, and, in some cases, receive recommendations for improvement. Additionally, internal examinations of controls are performed as business needs or regulatory environments dictate.

The stakeholders in the audit processes report any finding to a member of the senior management team. The senior management team meets on a bi-weekly basis to review company issues and plan direction. Reviews of current and upcoming audits are performed quarterly during these meetings and input is solicited from the team. Product managers are encouraged to review controls effecting their products and recommend updates to further enhance compliance efforts.

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 trees are in place depending on severity level of an alert with Class 1 and Class 2 alerts receiving vice president level notification within four hours of occurrence, if not resolved.

Evaluating and Communicating Deficiencies

Customer complaints are tracked in an automated ticketing system and reviewed on a quarterly basis for consideration on how to improve control activities. Regulator comments and feedback are incorporated and reviewed by senior management at the conclusion of any audit or auditable actions.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria. Therefore, the description does not address a portion of the (a)(i)(7) criteria in Section 2 related to user-entity controls.

SECTION 4

APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

SECURITY PRINCIPLE AND CRITERIA TABLE

Criteria	Risks	Control Activity Specified by the Service Organization
CC1.0: Common Criteria Related to Organization and Management		
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.	The entity's organizational structure does not provide the necessary information flow to manage security and availability activities. Reporting relationships and organizational structure do not permit effective senior management oversight of security and availability activities.	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
	The roles and responsibilities of key managers are not sufficiently defined to permit proper oversight; management, and monitoring of security and availability activities. Personnel have not been assigned responsibility or delegated sufficient authority to meet security and availability commitments and requirements.	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operations.	Personnel have not been assigned responsibility or delegated sufficient authority to meet security and availability commitments and requirements.	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
CC1.3: Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security and availability have the qualifications and resources to fulfill their responsibilities.	Newly hired or transferred personnel do not have sufficient knowledge and experience to perform their responsibilities.	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
		New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
	Personnel do not have sufficient continuous training to perform their responsibilities.	Employees are required to complete security awareness training on an annual basis to ensure they understand their obligations and responsibilities to comply with the corporate and business unit security policies.
		Management monitors compliance with training requirements on an annual basis.

Criteria	Risks	Control Activity Specified by the Service Organization
	Tools and knowledge resources are insufficient to perform assigned tasks.	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC1.4: The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.	Personnel do not adhere to the code of conduct.	Policies and procedures require that employees sign an acknowledgment form upon hire, indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.
	Candidate has a background considered to be unacceptable by management of the entity.	Background checks are performed for employees as a component of the hiring process.
CC2.0: Common Criteria Related to Communications		
CC2.1: Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	Users misuse the system due to their failure to understand its scope, purpose, and design. Users are unaware of key organization and system support functions, processes, roles and responsibilities. External users fail to address risks for which they are responsible that arise outside the boundaries of the system.	A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to authorized internal and external users.
CC2.2: The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	Users misunderstand the capabilities of the system in providing for security and availability and take actions based on the misunderstanding.	The entity's security and availability commitments and the associated system requirements are documented in customer contracts and service level agreements.
	The entity fails to meet its commitments due to lack of understanding on the part of personnel responsible for providing the service.	Employees are required to complete training on an annual basis to ensure they understand their obligations and responsibilities to comply with the corporate and business unit commitments and the associated system requirements.
		Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet.
		New hires and users requesting access to the network domain are required to acknowledge in writing that they have read and understood the documented policies and procedures that outline the system requirements.

Criteria	Risks	Control Activity Specified by the Service Organization
CC2.3: The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.	The system fails to function as designed due to internal users' failure to comply with their responsibilities.	Employees are required to complete training on an annual basis to ensure they understand their obligations and responsibilities to comply with the corporate and business unit commitments and the associated system requirements.
		Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet.
		New hires and users requesting access to the network domain are required to acknowledge in writing that they have read and understood the documented policies and procedures that outline the system requirements.
	The system fails to function as designed due to external users' failure to meet their responsibilities.	The entity's security and availability commitments and the associated system requirements are documented in customer contracts and service level agreements.
CC2.4: Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, have the information necessary to carry out those responsibilities.	Controls fail to function as designed or operate effectively due to misunderstanding on the part of personnel responsible for implementing and performing those controls resulting in failure to achieve security and availability commitments and requirements.	Employees are required to complete training on an annual basis to ensure they understand their obligations and responsibilities to comply with the corporate and business unit commitments and the associated system requirements.
		Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet.
		New hires and users requesting access to the network domain are required to acknowledge in writing that they have read and understood the documented policies and procedures that outline the system requirements.
CC2.5: Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	System anomalies are detected by internal or external users but the failures are not reported to appropriate personnel resulting in the system failing to achieve its security and availability commitments and requirements.	Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.

