LightEdge Solutions, LLC

Independent Practitioner's Report on the Controls Related to the National Institute of Standards and Technology (NIST) Publication Series 800-53 for the Colocation, Managed, and Hosted Services

July 31, 2022

Attestation and Compliance Services

This report is intended solely for use by the management of LightEdge Solutions, LLC (“LightEdge”), its user entities (i.e., customers) that utilized the services covered by this report during the specified time period (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 PRACTITIONER'S REPORT

INDEPENDENT PRACTITIONER'S REPORT

To LightEdge Solutions, LLC:

Scope

We have examined LightEdge Solutions, LLC ("LightEdge") assertion that the description of its controls supporting its colocation, managed, and hosted services performed at the facilities listed in Section 3 (the "description") are fairly presented as of July 31, 2022, and that controls supporting the colocation, managed, and hosted services conforms, as applicable, with the control guidance from the National Institute of Standards and Technology ("NIST") Special Publication Series 800-53 revision 5 with the moderate categorization (as defined by the Federal Information Processing Standard (FIPS-199)) control specifications for the specified control families, is presented in accordance with the criteria set forth in the LightEdge assertion in Section 2.

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description includes only the controls of LightEdge and excludes the controls of the subservice organization. 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.

In Section 5, LightEdge has provided additional information that is not a part of LightEdge's description. Such information has not been subjected to the procedures applied in our examination of the description and of the suitability of design of controls to achieve the related control objectives stated in the description, and accordingly, we express no opinion on it.

LightEdge's Responsibilities

LightEdge has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria. LightEdge is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services and related controls covered by the description; determining the applicability of the controls; and implementing the controls described therein conform to the NIST standard for the specified control families.

Independent Practitioner's Responsibilities

Our responsibility is to express an opinion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence regarding the supporting information security program supporting the colocation, managed, and hosted services system and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls may not prevent, or detect and correct, all errors or omissions related to a system or 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 is subject to the risk that controls may become inadequate or fail.

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 controls supporting the colocation, managed, and hosted services at the facilities listed in Section 3 that were designed and implemented as of July 31, 2022.

b. The controls supporting the colocation, managed, and hosted services met applicable control guidance from the NIST Special Publication Series 800-53 revision 5 with the moderate categorization (as defined by FIPS-199) control specifications for the specified control families, based on the criteria set forth in management's assertions.

Restricted Use

This report is intended solely for the information and use of LightEdge and customers of LightEdge's colocation, managed, and hosted services as of July 31, 2022, who have sufficient knowledge and understanding of the following:

- The nature of the service provided by LightEdge;
- The nature of the data provided to LightEdge;
- How LightEdge's system interacts with customers;
- Internal control and its limitations;
- The applicable NIST Standards; and
- The risks that may threaten the achievement of the applicable NIST Standards and how controls address those risks.

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

Schellman & Company, LLC

Tampa, Florida
August 29, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of LightEdge Solutions, LLC ("LightEdge") controls supporting the colocation, managed, and hosted services at the facilities listed in Section 3 provided to customers of LightEdge's colocation, managed, and hosted services as of July 31, 2022 (the "Description"). We confirm, to the best of our knowledge and belief, that:

a. Management's Description fairly presents LightEdge's controls for its colocation, managed, and hosted services that were designed and implemented as of July 31, 2022 (the "Controls"). The criteria we used in making this assertion were that the Description:

   i.) presents the Controls as designed and implemented to support the colocation, managed, and hosted services;

   ii.) describes the specified Controls designed to achieve the information security program's objectives; and

   iii.) does not omit or distort information relevant to the Controls.

b. The controls governing the colocation, managed, and hosted services conform to the applicable control guidance from the National Institute of Standards and Technology ("NIST") Special Publication Series 800-53 revision 5 with the moderate categorization (as defined by FIPS-199) control specifications for the specified control families. The criteria we used in making this assertion were that:

   i.) we performed an assessment to determine the applicability and implementation status of the controls supporting the colocation, managed, and hosted services with each applicable control identified as implemented, partially implemented, or not implemented; and

   ii.) the controls documented included moderate baseline controls from the following NIST SP 800-53 revision 5 control families:

   - Awareness and Training (AT);
   - Contingency Planning (CP);
   - Personnel Security (PS);
   - Physical and Environmental Protection (PE); and
   - Risk Assessment (RA); and

   iii.) the controls, both automated and manual, were implemented as designed.

Section 3 of this report includes LightEdge's description of the controls supporting its colocation, managed, and hosted services that is covered by this assertion.

Section 3

Description of the Controls Supporting the Colocation, Managed, and Hosted Services

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 description below is based on information security program elements cited in Federal Information Security Management Act (FISMA), specifically §3544(b) (or 44 U.S.C. §3544). As FISMA makes references to NIST for detailed guidance, our detailed control activities in Section 4 are presented alongside the content of NIST SP 800-53 Revision 5 (or "NIST 800-53"). Sections of the NIST 800-53 standard that were completely not applicable, or the customers' responsibility, were not included in Section 4.

Infrastructure and Processes

Awareness and Training

LightEdge continually monitors the competence levels of its employees and provides them with the ability to participate in a variety of training courses relevant to information security. 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. Security policies and training and awareness content are updated annually and made in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. The training content incorporates lessons learned from internal or external security incidents or breaches and also instructs employees how to recognize and report potential and actual instances of social engineering and social mining. Furthermore, LightEdge has designated a Chief Security Officer (CSO) to manage the development, documentation, and dissemination of the awareness and training policies and procedures. Additional training courses are available to new and existing employees to maintain and advance the skill level of personnel. LightEdge management monitors the compliance of employees in completing required trainings through their learning management system on at least an annual basis.

Contingency Planning

A business continuity plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Contingency plans and policies are documented consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Contingency planning activities include ensuring alternate telecommunications provider agreements are in place in the event of a primary provider outage and daily data backups are completed to help ensure system recovery. In addition, backup data is replicated between geographically separate data centers at a frequency determined by the customer. Management performs contingency plan testing on at least an annual basis including a test of the integrity of backup data. Lessons learned from contingency plan testing, training, or actual contingency activities are incorporated into contingency testing and training. LightEdge has designated the CSO to manage the development, documentation, and dissemination of the contingency planning policy and procedures.

Personnel Security

Documented organizational and security policies are in place to communicate entity values and behavioral standards to personnel. These policies are managed by the CSO and documented consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Hiring procedures include candidate interviews and background checks. LightEdge employees are required to be re-screened in the event a previous employee is rehired. Documented position descriptions are in in place to communicate required levels of knowledge to perform the day-to-day requirements and includes security and privacy roles and responsibilities required of the position. 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, an exit interview is performed, management personnel notify security personnel of employee termination, and a termination ticket is created. Security personnel complete a termination checklist and track the process within the termination ticket. The terminated employee’s access credentials are then disabled and LightEdge system and security related property is retrieved. Additionally, employee’s access credentials are also reviewed, and modified if needed, when an employee is reassigned or transferred within the organization.

Physical and Environmental Protection

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.

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.

Risk Assessment

A formal risk assessment policy is in place to guide personnel in performing risk assessments. LightEdge has designated a management review board to manage the development, documentation, and dissemination of the risk assessment policy and procedures. Additionally, risk assessment policies and procedures are made to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. The risk assessment process includes identification and analysis of risks that pose a threat the organization's ability to perform the in-scope services, including supply chain risks associated with system components and 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.

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

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

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.

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

Critical system components and functions are identified by performing a criticality analysis for system components and services during the annual internal audit. Vulnerability assessments are performed on a monthly basis to identify threats and assess their potential impact to system security. Identified security vulnerabilities are triaged by the Information Security Team and monitored through resolution.

In-Scope NIST 800-53 Control Families

Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Applicable Control Matrix

The below table documents the status and applicability of each NIST 800-53 rev 4 moderate control to LightEdge's colocation, managed, and hosted services. Section 4, the testing matrices, includes only the control families that are applicable to the colocation, managed, and hosted services. The status legend is as follows:

- "I" indicates the control is in place.
- "P" indicates the control is partially in place due to deviation.
- "N" indicates the control is not in place due to deviation.
- "N/A" indicates the control is not applicable.