Criteria	Risks	Control Activity Specified by the Service Organization
CC2.6: System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.	Users misunderstand changes in system capabilities or their responsibilities in providing for security and availability due to system changes and take actions based on the misunderstanding.	A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.
		Release notes are documented and communicated to management and users for changes and maintenance activities that affect system security.
	Changes in roles and responsibilities and changes to key personnel are not communicated to internal and external users in a timely manner.	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
		Documented position descriptions are in place and updated as needed to communicate changes in roles and responsibilities.
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls		
CC3.1: The entity (1) identifies potential threats that would impair system security and availability commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	Not all system components are included in the risk management process resulting in a failure to identify and mitigate or accept risks.	An inventory listing of all hardware and software within the scope of services is maintained and reviewed on at least an annual basis during the risk assessment process.
	Personnel involved in the risk management process do not have sufficient information to evaluate risks and the tolerance of the entity for those risks.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.
	One or more internal or external risks, that are significant, threaten the achievement of security and availability commitments and requirements that can be addressed by security controls, are not identified.	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.2: The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	Controls and mitigation strategies selected, developed and deployed do not adequately mitigate risk.	A monitoring application is in place to monitor the performance and availability of production sites, servers and devices.
	Deployed controls and mitigation strategies create new risks that fail to be assessed.	An inventory listing of all hardware and software within the scope of services is maintained and reviewed on at least an annual basis during the risk assessment process.
		Documented policies and procedures are in place to guide personnel when performing the risk assessment process.

Criteria	Risks	Control Activity Specified by the Service Organization
		A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.3: The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological) that could significantly affect the system of internal control for security and availability and reassess risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	Not all changes that significantly affect the system are identified resulting in a failure to reassess related risks.	The entity's IT security group monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by senior management.
	Changes that are not properly identified create risks due to the failure of those changes to undergo the risk management process.	Developments in technology and the impact of applicable laws or regulations are considered by senior management as part of the annual risk assessment and IT security planning process.
CC4.0: Common Criteria Related to Monitoring Controls		
CC4.1: The design and operating effectiveness of controls are periodically evaluated against security and availability commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Controls are not suitably designed, configured in accordance with established policies, or operating in an effective manner resulting in a system that does not meet system commitments and requirements.	A monitoring application is in place to monitor the performance and availability of production sites, servers and devices.
		The monitoring application is configured to alert operations personnel via onscreen alert notifications when predefined thresholds are exceeded on monitored systems.
		Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.
CC5.0: Common Criteria Related to Logical and Physical Assess Controls		
CC.5.1: Logical access to security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized users access to system components, or portions thereof, authorized by management including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Not all system infrastructure or system components are protected by logical access security measures resulting in unauthorized modification or use.	Documented standard build procedures are utilized for installation and maintenance of production servers and include use of an access control system to restrict the ability to apply patches to authorized users.
		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 an annual basis to help ensure that access to data is restricted and authorized.
		The network domain is configured to log access related events including, but not limited to, the following: • Account logon • Account logout • Privileged use

Criteria	Risks	Control Activity Specified by the Service Organization
	Logical access security measures do not identify or authenticate users prior to permitting access to IT components.	The network domain is configured to authenticate users with a user account and password. The network domain is configured to enforce predefined user account and password requirements.
		Administrative users authenticate to the badge access system via a user account and password.
		Encrypted VPNs are required for remote access to production and authenticate users with a user account and password.
		myLightEdge is configured to require users to authenticate via a user account and password.
	Logical access security measures do not provide for the segregation of duties required by the system design.	Predefined security groups are utilized to assign role-based access privileges and segregate access within the network domain.
		The ability to create, modify and delete user badge access privileges is restricted to user accounts accessible by authorized personnel (15).
		Privileged user access reviews are performed on an annual basis to help ensure that access to data is restricted and provides for appropriate segregation of duties.
		The online portal is configured to restrict customers from accessing other customers' data.
	Logical access security measures do not restrict access to system configurations, privileged functionality, master passwords, powerful utilities, security devices, and other high risk resources.	Administrative access privileges to the network domain are restricted to user accounts accessible by authorized personnel.
		Administrative users authenticate to the badge access system via a user account and password.
		The ability to create, modify and delete user badge access privileges is restricted to user accounts accessible by authorized personnel (15).
		Privileged user access reviews are performed on an annual basis to help ensure that access to data is restricted and authorized.
		Engineering and system support personnel utilize a client password database to maintain and secure the passwords used to access customer infrastructure.