Control	Status	Control	Status	Control	Status	Control	Status
AT-1	I	**CP-7**	I	**PE-6**	I	**PS-5**	I
AT-2	I	**CP-7(1)**	I	**PE-6(1)**	I	**PS-6**	I
AT-2(2)	I	**CP-7(2)**	I	**PE-8**	I	**PS-7**	I
AT-2(3)	I	**CP-7(3)**	N/A	**PE-9**	I	**PS-8**	I
AT-3	I	**CP-8**	I	**PE-10**	I	**PS-9**	I
AT-4	I	**CP-8(1)**	N/A	**PE-11**	I	**RA-1**	I

Control	Status	Control	Status	Control	Status	Control	Status
CP-1	I	**CP-8(2)**	I	**PE-12**	I	**RA-2**	I
CP-2	I	**CP-9**	I	**PE-13**	I	**RA-3**	I
CP-2(1)	I	**CP-9(1)**	I	**PE-13(1)**	I	**RA-3(1)**	I
CP-2(3)	I	**CP-9(8)**	I	**PE-14**	I	**RA-5**	I
CP-2(8)	I	**CP-10**	I	**PE-15**	I	**RA-5(2)**	I
CP-3	I	**CP-10(2)**	N/A	**PE-16**	I	**RA-5(5)**	I
CP-4	I	**PE-1**	I	**PE-17**	I	**RA-5(11)**	I
CP-4(1)	I	**PE-2**	I	**PS-1**	I	**RA-7**	I
CP-6	I	**PE-3**	I	**PS-2**	I	**RA-9**	I
CP-6(1)	I	**PE-4**	I	**PS-3**	I		
CP-6(3)	I	**PE-5**	I	**PS-4**	I		

The following control families were not applicable to LightEdge's colocation, managed, and hosted services and are not represented in the table above:

- Access Control
- Audit and Accountability
- Assessment, Authorization, and Monitoring
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Planning
- Program Management
- Personally Identifiable Information Processing and Transparency
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Supply Chain Risk Management

Section 4

Controls Implemented by LightEdge Supporting the Colocation, Managed, and Hosted Services

Awareness and Training

#	Baseline	NIST Control	Comment
AT-1	M	a. Develop, document, and disseminate to *LightEdge employees*: 1. Organization-level awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;	In place.
		b. Designate a chief security officer to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and	In place.
		c. Review and update the current awareness and training: 1. Policy *annually* and following *system changes*; and 2. Procedures *annually* and following *system changes*.	In place.
AT-2	M	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and *monthly* thereafter; and 2. When required by system changes;	In place.
		b. Employ the following techniques to increase the security and privacy awareness of system users: • *Physical security policies and procedures posted for review at data center facilities; and* • *Quarterly All-Hands Meetings;*	In place.
		c. Update literacy training and awareness content *annually* and following *changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines*; and	In place.
		d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	In place.
AT-2(2)	M	Provide literacy training on recognizing and reporting potential indicators of insider threat.	In place.
AT-2(3)	M	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	In place.
AT-3	M	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: 1. Before authorizing access to the system, information, or performing assigned duties, and *annually* thereafter; and 2. When required by system changes;	In place.
		b. Update role-based training content *annually* and following *system changes*; and	In place.
		c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	In place.

#	Baseline	NIST Control	Comment
AT-4	M	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and	In place.
		b. Retain individual training records for *at least 12 months*.	In place.

Contingency Planning

#	Baseline	NIST Control	Comment
CP-1	M	a. Develop, document, and disseminate to *LightEdge employees*: 1. Organization-level contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;	In place.
		b. Designate a chief security officer to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and	In place.
		c. Review and update the current contingency planning: 1. Policy *annually* and following *system changes*; and 2. Procedures *annually* and following *system changes*.	In place.
CP-2	M	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by *the chief security officer*;	In place.
		b. Distribute copies of the contingency plan to *the emergency response team*;	In place.
		c. Coordinate contingency planning activities with incident handling activities;	In place.
		d. Review the contingency plan for the system *annually*;	In place.
		e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;	In place.
		f. Communicate contingency plan changes to *the emergency response team;*	In place.

#	Baseline	NIST Control	Comment
		g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and	In place.
		h. Protect the contingency plan from unauthorized disclosure and modification.	In place.
CP-2(1)	M	Coordinate contingency plan development with organizational elements responsible for related plans.	In place.
CP-2(3)	M	Plan for the resumption of essential] mission and business functions within *12 hours* of contingency plan activation.	In place.
CP-2(8)	M	Identify critical system assets supporting *essential* mission and business functions.	In place.
CP-3	M	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within *12 months* of assuming a contingency role or responsibility; 2. When required by system changes; and 3. *Annually* thereafter; and	In place.
		b. Review and update contingency training content *annually* and following *system changes*.	In place.
CP-4	M	a. Test the contingency plan for the system *annually* using *tabletop testing* to determine the effectiveness of the plan and the readiness to execute the plan;	In place.
		b. Review the contingency plan test results; and	In place.
		c. Initiate corrective actions, if needed.	In place.
CP-4(1)	M	Coordinate contingency plan testing with organizational elements responsible for related plans.	In place.
CP-6	M	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and	In place.
		b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	In place.
CP-6(1)	M	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	In place.
CP-6(3)	M	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	In place.
CP-7	M	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of *information system operations* for essential mission and business functions within *12 hours* when the primary processing capabilities are unavailable;	In place.
		b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and	In place.
		c. Provide controls at the alternate processing site that are equivalent to those at the primary site.	In place.
CP-7(1)	M	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	In place.
CP-7(2)	M	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	In place.

#	Baseline	NIST Control	Comment
CP-7(3)	M	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Not applicable.
CP-8	M	Establish alternate telecommunications services, including necessary agreements to permit the resumption of *information system operations* for essential mission and business functions *immediately* when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	In place.
CP-8(1)	M	(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and	Not applicable.
		(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Not applicable.
CP-8(2)	M	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	In place.
CP-9	M	a. Conduct backups of user-level information contained in *the information system daily*;	In place.
		b. Conduct backups of system-level information contained in the system *daily*;	In place.
		c. Conduct backups of system documentation, including security- and privacy-related documentation *continuously;* and	In place.
		d. Protect the confidentiality, integrity, and availability of backup information.	In place.
CP-9(1)	M	Test backup information *annually* to verify media reliability and information integrity.	In place.
CP-9(8)	M	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of *organization-defined backup information*.	In place.
CP-10	M	Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure.	In place.
CP-10(2)	M	Implement transaction recovery for systems that are transaction-based.	Not applicable.

Personnel Security

#	Baseline	NIST Control	Comment
PS-1	M	a. Develop, document, and disseminate to *LightEdge employees*: 1. Organization-level personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;	In place.

#	Baseline	NIST Control	Comment
		b. Designate a chief security officer to manage the development, documentation, and dissemination of the personnel security policy and procedures; and	In place.
		c. Review and update the current personnel security: 1. Policy *annually* and following *system changes*; and 2. Procedures *annually* and following *system changes*.	In place.
PS-2	M	a. Assign a risk designation to all organizational positions;	In place.
		b. Establish screening criteria for individuals filling those positions; and	In place.
		c. Review and update position risk designations *annually*.	In place.
PS-3	M	a. Screen individuals prior to authorizing access to the system; and	In place.
		b. Rescreen individuals in accordance with *background check policies and when a previous employee is rehired*.	In place.
PS-4	M	Upon termination of individual employment: a. Disable system access within *24 hours*;	In place.
		b. Terminate or revoke any authenticators and credentials associated with the individual;	In place.
		c. Conduct exit interviews that include a discussion of *the reason for leaving, how LightEdge could improve, and details on the employee's termination date*;	In place.
		d. Retrieve all security-related organizational system-related property; and	In place.
		e. Retain access to organizational information and systems formerly controlled by terminated individual.	In place.
PS-5	M	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;	In place.
		b. Initiate *transition procedures* within *one week from the transition effective date*;	In place.
		c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and	In place.
		d. Notify *compliance and security* within *24 hours*.	In place.
PS-6	M	a. Develop and document access agreements for organizational systems;	In place.
		b. Review and update the access agreements *annually*; and	In place.
		c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or *annually*.	In place.
PS-7	M	a. Establish personnel security requirements, including security roles and responsibilities for external providers;	In place.
		b. Require external providers to comply with personnel security policies and procedures established by the organization;	In place.
		c. Document personnel security requirements;	In place.
		d. Require external providers to notify *LightEdge support* of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within *24 hours*; and	In place.
		e. Monitor provider compliance with personnel security requirements.	In place.