Criteria	Risks	Control Activity Specified by the Service Organization
		The ability to access the client password database is restricted to user accounts accessible by authorized personnel (96).
		The client password database stores passwords in an encrypted format.
CC.5.2: New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	Valid user identities are granted to unauthorized persons.	Employee and contractor user access requests are documented on a standard access request form and require the approval of a manager.
		Dedicated engineering and operations teams are responsible for provisioning logical access to managed infrastructure and hosting services.
		The network domain is configured to authenticate users with a user account and password. The network domain is configured to enforce predefined user account and password requirements.
	A user that is no longer authorized continues to access system resources.	System owners disable user accounts assigned to terminated employees.
CC.5.3: Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software and data).	Users are not identified when accessing information system components.	The network domain is configured to authenticate users with a user account and password. The network domain is configured to enforce predefined user account and password requirements.
	Valid user identities are assumed by an unauthorized person to access the system. User access credentials are compromised allowing an unauthorized person to perform activities reserved for authorized persons.	The network domain is configured to authenticate users with a user account and password. The network domain is configured to enforce predefined user account and password requirements.
		Encrypted VPNs are required for remote access to production and authenticate users with a user account and password.
CC.5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	Valid users obtain unauthorized access to the system resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error. Access granted through the provisioning process compromises segregation of duties or increases the risk of intentional malicious acts or error.	Predefined security groups are utilized to assign role-based access privileges and segregate access within the network domain.
		Employee and contractor user access requests are documented on a standard access request form and require the approval of a manager.
		Dedicated engineering and operations teams are responsible for provisioning logical access to managed infrastructure and hosting services.
		Privileged user access reviews are performed on an annual basis to help ensure that access to data is restricted and authorized.
		The online portal is configured to restrict customers from accessing other customers' data.

Criteria	Risks	Control Activity Specified by the Service Organization
CC.5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within these locations) is restricted to authorized personnel.	Unauthorized persons gain physical access to system components resulting in damage to components (including threats to personnel), fraudulent or erroneous processing, unauthorized logical access, or compromise of information.	Physical access control systems are in place to restrict access to and within the corporate facility and data centers housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorized individuals.
		Administrative users authenticate to the badge access system via a user account and password.
		The ability to create, modify and delete user badge access privileges is restricted to user accounts accessible by authorized personnel (15).
		Physical access requests are documented on a standard access request form and require manager approval.
	Formerly appropriate physical access becomes inappropriate due to changes in user job responsibilities or system changes resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	Department managers review badge access privileges on an annual basis.
		Badge access privileges are revoked as a component of the employee termination process.
	A formerly authorized person continues to access system resources after that person is no longer authorized.	Department managers review badge access privileges on an annual basis.
		Badge access privileges are revoked as a component of the employee termination process.
		Badge access privileges are sent to authorized client administrators for validation on an annual basis.
	A user obtains the identification credentials and authentication credentials of a formerly authorized person and uses them to gain unauthorized access to the system.	Department managers review badge access privileges on an annual basis.
		Badge access privileges are revoked as a component of the employee termination process.
		Visitors are required to surrender their badges upon exit of the Altoona and Kansas City data centers; visitor badges are not provided at the Minneapolis data center. Visitors are required to be escorted at all times within the data center facilities.
CC.5.6: Logical access security measures have been implemented to protect against to security and availability threats from sources outside the boundaries of the system.	Threats to the system are obtained through external points of connectivity.	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.
		An intrusion prevention system (IPS) is utilized to analyze and report network events.
		Web servers utilize secure sockets layer (SSL) encryption for web communication sessions.

Criteria	Risks	Control Activity Specified by the Service Organization
		Encrypted VPNs are required for remote access to production and authenticate users with a user account and password.
	Authorized connections to the system are compromised and used to gain unauthorized access to the system.	Firewall and router rules are reviewed on an annual basis to ensure that only necessary connections are configured within the rulesets.
CC.5.7: The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they related to security and availability.	Nonpublic information is disclosed during transmission over public communication paths.	Encrypted VPNs are required for remote access to production and authenticate users with a user account and password.
		Web servers utilize secure sockets layer (SSL) encryption for web communication sessions.
		Policies are in place that prohibit the transmission of sensitive information over the Internet or other pubic communications paths unless it is encrypted.
	Removable media (for example, USB drives, DVDs, or tapes) are lost, intercepted, or copied during physical movement between locations. Removable media used to make unauthorized copies of software or data are taken beyond the boundaries of the system.	The automated backup systems are configured to encrypt backup data during transit.
		Documented policies and procedures are in place to guide personnel in the securing of removable media.
CC.5.8: Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	Malicious or otherwise unauthorized code is used to intentionally or unintentionally compromise logical access controls or system functionality through data transmission, removable media, and portable or mobile devices.	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients on a real-time basis • Scan registered clients on a daily basis
CC6.0: Common Criteria Related to System Operations		
CC.6.1: Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	The network domain is configured to log access related events including, but not limited to, the following: • Account logon • Account logout • Privileged use
		A monitoring application is in place to monitor the performance and availability of production sites, servers and devices.