#	Baseline	NIST Control	Comment
PS-8	M	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and	In place.
		b. Notify *general counsel* within *24 hours* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	In place.
PS-9	M	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	In place.

Physical and Environmental Protection

#	Baseline	NIST Control	Comment
PE-1	M	a. Develop, document, and disseminate to *LightEdge employees*: 1. Organization-level physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;	In place.
		b. Designate a chief security officer to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and	In place.
		c. Review and update the current physical and environmental protection: 1. Policy *annually* and following *system changes*; and 2. Procedures *annually* and following *system changes*.	In place.
PE-2	M	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;	In place.
		b. Issue authorization credentials for facility access;	In place.
		c. Review the access list detailing authorized facility access by individuals *annually*; and	In place.
		d. Remove individuals from the facility access list when access is no longer required.	In place.
PE-3	M	a. Enforce physical access authorizations at *entry/exit points to the facility where the information systems reside* by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using an electronic badge system;	In place.
		b. Maintain physical access audit logs for *entry/exit points*;	In place.

#	Baseline	NIST Control	Comment
		c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: 1. Electronic badge access system; 2. Biometric scanners; 3. PIN keypads; and 4. Surveillance cameras;	In place.
		d. Escort visitors and control visitor activity *while on-site at one of the data center facilities*;	In place.
		e. Secure keys, combinations, and other physical access devices;	In place.
		f. Inventory *physical keys and badges and verifies badge access and biometric readers are in an operational state* every *day*; and	In place.
		g. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.	In place.
PE-4	M	Control physical access to *system distribution and transmission lines* within organizational facilities using *telecommunication rooms requiring electronic badge and multi factor authentication; surveillance cameras; and wiring located out of arms reach*.	In place.
PE-5	M	Control physical access to output from *information system output devices* to prevent unauthorized individuals from obtaining the output.	In place.
PE-6	M	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;	In place.
		b. Review physical access logs *continuously* and upon occurrence of *notification from the monitoring systems*; and	In place.
		c. Coordinate results of reviews and investigations with the organizational incident response capability.	In place.
PE-6(1)	M	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	In place.
PE-8	M	a. Maintain visitor access records to the facility where the system resides for *90 days*;	In place.
		b. Review visitor access records *in the event of a reported physical security incident*; and	In place.
		c. Report anomalies in visitor access records to *the compliance and security teams.*	In place.
PE-9	M	Protect power equipment and power cabling for the system from damage and destruction.	In place.
PE-10	M	a. Provide the capability of shutting off power to *the information system or individual system components* in emergency situations;	In place.
		b. Place emergency shutoff switches or devices in *accordance with local laws and regulations* to facilitate access for authorized personnel; and	In place.
		c. Protect emergency power shutoff capability from unauthorized activation.	In place.
PE-11	M	Provide an uninterruptible power supply to facilitate *transition of the information system to long-term alternate power* in the event of a primary power source loss.	In place.
PE-12	M	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	In place.

#	Baseline	NIST Control	Comment
PE-13	M	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	In place.
PE-13(1)	M	Employ fire detection systems that activate automatically and notify *operation staff* and *fire authorities* in the event of a fire.	In place.
PE-14	M	a. Maintain *temperature and humidity* levels within the facility where the system resides at *70-72 degrees Fahrenheit with a humidity level of 45%*; and	In place.
		b. Monitor environmental control levels *on a real-time basis through the data center building management system (BMS)*.	In place.
PE-15	M	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	In place.
PE-16	M	a. Authorize and control *assets* entering and exiting the facility; and	In place.
		b. Maintain records of the system components.	In place.
PE-17	M	a. Determine and document the *continuity facilities* allowed for use by employees;	In place.
		b. Employs *physical and environmental security controls* at alternate work sites;	In place.
		c. Assess the effectiveness of controls at alternate work sites; and	In place.
		d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	In place.

Risk Assessment

#	Baseline	NIST Control	Comment
RA-1	M	a. Develop, document, and disseminate to *LightEdge employees*: 1. Organization-level risk assessment policy that: a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;	In place.
		b. Designate a *management review board* to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and	In place.
		c. Review and update the current risk assessment: 1. Policy *annually* and following *system changes*; and 2. Procedures *annually* and following *system changes*.	In place.

#	Baseline	NIST Control	Comment
RA-2	M	a. Categorize the system and information it processes, stores, and transmits;	In place.
		b. Document the security categorization results, including supporting rationale, in the security plan for the system; and	In place.
		c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	In place.
RA-3	M	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;	In place.
		b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;	In place.
		c. Document risk assessment results in *the risk register and risk assessment report*;	In place.
		d. Review risk assessment results *annually*;	In place.
		e. Disseminate risk assessment results to *the management review board*; and	In place.
		f. Update the risk assessment *annually* or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	In place.
RA-3(1)	M	(a) Assess supply chain risks associated with system components and services; and	In place.
		(b) Update the supply chain risk assessment *annually,* when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	In place.
RA-5	M	a. Monitor and scan for vulnerabilities in the system and hosted applications *at least monthly* and when new vulnerabilities potentially affecting the system are identified and reported;	In place.
		b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact;	In place.
		c. Analyze vulnerability scan reports and results from vulnerability monitoring;	In place.
		d. Remediate legitimate vulnerabilities *within 7 days for emergency, 30 days for high, 60 days for moderate, and 90 days for low rated vulnerabilities* in accordance with an organizational assessment of risk;	In place.
		e. Share information obtained from the vulnerability monitoring process and control assessments with *security, engineering, and operations* to help eliminate similar vulnerabilities in other systems; and	In place.
		f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.	In place.

#	Baseline	NIST Control	Comment
RA-5(2)	M	Update the system vulnerabilities to be scanned *daily when new vulnerabilities are identified and reported*.	In place.
RA-5(5)	M	Implement privileged access authorization to *vulnerability scanning tools* for *vulnerability scanning activities*.	In place.
RA-5(11)	M	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	In place.
RA-7	M	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	In place.
RA-9	M	Identify critical system components and functions by performing a criticality analysis for *system components and services during the annual internal audit*.	In place.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

NIST 800-171 TO NIST 800-53 MAPPING

The information contained within this section is for informational purposes only. The table below maps each NIST 800-171 control to the NIST 800-53 control at the moderate baseline.

✓ indicates the requirement was tested (refer to Section 4) based on the subset of NIST 800-53 control families included within this report relevant to LightEdge's colocation, managed, and hosted services.

NIST 800-171 Control	NIST 800-53 Control	Tested	NIST 800-171 Control	NIST 800-53 Control	Tested
3.1.1	AC-2		**3.6.3**	IR-3	
	AC-3		**3.7.1**	MA-2	
	AC-17			MA-3	
3.1.2	AC-2			MA-3(1)	
	AC-3			MA-3(2)	
	AC-17		**3.7.2**	MA-2	
3.1.3	AC-4			MA-3	
3.1.4	AC-5			MA-3(1)	
3.1.5	AC-6			MA-3(2)	
	AC-6(1)		**3.7.3**	MA-2	
	AC-6(5)		**3.7.4**	MA-3(2)	
3.1.6	AC-6(2)		**3.7.5**	MA-4	
3.1.7	AC-6(9)		**3.7.6**	MA-5	
	AC-6(10)		**3.8.1**	MP-2	
3.1.8	AC-7			MP-4	
3.1.9	AC-8			MP-6	
3.1.10	AC-11		**3.8.2**	MP-2	
	AC-11(1)			MP-4	
3.1.11	AC-12			MP-6	
3.1.12	AC-17(1)		**3.8.3**	MP-2	
3.1.13	AC-17(2)			MP-4	
3.1.14	AC-17(3)			MP-6	
3.1.15	AC-17(4)		**3.8.4**	MP-3	
3.1.16	AC-18		**3.8.5**	MP-5	
3.1.17	AC-18(1)		**3.8.6**	MP-5(4)	
3.1.18	AC-19		**3.8.7**	MP-7	
3.1.19	AC-19(5)		**3.8.8**	MP-7(1)	
3.1.20	AC-20		**3.8.9**	CP-9	✓
	AC-20(1)		**3.9.1**	PS-3	✓