Criteria	Risks	Control Activity Specified by the Service Organization
	Security or other system configuration information is corrupted or otherwise destroyed, preventing the system from functioning as designed.	The automated backup systems are configured to perform backups of client production environments on a daily basis.
CC.6.2: Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Breaches and incidents are not identified, prioritized, or evaluated for effects.	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.
	Corrective measures to address breaches and incidents are not implemented in a timely manner.	Management meetings are held on an as needed basis to discuss incidents and corrective measures to help ensure that incidents are resolved.
	Corrective measures are not effective or sufficient.	Operations personnel utilize an automated issue management system to document, prioritize, escalate and resolve problems affecting contracted services.
		Management meetings are held on an as needed basis to discuss incidents and corrective measures to help ensure that incidents are resolved.
	Lack of compliance with policies and procedures is not addressed through sanctions or remedial actions resulting in increased noncompliance in the future.	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
		New hires and users requesting access to the network domain are required to acknowledge in writing that they have read and understood the documented policies and procedures that outline the system requirements.
	Breaches and incidents recur because preventive measures are not implemented after a previous event.	Operations personnel utilize an automated issue management system to document, prioritize, escalate and resolve problems affecting contracted services.
		Incidents requiring a change to the system follow the standard change control process.
CC7.0: Common Criteria Related to Change Management		
CC.7.1: Security and availability commitments and requirements are addressed during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Commitments and requirements are not addressed at one or more points during the system development lifecycle resulting in a system that does not meet system commitments and requirements.	A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.
		Changes made to existing customer infrastructure are authorized, approved, and documented prior to implementation.

Criteria	Risks	Control Activity Specified by the Service Organization
CC.7.2: Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security and availability.	System components are not updated for changes in requirements resulting in a system that does not meet system commitments and requirements.	A formal risk assessment is performed on an annual basis. Risks that are identified and require changes to the system are documented in the change management system.
		Management meetings are held on an as needed basis to discuss incidents and corrective measures to help ensure that incidents are resolved.
CC.7.3: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Identified breaches, incidents, and other system impairments are not considered during the change management lifecycle.	Incidents requiring a change to the system follow the standard change control process.
CC.7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and availability commitments and requirements.	System changes are not authorized by those responsible for the design and operation of the system resulting in changes to the system that impairs its ability to meet system commitments and requirements. System changes do not function as intended resulting in a system that does not meet system commitments and requirements.	Changes made to existing customer infrastructure are authorized, approved, and documented prior to implementation.
		The ability to implement changes to existing customer infrastructure is restricted to user accounts accessibly by authorized personnel.
	Unforeseen system implementation problems impair system operation resulting in a system that does not function as designed.	Documented policies and procedures are in place to guide personnel in the rollback of changes in the event that a change impairs system operation.
	Incompatible duties exist within the change management process, particularly between approvers, designers, implemented testers, and owners, resulting in the implemented system not functioning as intended.	Change management policies and procedures are documented that outline that change management separation of duties such that authorization, testing and implementation are segmented functions within the process.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Criteria	Risks	Control Activity Specified by the Service Organization
A1.1: Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	Current processing capacity is not sufficient to meet availability commitments and requirements in the event of the loss of individual elements within the system components.	A monitoring application is in place to monitor the performance and availability of production sites, servers and devices.
	Processing capacity is not monitored, planned, and expanded or modified, as necessary, to provide for the continued availability of the system in accordance with system commitments and requirements.	A monitoring application is in place to monitor the performance and availability of production sites, servers and devices.
		Management meetings are held on a monthly basis to review availability trends and availability forecasts as compared to system commitments.
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet availability commitments and requirements.	Environmental vulnerabilities and changing environmental conditions are not identified or addressed through the use of environmental protections resulting in a loss of system availability.	The data centers are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • Uninterruptible power supply (UPS) systems • Generators • Air conditioning units
		The CSO retains the inspection report received from third party specialists evidencing completion of inspection and maintenance of the following on a periodic basis: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units
	Environmental vulnerabilities are not monitored or acted upon increasing the severity of an environmental event.	Operations personnel monitor client environments 24 hours per day.
	Software or data are lost or not available due to processing error, intentional act, or environmental event.	The automated backup systems are configured to perform backups of client production environments on a daily basis.
		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.
		Backup data is replicated between data centers that are geographically separated.

Criteria	Risks	Control Activity Specified by the Service Organization
	System availability commitments and requirements are not met due to a lack of recovery infrastructure.	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
		Backup data is replicated between data centers that are geographically separated.
A1.3: Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	Recovery plans are not suitably designed and backups are not sufficient to permit recovery of system operation in accordance with commitments and requirements.	IT personnel perform restoration of backup files as a component of business operations.
		Disaster recovery plans are tested on a quarterly basis.