NIST 800-171 Control	NIST 800-53 Control	Tested	NIST 800-171 Control	NIST 800-53 Control	Tested
3.1.21	AC-20(2)		**3.9.1 *(cont.)***	PS-4	✓
3.1.22	AC-22			PS-5	✓
3.2.1	AT-2	✓	**3.9.2**	PS-3	✓
	AT-3	✓		PS-4	✓
3.2.2	AT-2	✓		PS-5	✓
	AT-3	✓	**3.10.1**	PE-2	✓
3.2.3	AT-2(2)	✓		PE-4	✓
3.3.1	AU-2			PE-5	✓
	AU-3			PE-6	✓
	AU-3(1)		**3.10.2**	PE-2	✓
	AU-6			PE-4	✓
	AU-11			PE-5	✓
	AU-12			PE-6	✓
3.3.2	AU-2		**3.10.3**	PE-3	✓
	AU-3		**3.10.4**	PE-3	✓
	AU-3(1)		**3.10.5**	PE-3	✓
	AU-6		**3.10.6**	PE-17	✓
	AU-11		**3.11.1**	RA-3	✓
	AU-12		**3.11.2**	RA-5	✓
3.3.3	AU-2(3)			RA-5(5)	✓
3.3.4	AU-5		**3.11.3**	RA-5	✓
3.3.5	AU-6(3)		**3.12.1**	CA-2	
3.3.6	AU-7			CA-5	
3.3.7	AU-8			CA-7	
	AU-8(1)			PL-2	
3.3.8	AU-9		**3.12.2**	CA-2	
3.3.9	AU-9(4)			CA-5	
3.4.1	CM-2			CA-7	
	CM-6			PL-2	
	CM-8		**3.12.3**	CA-2	
	CM-8(1)			CA-5	
3.4.2	CM-2			CA-7	
	CM-6			PL-2	
	CM-8		**3.12.4**	CA-2	
	CM-8(1)			CA-5	
3.4.3	CM-3			CA-7	

NIST 800-171 Control	NIST 800-53 Control	Tested	NIST 800-171 Control	NIST 800-53 Control	Tested
3.4.4	CM-4		**3.12.4 (cont.)**	PL-2	
3.4.5	CM-5		**3.13.1**	SC-7	
3.4.6	CM-7			SA-8	
3.4.7	CM-7(1)		**3.13.2**	SC-7	
	CM-7(2)			SA-8	
3.4.8	CM-7(4)		**3.13.3**	SC-2	
	CM-7(5)		**3.13.4**	SC-4	
3.4.9	CM-11		**3.13.5**	SC-7	
3.5.1	IA-2		**3.13.6**	SC-7(5)	
	IA-3		**3.13.7**	SC-7(7)	
	IA-5		**3.13.8**	SC-8	
3.5.2	IA-2			SC-8(1)	
	IA-3		**3.13.9**	SC-10	
	IA-5		**3.13.10**	SC-12	
3.5.3	IA-2(1)		**3.13.11**	SC-13	
	IA-2(2)		**3.13.12**	SC-15	
	IA-2(3)		**3.13.13**	SC-18	
3.5.4	IA-2(8)		**3.13.14**	SC-19	
	IA-2(9)		**3.13.15**	SC-23	
3.5.5	IA-4		**3.13.16**	SC-28	
3.5.6	IA-4		**3.14.1**	SI-2	
3.5.7	IA-5(1)			SI-3	
3.5.8	IA-5(1)			SI-5	
3.5.9	IA-5(1)		**3.14.2**	SI-2	
3.5.10	IA-5(1)			SI-3	
3.5.11	IA-6			SI-5	
3.6.1	IR-2		**3.14.3**	SI-2	
	IR-4			SI-3	
	IR-5			SI-5	
	IR-6		**3.14.4**	SI-3	
	IR-7		**3.14.5**	SI-3	
3.6.2	IR-2		**3.14.6**	SI-4	
	IR-4			SI-4(4)	
	IR-5		**3.14.7**	SI-4	
	IR-6				
	IR-7				